AZƏRBAYCAN RESPUBLİKASI

Əlyazması hüququnda

MƏXFİ İNFORMASİYANIN GİZLƏDİLMƏSİ ÜÇÜN EFFEKTİV ALQORİTMLƏRİN TƏDQİQİ VƏ İŞLƏNİLMƏSİ

İxtisas: 3339.01 – İnformasiyanın mühafizəsi üsulları və sistemləri, informasiya təhlükəsizliyi

Elm sahəsi: Texnika elmləri

Fəlsəfə doktoru elmi dərəcəsi almaq üçün təqdim edilmiş

DİSSERTASİYA

İddiaçı: Ababil Faxrəddin qızı Nağıyeva

Elmi rəhbər: professor, texnika elmləri doktoru Sakit Qambay oğlu Verdiyev

Gəncə – 2025

MÜNDƏRİCAT

GİRİŞ

İşin aktuallığı. İnternetin və müasir naqilsiz rabitə vasitələrinin geniş tətbiqi multimedia növlü informasiyanın kütləvi halda mübadilə edilməsinə yeni imkanlar yaratmışdır. Bununla əlaqədar olaraq həm saxlanılan, həm də qlobal və lokal şəbəkələrlə ötürülən informasiyanın təhlükəsizliyinə aid yeni problemlər meydana çıxıb. Son zamanlarda yaradılan və ümumdünya səviyyəsində istifadə edilən şəbəkələr, proqram təminatları və müxtəlif rəqəmsal qurğular kompüter istifadəçilərinin qlobal səviyyədə multimedia resurslarına əlçatanlıq imkanlarını genişləndirib. Nəticədə bədniyyətli hücumçuların açıq kommunikasiya kanalları ilə ötürülən məxfi informasiyanın aşkarlanmasına olan marağın artmasına səbəb olub. Rəqəmsal aləmdə məxfi informasiyanın icazəsiz müdaxilələrdən qorunması həddən artıq mühüm məsələdir. İnformasiya təhlükəsizliyində müxtəlif istiqamətlər işlənilərək tətbiq edilir – kriptoqrafiya, steqanoqrafiya, su nişanı və s. Kriptoqrafik üsullarda informasiyanın məzmunu şifrlənərək qorunur. Bədniyyətli məxfi informasiyanın ötürülməsini görür, lakin onu deşifrə edə bilmədiyi üçün istifadə edə bilmir.

İnformasiyanın gizlədilməsini həyata keçirən steqanoqrafiya məxfi kommunikasiyada böyük rol oynayır. Steqanoqrafiya məxfi informasiyaların müxtəlif multimedia fayllarında, misal üçün təsvirlərdə, audio, video, mətn fayllarında gizlədilərək ötürülməsinə həsr edilən elm sahəsidir. Steqanoqrafiyanın istifadəsi zamanı ötürülən informasiyanın nəzərə çarpmaması və hücum edənin hədəfi aşkarlaya bilməməsi nəzərdə tutulur. Deməli, burada əsas məqsəd ötürülən informasiyanın ötürülmə faktının mövcudluğunun gizlədilməsidir. Steqanoqrafiyanın üstünlüyü elə ondan ibarətdir ki, gizlədilən məxfi informasiya bədniyyətli hücumçular üçün görünməz olur. Qəbul edən tərəfdə gizlədilmiş məxfi informasiya heç bir pozuntu və itkiyə məruz qalmadan müvəffəqiyyətlə məxfi informasiyanın daşıyıcısından, yəni steqo-fayldan çıxardılaraq istifadə edilir. Steqanoqrafik sistemlər yaradılarkən, əsasən aşağıdakı məsələlərə diqqət yetirilir:

- aşkarlanmama;

- dayanıqlılıq (müxtəlif hücum növlərinə qarşı dayanıqlı olması);,
- konteynerə gizlədiləcək məxfi informasiyanın həcmi;,
- steqo-təsvirin vizual keyfiyyəti.

Steqanoqrafiya elmi bir çox sahələrdə tətbiq edilir. Misal üçün məxfi yazışmalarda, tibbi , hərbi və s. sahələrdə istifadə olunur. Xəstəxanalarda dövr edən kliniki informasiya tibbi təsvirlərə yerləşdirilərək uzaq məsafədə fəaliyyət göstərən hər hansı həkimə ötürülə bilər. Aydın məsələdir ki, bu zaman dəqiq diaqnoz qoymaq üçün orijinal təsvirdə hətta cüzi bir dəyişiklik xəstə haqqındakı informasiyanın təhrif olunmasına gətirib çıxardar ki, bu da yol verilməz haldır.

Məxfi informasiyanı gizlətmə alqoritminin effektivliyini xarakterizə edən faktorlar əsasən aşağıdakılardan ibarətdir:

- Məxfi informasiyanın ümumi həcmi;
- Məxfi informasiya daşıyıcısı olan rəqəmsal təsvirin vizual keyfiyyət parametrləri;
- Gizlədilmiş məxfi informasiyanın həcmi.

Gizlədilmiş məxfi informasiyanın həcmi dedikdə istifadə edilən gizlədilmə alqoritmi vasitəsilə konteyner təsvirə yerləşdirilməsi mümkün olan məxfi informasiya bitlərinin ümumi miqdarı nəzərdə tutulur.

İnformasiya gizlədilmiş konteyner təsvir steqo−təsvir adlanır və gizlədilmə alqoritminin keyfiyyətini müəyyən etmək üçün hər iki təsvirin oxşarlıq dərəcəsi qəbul edilmiş üsullarla hesablanaraq yoxlanılmalıdır. Yerləşdirmə həcmi ilə vizual keyfiyyət arasında bir kompromis əldə edilməlidir. Çünki həcm artdıqca təsvirdəki pozuntular artır və təsvirin keyfiyyəti azalır. Məxfi informasiyanın gizlədilməsi sahəsində çalışan hər bir tədqiqatçı həmin kompromisi əldə etməyə cəhd edir. Alqoritmləri xarakterizə edən əsas üç parametr – yerləşdirmə həcmi, vizual keyfiyyət və dayanıqlılıq bir-biri ilə ziddiyyət təşkil etdiyinə görə kompromis əldə etmək tədqiqatçıların qarşısında duran böyük problemdir. Ona görə də, hər bir konkret halda, alqoritmin istifadə xüsusiyyətindən asılı olaraq müəyyən bir parametrin göstəricisində güzəştə getmək lazım gəlir. Dərc edilən alqoritmlərlə müqayisədə daha yüksək göstəricilərə malik yeni informasiya gizlədilmə alqoritmlərinin istifadəsi

maraqlı tərəflər arasında informasiyanın məxfi ötürülmə sistemini yaratmağa imkan verir. Bədniyyətlilər üçün ötürmə prosesi adi bir fayl mübadiləsi kimi təsəvvür edilir. Beləliklə, bu nəticəyə gəlmək olar ki, informasiya sistemlərinin təhlükəsizliyi sahəsində aparılan tədqiqatların rolu danılmazdır. Lakin, verilənlərin daha effektiv yeni gizlədilmə alqoritmlərinin işlənilməsi bu günün ən aktual məsələsi hesab edilir. Bununla da burada aparılan tədqiqatların aktuallığı təsdiq olunur.

Tədqiqat obyekti. Açıq rabitə kanalları ilə ötürülən böyük həcmli məxfi informasiyanın rəqəmsal təsvirdə steqanoqrafik üsullarla gizlədilməsi.

Tədqiqat predmeti. Böyük həcmdə məxfi informasiyanın, konteyner kimi istifadə edilən boz və rəngli təsvirlərdə nəzərə çarpacaq vizual iz qoymadan məxfi ötürülməsinə imkan verən steqanoqrafik alqoritmlərin işlənilməsi.

İşin məqsədi. Açıq rabitə kanalı vasitəsilə göndərilən məxfi informasiyanın qorunmasını təmin edən steqanoqrafik metod və alqoritmlərin araşdırılması, perspektivli steqanoqrafik metod və alqoritmlərin seçilərək müqayisəli analizlərin aparılması, yeni steqanoqrafik alqoritmlərin işlənilməsi.

Bu məqsədlə dissertasiya işində aşağıdakı məsələlər qoyulmuşdur:

- Qarşıya qoyulan problemin dünya miqyasında işlənilmə səviyyəsinin müəyyən edilməsi üçün son illərdə xarici ədəbiyyatlarda dərc edilən steqanoqrafik metod və alqoritmlərin öyrənilməsi və həll edilməsi probleminin qoyuluşu;
- Böyük həcmdə məxfi informasiyanın steqo-sistemin girişində rəqəmsal təsvirlərə gizlədilməsini və çıxışında steqo-təsvirdən çıxardılmasını təmin edən steqanoqrafik alqoritmlərin işlənilməsi;
- Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilməsi alqoritminin işlənilməsi;
- Təsvir interpolyasiyası əsasında böyük həcmdə informasiyanın gizlədilməsini təmin edən alqoritmin işlənilməsi;
- Kvorum funksiyasına əsaslanan böyük həcmdə məxfi informasiyanın gizlədilməsini təmin edən alqoritmin işlənilməsi;

- Rəngli təsvirlərdə SIFT (scale invariant feature transform- miqyasca dəyişməyən xüsusiyyət çevrilməsi) alqoritmindən istifadə edərək məxfi informasiya gizlədilmə alqoritminin işlənilməsi.

Tədqiqat metodları. Dissertasiyada təqdim edilən məsələləri həll etmək üçün məxfi informasiyanın konteyner təsvirinə sahə domeni üsulları ilə (fəza sahəsində) gizlədilməsi, təsvirlərin interpolyasiyası, ən az əhəmiyyətli bitlərin əvəzlənməsi, piksellərin fərq qiymətləri və SIFT alqoritmləri əsasında məxfi informasiyanın gizlədilməsi, steqanoqrafik analiz, pik siqnal səs-küy dərəcəsi (Peak signal noise rate (PSNR)) ilə təsvirlərin oxşarlıq dərəcəsinin ölçülməsi, histoqram üsulu, təsvirlərin struktur analizi istifadə edilmişdir.

Müdafiəyə çıxarılan əsas müddəalar:

- Son illərdə bu sahədə ölkədə və xaricdə aparılan tədqiqatlarda mövcud olan və yüksək göstəriciləri ilə fərqlənən gizlədilmə alqoritmlərinin geniş tədqiqi;
- Təsvirin vizual keyfiyyəti prioritetli informasiya gizlədilmə alqoritmi;
- İnterpolyasiya əsaslı verilənlərin gizlədilmə alqoritmi;
- Kvorum funksiyasına əsaslanan böyük həcmdə məxfi informasiyanın gizlədilməsini və vizual keyfiyyətini təmin edən steqanoqrafik alqoritm;
- SIFT alqoritmindən istifadə etməklə rəngli təsvirlərdə məxfi informasiyanın gizlədilmə alqoritmləri.

Elmi yeniliyi. Dissertasiya işində aşağıda göstərilən elmi və praktiki cəhətdən yeniliklə xarakterizə edilən nəticələr alınıb:

- Təsvirlərdə informasiyanın gizlədilməsini həyata keçirən yeni steqanoqrafik alqoritmin işlənilməsi;
- Elmi ədəbiyyatda son illərdə dərc olunan və yüksək göstəriciləri ilə fərqlənən, nümunə kimi qəbul edilən gizlədilmə metodları və alqoritmlərinin tədqiqi;
- Təsvirlərin keyfiyyəti prioritetli yüksək dayanıqlılığa malik və eyni zamanda kifayət qədər yüksək həcmli informasiya gizlədilməsini təmin edən məxfi informasiya gizlətmə alqoritminin işlənilməsi;

- Təsvirlərin interpolyasiyasına əsaslanan böyük həcmdə informasiyanı gizlətməyə malik yeni steqanoqrafik alqoritmin işlənilməsi;
- Kvorum funksiyasına əsaslanan böyük həcmli məxfi informasiyanı gizlədə bilən steqanoqrafik alqoritmin işlənilməsi;
- SIFT alqoritmi əsasında rəngli təsvirlərdə yüksək keyfiyyətə malik məxfi informasiya gizlədilmə alqoritminin işlənməsi.

Tədqiqatın nəzəri-praktiki əhəmiyyəti.

- Aparılan analiz və eksperimentlərin nəticələri yeni steqanoqrafik alqoritmlərin yaradılmasında istifadə oluna bilər.
- İşlənilən alqoritmlər məxfi yazışmalarda, tibbi təsvirlərdə, müəllif hüquqlarının qorunmasında və s. istifadə edilə bilər.
- Təklif edilən hər bir yeni steqanoqrafik alqoritm böyük həcmdə məxfi informasiyanın gizlədilməsi və açıq rabitə kanalları ilə steqo−təsvirdə təhlükəsiz ötürülməsi üçün tətbiq edilə bilər.
- Hər bir alqoritm steqo−təsvirin vizual keyfiyyəti yüksək olduğuna görə xüsusi konfidensiallıq və dayanıqlılıq tələb edilən hallarda geniş istifadə edilə bilər.
- İşlənilmiş hər bir alqoritm digər alqoritmlər ilə müqayisədə realizə zamanı sadə hesablamalar ilə həyata keçirildiyi üçün özünə daha geniş tətbiq sahəsi tapa bilər.
- İnformasiya təhlükəsizliyi ixtisasında təhsil alan tələbələr üçün faydalı informasiya mənbəyi kimi istifadə oluna bilər.

İşin approbasiyası və tətbiqi. Dissertasiyanın əsas müddəaları aşağıda adları çəkilən elmi-praktik respublika və beynəlxalq konfranslarda məruzə edilərək geniş müzakirə edilib:

- Proqram mühəndisliyinin aktual elmi-praktiki problemləri. II respublika konfransı. – Bakı, 17 may 2017.
- Технические науки в России и за рубежом: VII Международная научная конференция. – Москва: ноябрь 2017.
- İnformasiya təhlükəsizliyinin aktual problemləri. III respublika elmi-praktik seminarı. – Bakı: 8 dekabr 2017.

- Актуальные проблемы инфотелекоммуникаций в науке и образовании: VII Международная научно-техническая и научно-методическая конференция, – Санкт-Петербург,28 февраля-1 марта 2018.
- İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri. IV respublika konfransı – Bakı: 14 dekabr 2018.
- İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri. V respublika konfransı. – Bakı: 29 noyabr 2019.
- Advances in computing, communication, embedding and secure system. II International conference. – India: 2-4 september 2021. (Scopus).
- Advances in computing, communication, embedding and secure system. III International conference. – India: 18-20 may 2023. (Scopus).

Elmi nəşrlər. Dissertasiyanın əsas materialları 5 məqalədə öz əksini tapıb. Onlardan 3 məqalə Rusiya Federasiyasının AAK-ın siyahısına aid jurnallarında – 1-i Scopus beynəlxalq indeksləmə bazasında yer alan, 1-i Rusiya indeksləmə sistemi – РИНЦ-də, 1-i isə Rusiyanın AAK-da yer alan jurnalında dərc olunub. 2 məqalə isə Azərbaycanda AAK-ın tələbinə uyğun jurnallarda dərc edilib.

Dissertasiya işinin yerinə yetirildiyi təşkilatın adı. Dissertasiya işi Azərbaycan Texnologiya Universitetinin Kompüter Mühəndisliyi və Telekommunikasiya kafedrasında yerinə yetirilmişdir.

İşin strukturu və həcmi. Dissertasiya işi giriş, 4 fəsil, nəticə, 109 adda ədəbiyyat siyahısı və əlavədən ibarətdir. Dissertasiya işində 23 cədvəl və 47 şəkil vardır. İşin ümumi həcmi 169 səhifədən ibarətdir, əsas mətn 140 səhifədə şərh edilmişdir.

Dissertasiyanın işarə ilə ümumi həcmi: 179 248 işarə. Dissertasiyanın struktur bölmələrinin ayrılıqda həcmi: Titul səhifəsi – 408–işarə, mündəricat – 1454 işarə, giriş – 10361—işarə, dissertasiyanın əsas məzmunu (fəsil, paraqraf, bənd) – 165647 işarə, nəticə – 1367 -işarə, istifadə edilmiş ədəbiyyat siyahısı – 18644 işarə, əlavə – 3610 işarə, ixtisarların və şərti işarələrin siyahısı 1702 işarədir.

I FƏSİL. İNFORMASİYA TƏHLÜKƏSİZLİYİNDƏ STEQANOQRAFİYANIN ƏHƏMİYYƏTİ VƏ İSTİQAMƏTLƏRİ

Bəşəriyyətin inkişafının bütün mərhələlərində informasiyanın icazəsiz mənimsənilməsinin qarşısının alınması, yəni informasiya mühafizəsi məsələləri hər zaman aktual olub və bu gün də tam olaraq öz həllini axıra kimi tapmayıb. İnternetin və rəqəmsal kommunikasiyanın geniş yayılması açıq rabitə kanalları ilə informasiyanın ötürülməsi zamanı təhlükəsizliyinin təmin olunması problemini doğurur.

İstənilən kompüter şəbəkəsi üçün informasiya təhlükəsizliyinin təmin edilməsi vacib məsələdir və buna xüsusi diqqət ayrılmalıdır. Müxtəlif qlobal əlaqə kanalları istifadə olunan kompüter şəbəkələrində informasiya təhlükəsizliyinin təmin edilməsinin əhəmiyyəti və mürəkkəbliyi dəfələrlə artır. Bu da kompüter şəbəkələrində ötürülən məxfi informasiyaya icazəsiz müdaxilələrin mümkün olduğu hallar və çoxlu sayda istifadəçilərin olması ilə bağlıdır.

İnformasiya təhlükəsizliyinin təmin olunması probleminin vacibliyini, eyni zamanda aktuallığını əsaslandıran və təsir məqsədlərinə görə təhlükələrin üç əsas növü ayırd edilir:

- İnformasiyanın konfidensiallığının pozulmasına yönələn təhlükələr;
- İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr;
- Əlyetənliyin pozulmasına yönələn təhlükələr.

İnformasiyanın konfidensiallığının pozulmasına aid olan təhlükələr informasiya təhlükələrinin subyektiv müəyyən olunan xassəsidir. Konfidensiallıq verilən informasiyaya müraciət icazəsi olan subyektlərin siyahısına məhdudiyyət qoyulmasının zəruriliyini göstərir. Konfidensiallığın pozulmasına yönələn təhlükələr məxfi informasiyanın üstünün açılmasına yönəlib. Belə təhlükələrin reallaşması halında informasiya ona müraciət icazəsi olmayan şəxslərə məlum olur.

Bütövlük – informasiyanın təhrifsiz şəkildə mövcud olma xassəsidir. İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb

ola bilər. İnformasiyanın bütövlüyü bədniyyətli tərəfindən qəsdən və ya sistemi əhatə edən mühit tərəfindən obyektiv təsirlər nəticəsində pozula bilər.

Əlyetənlik – müəyyən vaxt ərzində tələb olunan informasiya xidmətini almaq imkanıdır. Həmçinin, əlyetənlik daxil olan sorğulara xidmət üçün onlara müraciət zəruri olduqda uyğun xidmətlərin həmişə hazır olmasıdır. Əlyetənliyin pozulmasına yönələn təhlükələr elə şəraitin yaradılmasına yönəlib ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabiliyyətini aşağı salır, ya da sistemin müəyyən resurslarına girişi bağlayır.

İstənilən kompüter şəbəkələrinin yaradılması zamanı verilənlərin ötürülməsinin təhlükəsizliyi və məxfi informasiyanın icazəsiz daxil olmalardan mühafizəsi məsələlərinə əhəmiyyətli dərəcədə diqqət yetirilməlidir [12, s. 34-36].

Perspektivli istiqamət kimi məhz rəqəmsal steqanoqrafiya informasiya təhlükəsizliyi nöqteyi-nəzərindən daha çox maraq doğurur. İnformasiya təhlükəsizliyi sahəsinin bir istiqaməti olan steqanoqrafiya məxfi informasiyanın müxtəlif növ konteyner içərisində gizlədilərək ötürülməsinə həsr olunur.

Steqanoqrafiya bir çox müxtəlif sahələrdə - tibb, hərbi iş, müəllif hüquqlarının qorunması və s. kimi sahələrdə istifadə olunur.

Steqanoqrafik sistemlərin işlənilməsində, əsas məsələ yüksək dərəcədə dayanıqlılığı təmin edilməsi və daha çox məxfi informasiya ötürülməsidir. Bu məqsəd üçün, müxtəlif alqoritmlərdən istifadə olunur.

Steqanoqrafik alqoritmlərin qiymətləndirilməsi zamanı mənfi cəhət kimi konteyner içərisinə yerləşdiriləcək məxfi informasiyanın az həcmli olması hesab edilə bilər. Konteynerə yerləşdiriləcək məxfi informasiyanın həcminin artırılması tibbi diaqnostik təsvirlərdə, arxiv sənədlərində, coğrafi xəritələrdə, hərbi işlərdə və s. steqanoqrafik alqoritmlərdən istifadə zamanı xüsusi əhəmiyyətə malikdir. Steqanoqrafiyanın bir çox mühüm konsepsiyaları 1996-cı ildə Kembricdə keçirilən informasiya gizlədilməsinə həsr olunmuş I Beynəlxalq konfransda [108, s. 553-562] və 1998–ci ildə ABŞ-ın Portland şəhərində informasiyanın gizlədilməsinə aid seminarda geniş müzakirə olunub.

Azərbaycanda da steqanoqrafiya sahəsində maraqlı işlər Qasımov V. və digərləri tərəfindən yerinə yetirilib [32, s. 1-10, 33, s. 18-23]. [32, s. 1-10]–də müasir steqanoqrafiyanın təməl konsepsiyaları müzakirə edilib. Steqanoqrafik sistemlərin etibarlılığını təmin etmək üçün LSB əsaslı metod təklif edilib [33, s. 18-23]–də mətn fayllarında məxfi informasiyanın gizlədilməsi təklif edilib. Təklif edilən metoda əsasən, geniş diapazonda simvollar arası intervalların dəyişdirilməsi ilə daha çox miqdarda bit yerləşdirmək mümkün olub. Təklif edilən metod analoji metodlarla müqayisədə steqoanalizə qarşı daha dayanıqlıdır.

1.1. Steqanoqrafiya və məxfi informasiya bitlərinin gizlədilmə metodları

Kompüter şəbəkələrində məxfi informasiyaların təhlükəsizliyinin təmin olunması üçün iki fundamental istiqamət işlənilmişdir: kriptoqrafiya və steqanoqrafiya. Birinci halda məxfi informasiya açıq əlaqə kanalları ilə şifrlənmiş formada ötürülür, öz növbəsində qarşı tərəf gizli açarın köməyi ilə məxfi informasiyanı deşifrə edir [8, s. 366-370]. Kriptoqrafik şifrləmə standartlarına AES şifrləmə standartını nümunə göstərmək olar.

Kriptoqrafiyadan fərqli olaraq, steqanoqrafiyada rabitə kanalları ilə ötürülən məxfi informasiyanın mövcudluğu faktı gizlədilir [4, s. 79-81]. Steqanoqrafiya informasiya texnologiyaları sahəsində sürətlə inkişaf edən elmi istiqamətdir. Steqanoqrafiyadan istifadə zamanı məxfi informasiya konteyner içərisində gizlədilir və konteyner kimi rəqəmsal mətn, təsvir, video, audio faylları istifadə olunur. Burada əsas məqsəd informasiyanın ötürülməsi faktını məxfi saxlamaqdır. İnformasiya təhlükəsizliyinin istiqamətlərindən biri də su nişanı (Watermarking) alqoritmləridir [24, s. 1-13, 93, s. 43-60, 98, s. 1-22, 109, s. 996-989]. Su nişanı əsasən müəllif hüquqlarını qorumaq üçün istifadə olunur. Su nişanları elektron sənədlərə yerləşdirilir. Bu zaman həm müəlliflik hüququnun qorunması məsələsi həll olunur, həm də orijinallıq qorunmuş olur. Buna nümunə kimi məhsul üzərində holoqram-maların yerləşdirilməsi, kağız pulların üzərində yerləşdirilən orijinallıq işarələrini və s. göstərə bilərik.

İnformasiya təhlükəsizliyi alqoritmlərinin müqayisəsinə nəzər yetirək. Bu müqayisə Cədvəl 1.1 - də verilib.

Cədvəl 1.1.

İnformasiya təhlükəsizliyi alqoritmlərinin müqayisəli analizi

Meyarlar/Alqoritm	**Kriptoqrafiya**	**Su nişanı**	**Steqanoqrafiya**
Tarixi	Müasir	Müasir	Qədim
Məqsəd	Məlumatların mühafizəsi	Müəlliflik hüquqlarının müdafiəsi	Məxfi kommunikasiya
Nəticə	Şifrələnmiş mətn	Su nişanlı fayl	Steqo-fayl
Daşıyıcı	Mətn və təsvir	Təsvir və ya audio	Hər hansı rəqəmsal multimediya faylı
Məxfi informasiya	Sadə mətn	Nişan	Faydalı yük
	Strukturu dəyişdirilir	Strukturunda heç bir dəyişiklik edilmir	
Açar	Vacib	İxtiyari	
Məxfi informasiyanın çıxarılması	Açar ilə Deşifrə edilərək	Açar ilə təsdiqlənir	Müəyyən steqanoqrafik alqoritm ilə reallaşdırılır
Hücum növü	Kriptoanaliz	Təsvirlərin emalı (image processing)	Steqoanaliz
Təhlükə	Deşifrə edilməsi	Silinməsi və ya dəyişdirilməsi	Aşkarlanması
Açıq rabitə kanalında görünməsi	Hər zaman görünür	Bəzən görünür	Heç vaxt görünmür

Steqanoqrafiya 3 bölməyə ayrılır:

1. Klassik steqanoqrafiya – buraya informasiya texnologiyalarından istifadə etmədən həyata keçirilən steqanoqrafik üsullar aid ola bilər;

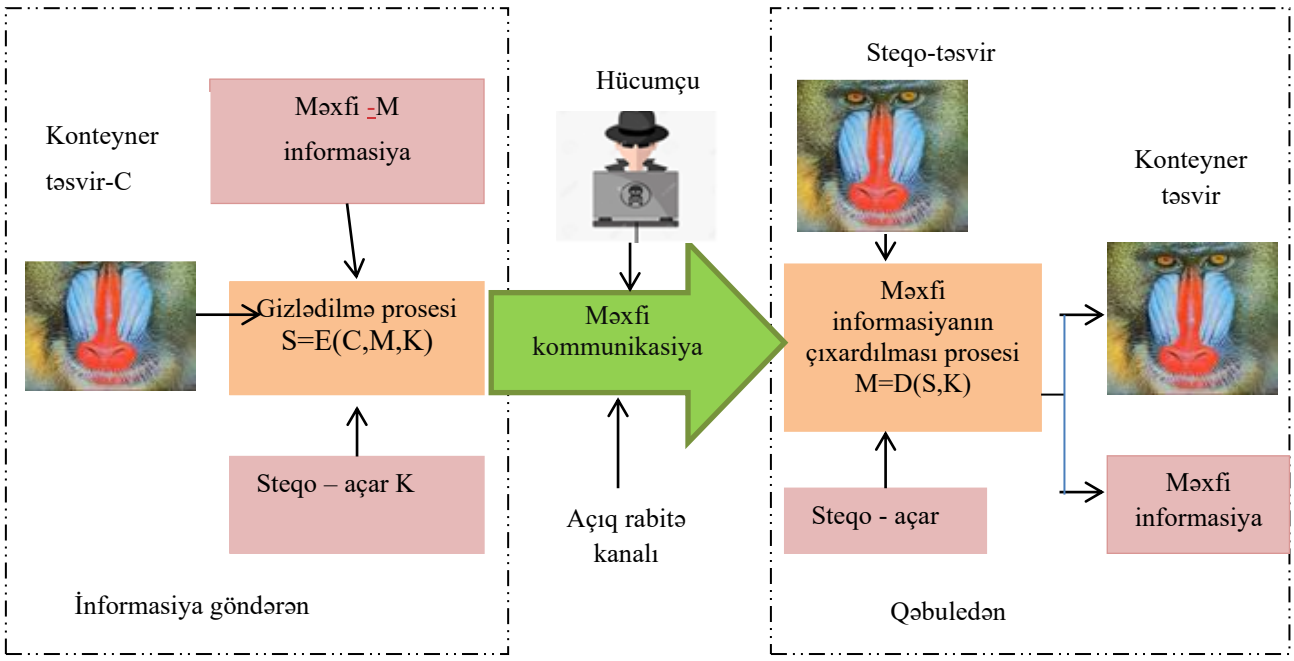
2. Kompüter steqanoqrafiyası – klassik steqanoqrafiyanın kompüter texnologiyalarına əsaslanan yeni istiqamətləri aiddir;

3. Rəqəmsal steqanoqrafiya – rəqəmsal obyektlərə məxfi informasiyaların gizlədilməsinə əsaslanan steqanoqrafiyadır.

Steqanoqrafiya sistemi müxtəlif üsulların və avadanlıqların toplusu kimi qəbul edilərək, məxfi informasiyanın açıq kommunikasiya kanalları ilə ötürülməsini təmin edir. Steqanoqrafiya proseslərinin əsas məqsədi məxfi informasiyanın konteyner daxilində görünməz qaydada ötürülməsini təmin etməkdir. Bu zaman ötürülən məxfi informasiyaların kriptoqrafiyadan fərqli olaraq [9, s. 5-7, 7, s. 29-33] şifrlənməsi nəzərdə tutulmur.

Konteynerə yerləşdirilmiş məxfi informasiya nəzərə çarpmadan görünməz halda açıq rabitə xətləri ilə ötürülür. Daha sonra məlumatın çatacağı mərhələdə məxfi informasiya bərpa olaraq steqo-konteynerdən çıxardılır. Steqanoqrafiyada məxfi informasiyanın gizlədilməsinin bir neçə metodu vardır [95, s. 54-68, 96, s. 3972-3976]. Onlar domeyin quruluşu, konteynerin tipi və məxfi informasiyanın gizlədilməsi alqoritmi ilə seçilirlər.

Steqo-sistemdə məxfi informasiya konteynerə elə gizlədilməlidir ki, onu açıq rabitə kanalında ötürən zaman göndərən və alandan başqa heç kəsin xəbəri olmasın (şəkil 1.1.1).



Şəkil 1.1.1. Steqo-sistemin struktur sxemi

Şəkil 1.1.1.-də göstərildiyi kimi steqo-sistemin işi dörd fazadan ibarətdir [76, s. 427-437]:

- Məxfi informasiyanın konteynerə gizlədilməsi;
- Dolu konteynerin açıq rabitə kanalı ilə ötürülməsi;
- Məxfi informasiyanın konteynerdən çıxarılması;
- Məxfi informasiyanın bədniyyətli tərəfindən hücuma məruz qalma ehtimalının nəzərə alınması

Şəkil 1.1.1-də konteyner C – məxfi informasiyanın müəyyən rəqəmsal mediada gizlədilməsi üçün istifadə olunan fayl, M – ötürülən məxfi informasiyadır. Məxfi informasiya mətn, təsvir, audio, video və s. tipli fayl ola bilər. E – məxfi informasiyanın konteyner təsvirə yerləşdirilmə fazası, D – məxfi informasiyanın steqo−təsvirdən çıxarılma fazası, K – konteyner təsvirə məxfi informasiya gizlədilmədən öncə şifrlənməsi üçün istifadə olunan rəqəmsal açardır. Bəzən steqo – sistemin funksionallığını sadələşdirmək məqsədilə steqo-açarsız sxemlər istifadə olunur. Kommunikasiya kanalı steqo-konteynerin ötürüldüyü rabitə kanalıdır. S – içərisində məxfi informasiya olan steqo-təsvirdir.

Yerləşdirmə fazası məxfi informasiyanın konteynerdə gizlədilməsini təmin edən prosedur və ya alqoritmdir. Ümumi olaraq bu fazanın riyazi modeli aşağıdakı kimidir.

$$E : c \times m \times k \to s \tag{1.1.1}$$

burada E– yerləşdirmə prosesidir, c– konteyner, m–məxfi informasiya, k–açar, s – steqo-konteynerdir. İnformasiyanın çıxarılması prosesi gizlədilmiş məxfi informasiyanın steqo-konteynerdən alıcısı tərəfindən çıxarılaraq bərpa edilməsidir. Bu prosedur steqo-açar vasitəsilə həyata keçirilir və aşağıdakı riyazi ifadə ilə təsvir edilir. Məxfi informasiyanın steqo-təsvirdən çıxarılması aşağıdakı kimi yazıla bilər (1.1.2) :

$$D : s \times k \to m \tag{1.1.2}$$

burada D məxfi informasiyanın çıxarılmasıdır.

Əgər steqo-sistemlərdə məxfi informasiyanın çıxarılması tələb olunmursa, bu, kor steqo-sistem hesab olunur. Hücum fazası bədniyyətli tərəfindən kommunikasiya kanalında qeyri-adi hal olduğu zaman həyata keçirilir. Bədniyyətlinin qarşısına qoyduğu məqsədlər müxtəlif formada mövcud olur.

Hücumçular passiv və aktiv ola bilər. Passiv hücumçunun məqsədi ötürülən faylın daxilində gizlədilmiş məxfi informasiyanın olmasını aşkarlamaqdır. Aktiv hücumçunun məqsədi isə gizlədilən məxfi informasiyanın deşifrlənməsi, dağıdılması və yaxud zədələnməsidir. Steqanoqrafiyaya aid bir çox xarici elmi ədəbiyyatda kifayət qədər məqalələr dərc edilib.

Onların sırasında Abbas Cheddad və digərləri tərəfindən steqanoqrafiyaya həsr olunan çox geniş icmal hazırlanmışdır [16, s. 727-752]. Bu icmalda rəqəmsal təsvirlərə həsr olunan alqoritmlər və metodlar geniş müzakirə edilib.

Mehdi Hüseyn və digərləri tərəfindən [68, s. 46-66] son illərdə sahə domeninə aid steqanoqrafik alqoritmlərın geniş icmalı verilib. Kriptoqrafiya, steqanoqrafiya və su nişanı arasındakı təməl fərqlər müzakirə edilib və müxtəlif konteyner vasitələrinə aid steqanoqrafiyanın arxitekturası təqdim edilib. İstifadə edilən mövcud gizlədilmə alqoritmlərinin müqayisəsi təsvir edilərək onların üstünlükləri və çatışmazlıqları göstərilib. Bundan əlavə ən çox istifadə edilən steqanoqrafik göstəricilərin qiymətləndirmə vahidləri, o cümlədən steqoanaliz hücumları müzakirə edilib.

Qədim steqanoqrafiya.

Steqanoqrafiya sözü yunan mənşəli olaraq stegano (gizlədilmiş) və graphia (yazı) sözlərindən yaranıb. Başqa sözlə desək, steqanoqrafiya görünməz kommunikasiyadır. Bu söz müxtəlif formalarda min illərdir ki, istifadə olunur. V əsrdə B.C. Histokisin. istifadə etdiyi klassik steqanoqrafiyada məxfi informasiya insanın qırxılmış baş dərisinə yazılır, saçın uzanması gözlənilir və bundan sonra öz təyinatı ilə lazım olan ünvana çatdırılırdı. V əsrdə yaşamış italyan riyaziyyatçısı Jerone Cardon qədim Çin məxfi yazışma üsulunu yenidən bərpa edərək istifadə edib. Bu proses kağızda müəyyən qaydada deşiklər açılmaqla həyata keçirilir. Həmin deşikli kağızlar iki nüsxə olaraq iki qrup arasında paylanılır. Daha sonra deşikli

kağızlar başqa kağız üzərinə qoyulur və göndərici öz məxfi yazısını bu deşiklər üzərində yazaraq qəbul edənə göndərir. O isə öz növbəsində çoxlu hərflərdən ibarət olan məktubu alır özündə olan deşikli kağızı həmin məktubun üzərinə yerləşdirərək məxfi məktubun mətnini üzə çıxarır. Bu üsul Cardan Grille üsulu adlanır. Bundan başqa Nazis dünya müharibəsi zamanı bir neçə steqanoqrafik üsul ixtira edib. Həmin üsullara misal kimi, görünməyən mürəkkəb şifri, mikro dot şifri, sıfır şifri (null chiper) və s. göstərmək olar. 1945- ci ildə Morze kodu ilə rəsmdə gizlədilmişdir, gizlədilən məxfi informasiya çay boyunca təsvir olunan otun üzərində şifrlənib. Uzun ot xətt, qısa ot isə nöqtə mənasını verirdi. Beləliklə məxfi informasiya alıcı tərəfindən oxunurdu.

Steqanoqrafiyanın rəqəmsal dövrü.

Rəqəmsal steqanoqrafiya öz üstünlüklərinə görə digər üsullarla müqayisədə daha geniş yayılıb. Kompüterlərin gücünün artması, İnternet və rəqəmli siqnalların emalı prosesinin inkişafı, informasiya nəzəriyyəsi və kodlama nəzəriyyəsi steqanoqrafiyanın rəqəmsal olmasına təkan verdi. Müasir məxfi informasiya gizlədilməsinin icmalı [16, s. 727-752]-də ədəbiyyatda əks edilib. Müzakirəyə çıxarılan ilk rəqəmsal steqanoqrafiya üsullarından biri Kurak və McHugh tərəfindən təklif olunub və bununla da LSB üsulunun inkişafı başlayıb. Onlar ilk dəfə olaraq məxfi informasiya bitlərini təsvirlərin ən az əhəmiyyətli bitləri ilə əvəzləyərək təsvirin vizual keyfiyyətinin aşağı düşməsini tədqiq etmişdirlər. Kibercinayətkarlar öz növbəsində bu rəqəmsal inqilabdan yararlanmağa cəhd edirlər. Abbas Cheddad və digərləri [16, s. 727-752] rəqəmsal təsvirlərin istifadə edildiyi steqanoqrafiya üsullarına aid geniş ədəbiyyat icmalı hazırlayıb. Hal-hazırda steqanoqrafiyanın inkişafını və perspektivini rəqəmsal mühitdən kənar təsəvvür etmək mümkün deyil.

Qədim yunanlar steqanoqrafiyanın ibtidai elementlərindən istifadə ediblər. Lakin bu gün istifadə olunan kompüter steqanoqrafiyası çox qısa bir zamanda sürətlə inkişaf edərək bir çox istiqamətlərə bölünüb. Məxfi informasiya müxtəlif multimedia vasitələrində gizlədilir. Konteynerdə istifadə edilməyən sahələr məxfi informasiyaların yerləşdirilməsi üçün əlverişli hesab olunur.

Həmin informasiya üçüncü şəxslər üçün görünməz olduqda kommunikasiya uğurlu hesab olunur. Beləliklə, məxfi informasiya həmin sahələrə yerləşdirilir və informasiyanı qəbul edən şəxsə göndərilir. İnformasiya konteynerin istənilən hissəsində yerləşdirilə bilər, lakin bəzi sahələr informasiya gizlədilməsi üçün daha əlverişlidir. Konteynerdən (konteyner faylının növündən) asılı olaraq müxtəlif tip steqanoqrafiya metodları məlumdur [22, s. 42-51, 29, s. 489-495, 46, s. 39-44, 51, s. 2017-2028, 52, s. 3236-3246, 97, s. 1129-1143]:

1. Mətn steqanoqrafiyası: bu yanaşmada gizlədilən informasiya mətn sənədinə yerləşdirilir;
2. Təsvir steqanoqrafiyası: məxfi informasiya təsvir piksellərində gizlədilir. Çünki orada böyük miqdarda məxfi informasiya gizlətmək üçün əlverişli informasiya sahələri var;
3. Audio steqanoqrafiyası: məxfi informasiya səs faylında gizlədilir;
4. Video steqanoqrafiyası: məxfi informasiya mp4, mpeg, avi sənədlərində yerləşdirilir;
5. Şəbəkə və yaxud protokol steqanoqrafiyası: bu zaman məxfi informasiya TCP/IP, UDP, IP və s. protokollarda yerləşdirilir;

Müxtəlif ölkələrdə rəqəmli steqanoqrafiyaya aid diqqətəlayiq işlər görülüb. Abbas Cheddadın [16, s. 727-752] məqaləsi geniş analitik iş olaraq informasiyanın gizlədilməsi sahəsində çalışan mütəxəssislərin diqqətini cəlb etmişdir. Həmin işdə 2009-cu ilə kimi hazırlanan steqanoqrafik üsullar dərindən təhlil edilərək sistemləşdirilib. Bu sistemləşdirməyə əsaslanaraq obyekt yönümlü gizlətmə mexanizmlərinə aid müəyyən tövsiyələr edilib.

Abbas Cheddadın [16, s. 727-752] təsnifatlaşdırmasına əsasən göstərilən üsulların steqanoqrafiya, su nişanı, kriptoqrafiya, o cümlədən müasir və geniş yayılmış informasiya gizlətmə üsullarından olan sahə domeni, transform domen, adaptiv steqanoqrafiya və digərlərinin müqayisəsi təqdim edilib. Bütün bu müqayisələr illüstrativ materiallarda geniş izah edilib. Bu üsulların bütün aspektləri müzakirə edilib. Ümumiyyətlə, bu iş informasiya gizlədilmə üsulları sahəsində ən

uğurlu icmal hesab edilə bilər. Digər daha geniş işlənilmiş icmal Mehdi Hüseyn və digərləri [68, s. 46-66] tərəfindən aparılıb. Bu icmalda steqanoqrafiyanın son 10 ildəki vəziyyəti araşdırılıb. İcmaldakı tənqidi fikirlərə görə Cheddad və başqaları öz məqalələrini 2009-cu ildə dərc etdirdikləri üçün son 10 ilin nailiyyətlərini əks etdirmir. Eyni zamanda Cheddad və digərlərinin təsvir steqanoqrafiyasını təsnifləşdirməsi sahə domeni, transform və adaptiv domen alqoritmləri ilə məhdudlaşdırılır. Buna görə də, Mehdi Hüseyn sahə domeni alqoritmi sahəsində yeni, daha geniş icmal hazırlayıb. Bu icmal Abbas Cheddad və digərlərinin icmalı ilə müqayisədə məxfi informasiya gizlədilmə domeninə, məxfi informasiyanın şifrlənmə növünə və təsvirlərin formatına görə fərqlənir. Ədəbiyyatda təklif olunan üsullar özünəməxsus güclü və zəif xüsusiyyətlərə malik olur və bunlar tətbiq məqsədindən asılı olaraq dəyişir. Dərc olunan məqalələrdə [43, s. 465-470, 46, s. 39-44, 54, s. 137-144, 82, s. 1-9] xüsusi diqqət gizlədilən məlumatın həcminə yönləndirilsə də, son illərin tədqiqatları ilə tanışlıq göstərir ki, tədqiqatlar daha çox yüksək təhlükəsizlik səviyyəsinə malik olan alqoritmlərin işlənilməsinə həsr olunur. Hər bir istifadə olunan üsul özünəməxsus xüsusiyyətə malikdir. Misal üçün ən az əhəmiyyətli bitlər (LSB) əsaslı sahə domeni alqoritmlərində böyük miqdarda informasiya gizlətmək mümkündür [29, s. 489-495, 38, s. 1-11, 65, s. 1-8, 73, s. 14867-14893, 90, s. 1-25]. Bu üsulda informasiyanın yerləşdirilməsi çox asanlıqla baş verir. Bundan başqa tətbiqi sadədir və digər müxtəlif üsullarla kombinə etmək olur. Eyni zamanda, qeyd etmək lazımdır ki, yerləşdirilən məxfi informasiyanın həcmi artdıqca təsvirin daha çox vizual pozulması müşahidə olunur. Piksellərin fərq qiyməti- PFQ (Pixel value difference PVD) üsulu [53, s. 94-103, 102, s. 1613-1626] isə daha dayanıqlı olması ilə xarakterizə edilir.

Steqanoqrafiyanın tətbiqləri.

Steqanoqrafiya hal-hazırda aşağıda göstərilən sahələrdə istifadə edilir:

- Məxfi kommunikasiya və məxfi informasiyanın gizlədilməsi;
- E-kommersiya;
- Saxlanılan verilənlərin dəyişdirilməkdən qorunması;

- Media;
- Verilənlər bazası sistemləri və s.

Təsvir steqanoqrafiyası.

Son illərdə dünya əhalisinin böyük hissəsi bir-biri ilə e-mail, sosial şəbəkələr və s. vasitələrlə əlaqə qururlar. Bu əlaqələrin əksər hissəsi təsvirlərlə müşahidə olunur. Bu isə öz növbəsində təsvir steqanoqrafiyasının sürətlə inkişafına və müvafiq olaraq istifadəsinə səbəb olur. Son zamanlar daha çox bilinən və geniş yayılmış steqanoqrafiya yeni yaradılmış üsullarla səciyyələnir. Təsvir steqanoqrafiyası məxfi informasiyanın rəqəmsal təsvirdə gizlədilməsini təmin edən informasiya texnologiyaları elminin müasir sahəsidir [2, s. 98-104, 52, s. 3236-3246, 72, s. 647-654, 91, s. 2995-3004]. Öz üstünlüklərinə görə təsvir steqanoqrafiyası digər üsullarla müqayisədə daha geniş yayılıb [13]. Təsvir steqanoqrafiyasında informasiya yerləşdirilməsi prosesində rəqəmsal təsvirlər konteyner kimi istifadə edilir və o gizlədilmiş informasiyanın daşıyıcısı rolunu oynayır. Konteyner çox dəqiq seçilməlidir, çünki steqo-sistemin effektivliyi təsvirin xarakteristikalarından bilavasitə asılıdır [16, s. 727-752]. Rəqəmsal təsvirlərin konteyner kimi istifadə edilməsinin xüsusi üsulları işlənilib [22, s. 42-51, 53, s. 94-103].

Bu məqsəd üçün müxtəlif təsvirlərin statistik xarakteristikaları müqayisə olunur və o nümunələr seçilir ki, steqo-təsvirin daha yüksək keyfiyyətini, daha böyük həcmdə məxfi informasiya gizlədilməsini, vizual keyfiyyətin daha yüksək göstəricilərini, yüksək dayanıqlılığı təmin etsin. Əgər üçüncü tərəfin (attacker) ötürülən informasiyadan məlumatı yoxdursa və gizlədilmiş informasiyanın mövcudluğundan şübhələnmirsə, kommunikasiya sistemi yüksək keyfiyyətli kimi qiymətləndirilə bilər. Bununla yanaşı müxtəlif konteynerlərin keyfiyyətinin əvvəlcədən yüksəldilmə texnologiyaları işlənilib və istifadə edilir. Bunlardan biri də təsvirin interpolyasiya edilməsi metodudur.

Təsvir steqanoqrafiyası informasiyanı rəqəmsal təsvirdə gizlətdikdən sonra onun steqanoqrafik təsvirə çevrilməsinə səbəb olur. Daha sonra steqo-təsvir açıq rabitə kanalı ilə ötürülərək informasiyanın təyinat nöqtəsinə çatdırılır. Məlumatın

gizlədilməsi alqoritmləri konteynerin yenidən bərpa olunması və yaxud da konteynerin pozulması halı ola bilər. 1-ci halda istifadə olunan alqoritmin növündən asılı olaraq məxfi informasiyanı qəbul edən məxfi informasiyanı steqo-açarla və yaxud açarsız steqo-təsvirdən çıxardıqdan sonra konteyner təsvir yenidən əvvəlki vəziyyətini alır. Konteynerin pozulması halında isə məxfi informasiyanı steqo−təsvirdən çıxardıqdan sonra konteyner təsvir pozulmuş olur, yəni yararsız vəziyyət alır. Adətən konteynerin yenidən bərpa olunması mümkün olan alqoritmləri geniş istifadə olunur [17, s. 1-24, 63, s. 102-111, 64, s. 499-511, 108, s. 553-562].

[16, s. 727-752, 83, s. 95-113]-də geniş yayılmış rəqəmsal təsvirlərin istifadə edildiyi steqanoqrafiya üsullarının icmalı verilib, iki kateqoriyaya aid olan mühüm təsvirlərin istifadə edildiyi formatlar müzakirə olunub. Bir çox hallarda təsvir steqanoqrafiyasında məxfi informasiya gizlədilməzdən əvvəl örtük təsvir müəyyən metodlarla emal edilir. Bunlardan biri də son zamanlar istifadə edilən miqyasca dəyişməyən xüsusiyyət çevrilməsi (scale invariant feature transform SIFT) alqoritmləridir.

SIFT alqoritmi və onun tətbiq sahələri

İnsan öz görmə qabiliyyəti ilə təsvirləri müqayisə edərək onların üzərində olan obyektləri müəyyən edə bilir. Lakin kompüter üçün təsvirlərdə mövcud olan obyektlər heç bir əhəmiyyət kəsb etməyən verilənlər yığımıdır. İnsanın seçmə və müəyyənetmə qabiliyyətini maşınlara aşılamaq üçün müxtəlif üsullar və vasitələr tətbiq edilir.

Təsvirlərin hər bir pikseli üçün müəyyən bir funksiyanın qiyməti hesablanır və həmin qiymətlərin əsasında təsvirə müəyyən bir xarakteristika müəyyən edilir. Belə olduqda təsvirlərin müqayisəsi bu xarakteristikaların müqayisəsinə yönəlir. Lakin bu zaman təsvirdəki xarakteristikaya daha çox nüfuz edən piksellərin xüsusi açar piksellərini seçərək yalnız onları müqayisəsində istifadə edilir. Bu zaman o piksel xüsusi təsvir edilmiş obyekt hesab edilir. Xüsusi əhəmiyyət kəsb edən açar pikselləri təsvirdən seçib üzə çıxaran vasitə detektor adlanır. Detektor təsvirin emalında baş verən hər bir dəyişmə zamanı invariantlığı, yəni xüsusi piksellərin tapılmasını təmin

etməlidir (hər bir təsvirin dəyişmə variantında). Burada deskriptor anlayışını izah etmək yerinə düşər. Deskriptorlar təsvirlərdə mövcud olan piksellər içərisindən əsas əhəmiyyət kəsb edən açar pikseli digər piksellərdən fərqləndirmək (ayırmaq) üçün istifadə edilən identifikatordur. Çünki detektorun tətbiqi zamanı açar piksellərin yalnız koordinatlarını tapmaq mümkün olur. O koordinatlar isə hər bir təsvirdə fərqlidir. Bu zaman deskriptorlar istifadə edilir. Deskriptor və ya açar piksellərin identifikatoru, açarı yerdə qalan piksellər kütləsindən seçə bilir. Bu zaman təbii ki, dəyişmələrin invariantlığı da təmin edilməlidir.

Təsvirlərin identifikasiyası kompüter görməsinin müxtəlif sahələrində ən mürəkkəb məsələlərdən biridir. Bunun üçün SIFT alqoritminin müxtəlif tətbiqləri işlənilərək istifadə edilir. Alqoritm kompüter görməsində istifadə edilən təsvirlərin lokal xüsusiyyətlərinin aşkarlanmasında və təsvir edilməsində istifadə edilir.

Eyni zamanda, çoxsaylı təsvir cütlükləri üçün yalan və həqiqi müsbət əmsallar hesablanır və identifikasiyada istifadə edilərək müqayisənin dəqiqliyini artırır. Digər təklif edilən məqalədə [34, s. 349-353] açar nöqtələrinin uyğunluğunu ölçmək üçün Evklid məsafəsini istifadə etməklə SIFT alqoritmitətbiq edilir. Nəticələr göstərir ki, SIFT alqoritmi döndərilmə, miqyaslanma halları üçün invariantdır. SIFT funksiyaları isə perspektivin, işıqlanmanın və küylərin dəyişməsi müqayisə edilən dərəcədə çox güclü dayanıqlılığa malikdir. [64, s. 499-511]-də təsvirin əlamətlərinin müqayisəetmə vaxtının azaldılması və SIFT alqoritminin istifadəsi zamanı yaranan səhvlərin minimuma endirilməsinə həsr edilib. [27, s. 454-460]-də isə SIFT əsaslı təsvirlərin tez qeydə alma alqoritmi təklif edilib. Alqoritm yüksək aydınlıq dərəcəsinə malik təsvirlərdən əlamətlər nöqtələrini seçir. Seçilmiş əlamət nöqtələri SIFT alqoritmi ilə çıxarıldıqdan sonra ilkin təsvir ilə birləşdirilir. Son zamanlar informasiya təhlükəsizliyi sahəsində SIFT alqoritmləri tətbiq edilir. Sənədlərdə saxtalaşdırmaların aşkarlanmasına həsr edilən uğurlu alqoritmlər işlənilib. Nümunə kimi nüsxələmə-yerdəyişmə saxtalaşması (copy-move forgery) alqoritmini göstərmək olar. Bu metod mətndəki fraqmentləri – sözləri, cümlələri nüsxələyərək orijinal sənəddə əvəzləmə ilə yerinə yetirilən saxtalaşmaları üzə çıxarır. Ona görə də, kriminalistika və məhkəmə

ekspertizasında istifadə edilir. [50, s. 29-39]-da tam qruplaşdırılmış təməlin qurulmasına əsaslanan informasiya gizlədilmə alqoritmi təklif edilib.

1.2. Steqanoqrafiya sahəsində elmi tədqiqatların müasir vəziyyətinin analizi

Steqanoqrafik üsullar əsasən aşağıda sadalanan kateqoriyalara bölünür:

- *Konteyner seçimi steqanoqrafiyası;*
- *Konteynerin generasiya edilməsi;*
- *Konteynerin modifikasiya edilməsi.*

Konteyner seçimi steqanoqrafiyası.

Steqanoqrafiyada informasiya gizlədilməsi üçün konteyner təsvirlərinin seçilməsi mümkündür [36, s. 297-316, 44, s. 36-39]. Təsvir steqanoqrafiyasında məxfi informasiyanı göndərən təsvirlər bazasından əlverişli konteyner təsvirini seçə bilər. Daha sonra məxfi informasiyanı həmin təsvirə yerləşdirməlidir. Konteyner kimi istifadə edilən təsvirin düzgün seçilməsinin steqanoqrafik sistemin effektivliyinə təsiri var. Çünki steqo-sistemin dayanıqlılığı konteynerdən asılı olur. Konteynerin ölçüləri bilavasitə steqanoqrafik məlumat kanalının məlumat ötürülmə qabiliyyətinə təsir edir [84, s. 19-24].

Hansi Subhedear [73, s. 14867-14893] öz məqaləsində məxfi informasiyanın düzgün seçilmiş konteyner təsvirinə yerləşdirilməsi, sistemin göstəricilərinin yüksəldilməsi və bunun nəticəsi kimi daha yüksək təhlükəsizlik sisteminin alınmasını yazmışdır.

Bu alqoritm təsvirlərin teksturasının oxşarlıq effektindən istifadə edir. Bu zaman konteyner təsvirinin bəzi blokları məxfi informasiyanın oxşar blokları ilə uyğunlaşır.

Məxfi informasiyanın və konteyner təsvirlərinin bloklarının müqayisəsinin nəticələri məxfi informasiyanın yerləşdirilməsi üçün daha əlverişli və yararlı təsvirin seçilməsinə imkan verir. Bundan başqa təsvir bloklarının və onların ətrafındakı statistik xüsusiyyətlərin istifadə olunduğu alqoritmlərin analizi verilib. Bu da alqoritmin təkmilləşdirilməsi ilə nəticələnib.

Sadkhan [85, s. 258-264] məlumat göndərənə təsvirlər bazasından daha əlverişli konteyner təsviri seçmək üçün imkan yaradan yeni bir sistem təklif edib. Bu üsul seçilən təsvirin statistik xarakteristikalarına əsaslanır. Təsvirin verilənlər bazasından götürülməsindən sonra istifadə edilən sistem təsvirin bəzi problemlərini müəyyənləşdirir. Bunun əsasında düzgün seçim barəsində qərar qəbul edilir. Steqanoqrafik agent sistemini istifadə edərkən daha yüksək dispersiya, entropiya və konstanta malik təsvirlər seçilir.

Konteynerin generasiya edilməsi.

Konteynerin generasiya edilməsi digər steqanoqrafiya üsullarından konteynerin mövcudluğunun tələb olunmaması ilə fərqlənir və konteyner təsvir steqo-sistemin özü tərəfindən generasiya edilir. Konteynerin generasiya edilməsinə aid müxtəlif generasiya üsulları təklif olunub [38, s. 1-11]. Həmin ədəbiyyatlarda konteyner generasiyasının nəzəriyyəsinin və alqoritminin geniş və sistemləşdirilmiş izahı verilib. Bununla yanaşı effektiv və steqo-hücumlara qarşı dayanıqlı generasiya üsulları təklif edilib. Ritchey [81, s. 549], konteyner generasiya üsullarının geniş icmalını aparıb. Konteyner generasiya üsulları yüksək dərəcədə steqoanalitik hücumlara dözümlü olurlar. Generasiya edilmiş konteyner ona daxil edilmiş informasiya bitləri çıxarıldıqdan sonra yenidən əvvəlki vəziyyətini ala bilməlidir.

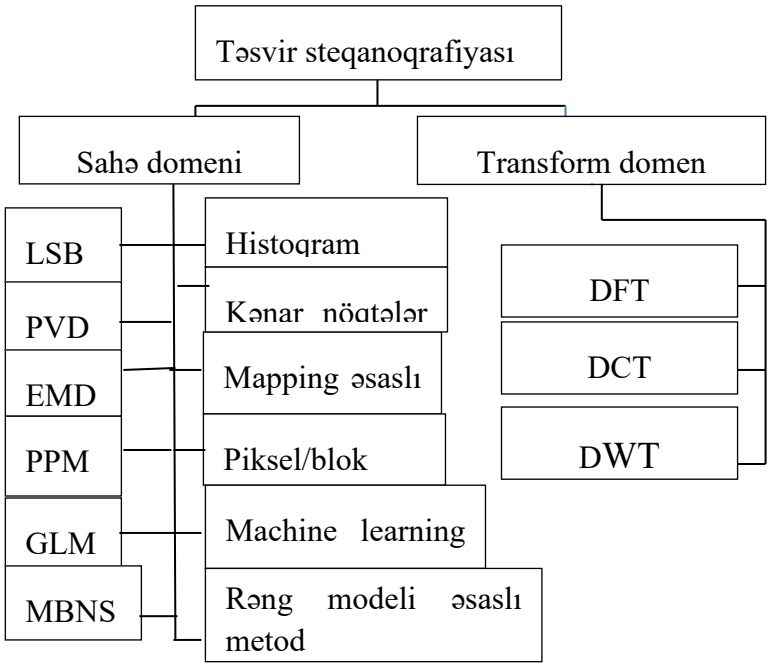
Konteynerin modifikasiya edilməsi.

Bu üsullar müvafiq olaraq göndərici konteyner təsvirinin piksellərini modifikasiya edərək məxfi informasiyanın bitlərini yerləşdirir, yəni konteyneri modifikasiya edir. Hər bir təsnifləşdirilmədə dinamik və adaptiv üsullar mövcuddur. Dinamik üsul informasiyanın bitlərindən asılıdır, adaptiv üsullar isə təsvirin statistik xüsusiyyətlərinə əsaslanır [69, s. 12-17]. Konteynerin həcmi və steqo−təsvirin vizual keyfiyyəti rəqəmsal təsvirin formatından asılıdır [68, s. 46-66]. Konteynerin seçilməsində aşağıdakı təsvir formatları istifadə edilir:

- BMP (Bit Map Point) – *Bit xəritəsi nöqtəsi;*
- TIFF (Targed Image File Format) – *hədəflənmiş şəkil fayl formatı;*
- PNG (Portable Network Graphics) – *portativ şəbəkə qrafikası;*

- JPEG (Joint Photographic Experts Group) – *birgə fotoqrafiya ekspertləri qrupu;*
- GİF (Graphical Data Interchange Format) *qrafik məlumat mübadiləsi formatı.*

Məxfi informasiya gizlədilmə alqoritmlərin hər biri öz növbəsində Mehdi Hüseynin təsnifatına [68, s. 46-66] görə bir neçə alt növə bölünür (Şəkil 1.2.1).



Şəkil 1.2.1 Təsvir steqanoqrafiyasının təsnifatı sxemi

Sahə domeni (Spatial domain) alqoritmi.

Mehdi Huseyn və digərlərinin təsnifatına uyğun olaraq [68, s. 46-66] sahə domeni üsullarına aşağıdakılar aid edilir:

- Least significant bits (LSB) – Ən az əhəmiyyətli bitlər (AƏB);
- Pixel value difference (PVD) – Piksellərin fərq qiyməti (PFQ);
- Exploiting modification direction (EMD) – Modifikasiya istiqamətindən istifadə (Mİİ);
- Multi-base notation system (MBNS) – Çox əsaslı işarələmə sistemi;
- Pixel pair matching (PPM) – Piksel cüt uyğunluğu (PCU);
- Gray level modification (GLM) – Boz səviyyə modifikasiyası (BSM);
- Histogram based methods – Histoqram əsaslı üsullar;

- Edge-based methods – Tillər əsaslı üsullar;
- Pixel/block indicator base methods – Piksel/blok göstərici əsas üsulları;
- Color model-based methods – Rəng modelinə əsaslanan metodlar;
- Machine learning-based methods – Maşın təliminə əsaslanan metodlar.

Sahə domeni alqoritmləri konteyner təsvirdə məxfi informasiya gizlədilmə prosesinə görə öz sadəliyi ilə fərqlənir [79, s. 134-148, 92, s.52-54]. Eyni zamanda yerləşdirilən məxfi informasiyanın həcmi daha çoxdur. Lakin bununla yanaşı, böyük həcmdə məxfi informasiyanın konteyner təsvirinə gizlədilməsindən sonra steqo−təsvirin vizual keyfiyyəti konteynerlə müqayisədə pozulur və ən mühüm çatışmazlığı steqo-hücumlara qarşı dayanıqsız olmasıdır. Steqo−təsvir ilə konteyner arasındakı pozuntunun miqdarı istifadə edilən məxfi informasiya gizlədilmə alqoritminin keyfiyyətini müəyyən edir.

Bu üsulla məxfi informasiyanın bitləri konteyner təsvirin bilavasitə müvafiq pikselinə və yaxud onunla əlaqəli piksellərə yerləşdirilir. Sahə domeni alqoritmlərinin bir nümunəsi də LSB alqoritmidir. LSB alqoritmi konteyner təsvirin hər bir pikselinin 7-ci və 8-ci biti məxfi informasiya biti ilə əvəzlənir. Bir çox mövcud yanaşmalarda hər bir pikselin LSB-nə məxfi informasiyanın bitlərini müəyyən ardıcıllıqla yerləşdirmək əvəzinə psevdo təsadüfi generatorundan istifadə edərək LSB bitlərinin miqdarı seçilir və məxfi informasiya bitləri ilə əvəz edilir. Bu zaman məxfi informasiya bitlərinin yerləşdirilməsi daha effektiv olur. Belə ki, məxfi informasiya bitləri konteyner təsvirinin xaotik seçilmiş piksellərində gizlədildiyindən konteyner təsvirin hamar zonasında nəzərə çarpan dərəcədə pozuntular baş vermir [30, s. 91-95, 55, s. 458-463].

Transform domeni metodu.

Transform domen metodları isə [19, s. 1-9, 61, s. 855-862, 70, s. 355-358] uyğun olaraq aşağıdakı kimi təsnif edilir:

1. Discrete fourier transform technique (DFT) – Diskret furye çevrilmə texnikası;
2. Discrete cosine transform techniques (DKT) – Diskret kosinus çevrilmə texnikası;

3. Discrete wavelet transform method (DVT) – Diskret wavelet çevrilmə metodu;
4. Loss less və ya reversible DCT– Az itki və ya geri qaytarıla bilən DCT;
5. Embedding in coefficient bits – Əmsal bitlərinə yerləşdirmə.

Transform domeyin metodu ilə məxfi informasiya gizlədilməsinin üstün cəhəti steqo-sistemin steqo-hücumlara qarşı dayanıqlı olması hesab olunur. Çatışmazlığı isə alqoritmlərinin daha mürəkkəb olması, tutumunun isə daha az olmasıdır.

Sahə domeni (Spatial Domain) alqoritmləri böyük üstünlüklərə malik olsa da gizlədilən məxfi informasiya miqdarının çox olması təsvirdə pozuntulara səbəb olur. Bu da öz növbəsində vizual keyfiyyətə mənfi təsir edir. Transform domeni alqoritmləri bu cəhətdən daha üstündür. Transform domeni alqoritmləri geniş istifadə edilən informasiya gizlətmə alqoritmlərindən biridir [15, s. 582]. Bu alqoritmlərdə ilk addım ən çox istifadə edilən Furye çevrilməsi (Fourier transforms (FT)), Diskret kosinus çevrilməsi (Discrete cosine transform (DCT)) və ya Diskret veyvelet çevrilməsi (Discrete wavelet transforms (DWT)) vasitəsilə konteyner təsvir transform domen əmsallarına çevrilir. Adı çəkilən çevrilmələr həm təsvirin ayrı-ayrı hissələrinə, həm də bütün təsvirə tətbiq edilə bilər. Daha sonra yuxarıda sadalanan çevrilmələr ilə generasiya olunan verilənlərin müxtəlif xarakteristikalarına uyğun olaraq məxfi informasiyanın bitləri transform domeninin əmsallarına yerləşdirilir. Yerləşdirmə prosesi başa çatdıqdan sonra məxfi bitlər yerləşdirilən əmsallar yenidən sahə domeninə çevrilir. Beləliklə, yerləşdirmə proseduru sona çatmış olur.

Transform domeni alqoritmlərinin üstün cəhəti steqoanaliz alqoritmləri və təsvir emalı əməliyyatlarına qarşı yüksək dayanıqlı olmasıdır. Bununla yanaşı, bu tip alqoritmlər mürəkkəb hesablamalar tələb etdiyinə görə çox böyük zaman sərfi hesabına baş tutur.

Adaptiv yerləşdirmə steqanoqrafiyası

Adaptiv yerləşdirmə steqanoqrafiyası sahə domeni və transform domeni alqoritmlərinin xüsusi bir halıdır. Eyni zamanda statistik məlumatların yerləşdirilməsi, maskalama və yaxud model əsaslı kimi də tanınır. Statistik məlumatlar təsvirin əvvəlcədən müəyyən olunan hissəsində dəyişiklik etməyə imkan

verir. Bu üsul konteyner təsvirindən asılı olaraq piksellərin ixtiyari adaptiv seçilməsi ilə xarakterizə edilir. Bununla da daha çox uyğun gələn piksellər seçilir. Sonra hamar sahələrdə eyni rəngli sahələri seçməyə imkan verir. Bütün bunlar adaptiv steqanoqrafiya vasitəsilə elə təsvirlər seçməyə imkan verir ki, həmin təsvirlərdə rənglərin müxtəlifliyini nəzərə almaq mümkün olsun.

Ədəbiyyatda müxtəlif növ təsvir steqanoqrafiyası alqoritmləri təklif olunub. Bunların böyük əksəriyyəti məxfi informasiya gizlədilməsinə nail olmaq üçün fərqli yanaşmalardan istifadə edir. Əgər model yanaşma əsaslı alqoritmləri təsnifləşdirmək qarşıya qoyulursa, gərək həmin üsullar onların tətbiq sahələrinə görə təhlil edilsin. Lakin onların hamısını dəqiq təsnif etmək mümkün deyil. Mehdi Hüseynin təsnifatında [68, s. 46-66] sadalanan üsulların əsas hədəfləri göstərilib.

[68, s. 46-66] ədəbiyyatı əsas götürərək 1-ci növbədə onları yerləşdirmə domeninə görə qiymətləndirmək olar. Əvvəl qeyd edildiyi kimi, adaptiv steqanoqrafiya hər iki metodun, yəni sahə domeni metodu və transform domeyin metodunun bir növü hesab oluna bilər. Çünki adaptiv steqanoqrafiyada hər iki üsuldan istifadə edilir. Digər təsnifat təsvirlərin kodlaşdırılmış formatları üçün bilavasitə işlənilib. Belə təsnifləşdirməyə, sıxlaşdırılmış JPEG və şifrlənmiş təsvir məlumatını (AES) misal göstərə bilərik. Ədəbiyyatda məxfi informasiyanın formatına və növünə istiqamətlənən alqoritmlər təklif olunur. Bu məsələlər və sahə domenində məxfi informasiya bir başqa konteyner təsvirin pikselinə yerləşdirilməsi [68, s. 46-66] –da göstərilib.

Bunun əksinə olaraq, transform domen üsullarında məxfi informasiyanı gizlətmək üçün əvvəl konteyner təsvirin pikselləri digər formaya çevrilir, daha sonra məxfi informasiya gizlədilir. Misal üçün DCT üsulu istifadə edilərkən əvvəl konteyner pikselləri istifadə edilərək başqa formaya çevirilir, daha sonra məxfi informasiya DCT bloklarının müxtəlif piksellərinə gizlədilir. [68, s. 46-66] –da işlənilib istifadə olunan məlum steqanoqrafik üsulların müqayisəsi yeni üsullar yaratmağa təkan verir.

Sahə domeni transform domenə görə daha geniş istifadə edilir. Çünki istifadəsi daha asan hesab olunur. Lakin bununla yanaşı qeyd olunmalıdır ki, dayanıqlılığı aşağıdır.

Ən az əhəmiyyətli bitlərin əvəzlənməsi üsulu

Məxfi informasiyanın təsvirdə yerləşdirilməsinə aid bir neçə üsul vardır. Məxfi informasiya ardıcıl və ya təsadüfi yollarla seçilmiş təsvirin piksellərinə gizlədilə bilər. Adətən küylü təsvir pikselləri məlumat yerləşdirilməsi üçün ideal sahələr hesab edilir. Çünki təsvirin küylü hissəsində olan piksellərin çoxu müxtəlif rənglərə malikdir. Buna görə də, təsvirdəki pozuntular təsvirin görünüşünə ciddi ziyan vurmur və insanın görmə sistemi tərəfindən görünməz olur. Ən az əhəmiyyətli bit üsulunun tətbiqi rəqəmsal təsvirin ən az əhəmiyyətli bitlərinin məxfi informasiya bitləri ilə əvəzlənməsinə əsaslanır. Ən az əhəmiyyətli bit üsulunun müxtəlif alqoritmlər ilə birlikdə istifadəsi də mümkündür ki, bu da daha effektiv nəticə almağa gətirib çıxarır.

Ən az əhəmiyyətli bit üsulunun tətbiqi zamanı dəyişikliklərin olacağı bitləri müxtəlif üsullarla müəyyən etmək mümkündür. Təsvirlər müxtəlif formatda ola bilərlər. Bu da konteynerin tutumuna təsir göstərən vacib amillərdən biridir.

Ən az əhəmiyyətli bit əvəzləməsinin təməl konsepsiyasına uyğun olaraq bit ardıcıllığındakı sonuncu bitlər ən az qiymətli bitlərdir. Əgər həmin bitlər məxfi informasiyanın bitləri ilə əvəzlənərsə, steqo−təsvirdəki pozuntular çox kiçik olar.

Ümumiyyətlə, 8 bitin hamısını əvəz etməyə imkan var. Lakin əvəzləmə üçün 2 bit istifadə olunur. Əgər təsvirə gizlədilən bitin qiyməti 1-ə bərabər olarsa, bu zaman konteyner təsvirin pikselinin qiyməti ya bir vahid azalır və yaxud bir vahid artır (+/-1). Əgər gizlədilən bitin qiyməti 0 olarsa, bu zaman konteyner təsvirin pikselinin qiyməti dəyişməz qalır.

Ən az əhəmiyyətli bitə əsaslanan steqanoqrafiya informasiya gizlədilmə üsulu rəqəmsal steqanoqrafiyanın təməl istiqamətlərindən biri kimi tanınır.

Piksellərin fərqinə əsaslanan yerləşdirmə metodu

Piksellərin qiymətinin fərqinə əsaslanan metodlar LSB-ə əsaslanan metodlarla müqayisədə daha çox informasiya gizlətməyə qadirdirlər [95, s. 54-68]. LSB

metodunda yerləşdiriləcək məxfi informasiya həcmi maksimum olmur, çünki həcm artarsa, təsvirin vizual keyfiyyəti aşağı düşər. Bu çatışmazlığı aradan qaldırmaq üçün Wu və digərləri [100, s. 611-615] piksellərin qiymətlərinin fərqinə əsaslanan steqanoqrafik yanaşma təklif ediblər. İki piksel arasındakı qiymətlərin fərqi yerləşdiriləcək məxfi informasiya bitlərinin sayını müəyyən etməyə imkan verir. Başqa sözlə desək, bu alqoritm təsvir pozuntularının miqyasının azalmasına səbəb olur. Bu üsulda örtük təsviri iki kəsişməyən ardıcıl piksel bloklarına ziq-zaq formada bölünür. Daha sonra hər bir blok daxilində iki qonşu piksel arasındakı fərq qiyməti hesablanır. Həmin fərqin əsasında yerləşdiriləcək bitlərin sayı müəyyən edilir. Nəticədə fərqin qiymətinə uyğun sayda məxfi informasiya bitləri pikselə yerləşdirilir və beləliklə, steqo-piksellər əldə edilir. Deməli, istifadəçi müxtəlif steqanoqrafik vasitələrlə asanlıqla məxfi informasiya ötürə bilər. Ədəbiyyatda göstərilən bir çox icmallar təsvir steqanoqrafiyasına aiddir [16, s. 727-752, 30, s. 91-95,]. Təsvir steqanoqrafiyasına həsr olunan məqalələr əsasən son illərdə dərc edilib. Bunların sırasında yaxşı tədqiqat kimi qəbul edilən Abbas Cheddad və digərlərinin işidir [16, s. 727-752]. Bu məqalədə bütün mövcud steqanoqrafik üsullar müxtəlif təsnifləşmələr formasında təklif olunur və bunlar gizlədilmə domeninə, məxfi informasiyanın növünə və təsvirin kodlama formatlarına əsasən bölünür. Mehdi Huseyn 2018-ci ildə təqdim etdiyi yeni geniş icmalı Cheddad və digərlərinin icmalı ilə müqayisədə son illərə aid alqoritmləri əhatə edir. Bundan başqa son zamanlarda Subhedear [83, s. 95-113] və digərləri öz icmalında təsvir steqanoqrafiyasından bəhs etmişlər. Onların məqaləsində steqanoqrafik sistemlərin təməl konsepsiyaları həm sahə, həm də transform domen sahəsində alqoritmlərin göstəricilərinin ölçülməsi və təhlükəsizlik aspektləri geniş formada təhlil edilib. Eyni zamanda, informasiyanın şifrlənməsi ilə gizlədilməsi arasındakı fərqi müqayisə edərək onların əsas xüsusiyyətlərini əks etdirib. Gizlədilən məxfi informasiyanın həcmi təsvirin piksel sahələrindən asılıdır.

Gizlədilən məxfi informasiyanın həcmini artırmaq üçün PVD ilə LSB əvəzləməsi üsullarını kombinə etmək mümkündür. Bu zaman yaxşı vizual keyfiyyət və daha böyük həcmdə məxfi informasiya gizlədilməsi əldə edilir. Bir metodda da

Multi- Way PVD üsulu ilə Tri- Way PVD və mod seçim prosesi kombinə edilir. Nəticədə isə vizual keyfiyyət yaxşılaşır, lakin gizlədilən məxfi informasiyanın həcmi azalır.

Təsvir interpolyasiyası

Steqanoqrafiyada konteynerin modifikasiya edilməsi üsullarına misal kimi konteynerin interpolyasiya edilərək alınmış piksellərə məxfi informasiya bitlərinin gizlədilməsini göstərə bilərik. İnterpolyasiya üsulu az aydınlıq dərəcəsinə malik təsvirdən daha yüksək aydınlıq dərəcəli təsvir alınmasına xidmət edir. İnterpolyasiya alqoritmləri məxfi informasiyanın ötürülməsi üçün istifadə edilən örtük təsvirinin keyfiyyətinin yüksəldilməsi məqsədilə istifadə edilir. Bu siqnal nəzəriyyəsində geniş istifadə edilən mühüm alqoritmlərdən biridir. Eyni zamanda kompüter qrafikası və təsvir emalına bənzər olaraq böyük tarixə malikdir.

Elmi ədəbiyyatda interpolyasiya alqoritmlərinin istifadəsinə aid kifayət qədər məqalələr mövcuddur [2, s. 98-104, 14, s.378-386, 37, s. 447-455, 48, s. 7795-7810, 47, s. 143-155, 63, s. 102-111, 80, s. 65-76, 105, s. 603-606]. Bu məqalələrdə təsvir interpolyasiya sahəsindəki tədqiqatların əsas məqsədi təsvirlərin üzərində aparılan hesablamaların sadələşdirilməsi və keyfiyyətinin yüksəldilməsidir. Bunlardan bəzilərini nəzərdən keçirib analiz edək. Ki-Hyun və digərləri [43, s. 465-470] 2009-cu ildə, interpolyasiyadan istifadə edərək yeni informasiya gizlətmə alqoritmi təklif ediblər. Alqoritm az mürəkkəbliyə və müvafiq olaraq sürətli hesablamaya malikdir. Qonşu piksellərin orta qiymətinə əsaslanan interpolyasiya (Neighbor Mean Interpolation, NMI) adlanan bu alqoritmə uyğun olaraq qonşu piksellərin qiymətlərinin orta qiymətləri hesablanır və daha sonra hesablanmış yeni qiymətə malik piksellərdə informasiya gizlədilir. Ümumiyyətlə bu üsuldan istifadə etməklə daha yüksək aydınlıq dərəcəsinə malik piksellər əldə etmək mümkündür. Bu da təklif olunan NMI alqoritminin üstün cəhətidir.

Təsvir interpolyasiyası üsulundan istifadə etməklə məxfi informasiyanın gizlədilməsi

Verilənlərin gizlədilməsi ötürülən informasiyanın mövcudluğunu gizlətməkdir. Məxfi informasiya steqo−təsvirdən çıxarıldıqdan sonra konteynerin yenidən bərpa olunması mümkün olan məlumatları gizlətmə alqoritmi (reversible data hiding) [39, s. 2911-2922, 59, s. 187-193, 60, s. 2400-2404], məxfi informasiyanı steqo−təsvirdən konteyner təsvirini təhrif etmədən çıxarmağa imkan verir [49, s. 2143-2155, 63, s. 102-111, 78, s. 214-230, 89, s. 9717-9735]. Birbaşa yerləşdirmə prosesində informasiyanın hər bir biti konteyner təsvirinin verilənlərinə gizlədilə bilər və yaxud seçilmə yolu ilə təsvirin küylü, az nəzərə çarpan sahələrində gizlədilir [62, s. 2374-2384]. Tətbiq olunan bir sıra gizlətmə üsullarından ən çoxu ümumi cəhətlərə malik üsul LSB, maskalanma, filtrlənmə alqoritimləri və çevrilmələridir [67, s. 286-291]. Konteynerin yenidən bərpa olunmasına əsaslanan informasiya gizlətmə alqoritmi konteyner təsvirin dəqiq bərpa olunma imkanına malikdir. Yəni, gizlədilmiş məlumat çıxarıldıqdan sonra konteynerdə heç bir itki baş vermədən geri qaytarılması təmin edilir. Bu tip məxfi informasiya gizlədilməsi metodları iki tipə bölünür: additiv paylanmış spektrli və host siqnalların seçilmiş xüsusiyyətlərinin modifikasiya edilmiş gizlədilmə metodları. Siqnal nəzəriyyəsində siqnalların interpolyasiyası və tədqiqat üsulları çox mühümdür və onların bir çox tətbiq sahələrinə tez-tez rast gəlinir [26, s. 209-215]. Təsvirin genişlənməsi üçün bir sıra üsullar istifadə edilir. Az aydınlığa malik təsvirlə yüksək aydınlıqlı təsvir arasındakı əlaqəni təsvir edən modellərdə interpolyasiya alqoritminin böyük rolu var. Adi xətti interpolyasiya sxemləri sabit fəza modellərinə əsaslanır. Burada təsvirin kənarlarındakı rəng çalarlarının kəskin dəyişdiyi sahələrin statistikasından istifadə edilir. Xətti interpolyasiya üsulları əsasən öz hesablama sadəliyinə görə üstün tutulur. Miqyası böyüdülmüş təsvirlər burada təklif edilən informasiya gizlədilmə alqoritmində konteyner təsvir kimi istifadə edilməsi üçün yaradılır. Təklif edilən qonşu piksellərin orta qiymətinə əsaslanan interpolyasiya üsulu (NMI) daha çox effektivdir.

Təsvir steqanoqrafiyasında məxfi verilənləri gizlətmək üçün müxtəlif metodlara əsaslanan alqoritmlərdən istifadə olunur. İnterpolyasiya üsulu siqnallar nəzəriyyəsində geniş istifadə olunan vacib üsullardan biridir. Eyni zamanda interpolyasiya üsullarına bir çox tətbiqlərdə də tez-tez rast gəlinir.

İnterpolyasiya üsullarının tətbiqinin əsas məqsədi daha az və asan hesablama üsullarından istifadə etməklə yüksək nəticələr əldə etməkdir. İnterpolyasiya alqoritmləri ilə yanaşı digər alqoritmlərə əsaslanan steqanoqrafik metodlar və alqoritmlər də bu fəsildə analiz edilir.

Qonşu piksellərin orta qiymətinə əsaslanan orta qiymət interpolyasiya metodu

Ənənəvi interpolyasiya üsulu kimi yaxın qonşu piksellərin interpolyasiya metodu və iki xətti interpolyasiya üsulları mövcuddur. İki xətti interpolyasiya metodu dörd yaxın piksellərdən istifadə edərək koordinatları müəyyən edir və təsvirin aydınlıq göstəricilərini (resolution) yaxşılaşdırır. Lakin yaxın qonşu piksellərin interpolyasiya metoduna görə 3-4 dəfə çox hesablama vaxtı tələb edir. Ki-Hyun Jung və Kee-Young Yoo "Data hiding method using image interpolation" [43, s. 465-470] adlı məqaləsində yeni interpolyasiya metodu təklif ediblər. Təklif olunan qonşu piksellərin orta qiymətinə əsaslanan interpolyasiya metodu (NMI) orta qiyməti hesablamaq üçün qonşu piksellərin qiymətini istifadə edir. Belə hesablama üsullarından istifadə edərək daha yüksək aydınlıq göstəricisi olan piksellər əldə etmək olur. Bu da müəlliflər tərəfindən təklif edilən qonşu piksellərin orta qiymətinə əsaslanan orta qiymət interpolyasiya metodunun üstünlüyüdür.

Çəki matrisinə əsaslanan reversiv məlumat gizlətmə alqoritmi

[45, s. 239-248]-də Jana Biskapati və s. yüksək tutuma malik çəki matrisinə əsaslanan yeni bir məlumat gizlətmə metodu təqdim edib. Həmin metodda ilkin təsvirin ölçüsü interpolyasiya olunaraq böyüdülür. Təklif edilən metodda yerləşdirilmiş məxfi informasiyanın həcmi orta hesabla 2,97 bit piksel (bpp) təmin edir, vizual keyfiyyəti isə PSNR 37,97 dp-dən yüksək olur.

Təklif edilən alqoritmi müxtəlif steqo hücumlara məruz qoyaraq təhlükəsizlik dərəcəsini müəyyən ediblər. Bu üsulun fərqləndirici xüsusiyyəti ondan ibarətdir ki,

çəki matrisi modifikasiya edilməklə məlumat gizlədilməsində, təhlükəsizlik dərəcəsi məxfi *k* açarı vasitəsilə yüksəldilir.

Burada müzakirə edildiyi kimi, alqoritm məxfi informasiya bitlərini bir blokda gizlətməyə imkan verir. Bu alqoritm [45, s. 239-248]-də ətraflı təsvir edilmişdir. Bu alqoritmin üstünlükləri faydalı yükün 2,97 bit/piksel (bpp) və PSNR 38 pp ilə təsvirin daha yüksək vizual keyfiyyəti hesab edilir. Bu alqoritm digər geniş istifadə olunan alqoritmlərlə müqayisə edilmiş və daha çox məxfi informasiya biti yerləşdirmə qabiliyyəti və vizual keyfiyyəti təsdiq edilmişdir.

Eyni zamanda, alqoritm müxtəlif hücumların vəziyyətini və müəyyən edilmiş təhlükəsizlik səviyyələrini sınaqdan keçirib. Təklif olunan alqoritm məlumatların gizlədilməsinin daha yüksək təhlükəsizlik səviyyəsinə malikdir ki, bu da məxfi *k* açarından istifadə etməklə və çəki matrisinin modifikasiyası ilə əldə edilir.

İnterpolyasiya və fərq qiymətinin əsasında təsvirin genişlənməsinə əsaslanan yüksək tutumlu iki mərhələli məlumat gizlətmə alqoritmi

[86, s. 1311-1316] Sabeen Govind və digərləri iki mərhələli yüksək yerləşdirmə tutumuna malik informasiya gizlətmə alqoritmi təklif ediblər. İlk mərhələdə ilkin təsvir təkmilləşdirilmiş qonşu piksellərin orta qiymətinə əsaslanan interpolyasiya (Enhanced Neighbor Mean Interpolation, ENMI) üsulu ilə interpolyasiya edilərək konteyner təsvir yaradılır. İstifadə olunan interpolyasiya üsulu Ya-Ting Chang və digərlərinin [105, s. 603-606] ədəbiyyatda təklif edilmişdir.

İki mərhələli alqoritmə görə daha çox məxfi informasiya bitinin yerləşdirilməsini təmin edən yeni bir metod işlənilib hazırlanmışdır [86, s. 1311-136]. Şəklin interpolyasiyasının birinci mərhələsində, (ENMI) alqoritmindən istifadə etməklə ilkin təsvirdən konteyner təsvir yaradılır.

Qonşu piksellər əsasında interpolyasiya metodu

[58, s. 6712-6719] Chin-Feng Lee və Yu-Lin Huang tərəfindən təklif etdilən interpolyasiya metodu Jung K.H. və Yoo K.Y. [43, s. 465-470] da təklif olunan üsulun təkmilləşdirilməsi ilə yerləşdirmə həcminin daha da artırılmasına yönəlib.

Ümumiyyətlə, yaradılmış konteyner təsviri ilə ilkin təsvir arasındakı oxşarlıq maksimum olmalıdır. Buna görə də, burada aparılan tədqiqat daha keyfiyyətli təsvirin interpolyasiyası metodunu təklif etmək üçün piksel lokallaşmasının xüsusiyyətini nəzərdən keçirir. Təsvirlər adətən müəyyən mövqedə piksel qiymətinin qonşu piksel qiymətinə oxşar olduğunu nəzərdə tutan bəzi ehtiyyatlardan ibarət olduğuna görə, gizlədiləcək məxfi informasiya bitinin sayının artırılması adətən təsvirin təhrifinə səbəb olur.

Bu tədqiqat, təsvirin daha az təhrif olunaraq gizlədilmə qabiliyyətinin yüksəldilməsinə yönəldilmişdir. Bu məqsədlə qonşu piksellər arasındakı fərq qiymətlərini maksimuma çatdırmaq üçün effektiv təsvir interpolyasiyasından əldə edilən artıqlığın yaxşı nəticələrindən istifadə edir.

Digər interpolyasiya alqoritmlərində yaxın yerlərdə yerləşən piksellər oxşar intensivlik qiymətlərinə malik olur. INP (Interpolation by Neighboring Pixels -qonşu piksellər üzrə interpolyasiya alqoritmi) metodu genişləndirilmiş təsviri yaratmaq üçün qonşu piksellərin oxşar xüsusiyyətlərindən istifadə edir.

Tutaq ki, (w/2) (h/2) ilkin təsvir var. Konteyner təsviri C kimi istifadə olunacaq w, h interpolyasiya təsvirini yaratmaq üçün təklif olunan INP, məxfi informasiyanın daxil edilməsinin növbəti mərhələsi üçün tətbiq edilir. INP (1.2.1) düsturu ilə təsvir edilə bilər. Burada $0 \le j \le i$ və $m,n = 0,1,2,....127$ bərabərdir.

$$C(i,j) = \begin{cases} I(i,j) & i = 2m, j = 2n \\ \left(I(i,j-1) + \left(I(i,j-1) + I(i,j+1)\right)/2\right)/2, & i = 2m, j = 2n+1 \\ \left(I(i-1,j) + \left(I(i-1,j) + I(i+1,j)\right)/2\right)/2 & i = 2m+1, j = 2n \\ \left(C(i-1,j) + C(i,j-1)\right)/2 \end{cases} \qquad (1.2.1)$$

burada $i = 2m, j = 2n$ üçün $C(i,j) = I(i,j)$ pikseli verilənlərin daxil edilməsinin növbəti mərhələsi emal edildikdə heç vaxt dəyişdirilməyəcək olan piksel kimi istinad edilir. INP-ni həyata keçirmək üçün fərz edilir ki, $I(x,y)$ilkin I təsvirdə (x,y)nöqtəsində yerləşən pikselin qiymətini ifadə edir. INP tətbiq edildikdən sonra konteyner təsvirinin konteyner pikseli $C(i,j)$və $C'(i,j)$ steqo-pikseli ifadə edir.

INP prosedurunun emal olunmasna aid nümunə [58, s. 6712-6719]-də göstərilib

Burada məxfi informasiyanın çıxarılması proseduru yerinə yetirildikdə, C konteyner təsvirinin dörd dəyişməyən (pivot) piksel qiymətinin I ilkin təsvirin dörd pikselinin qiymətlərinə bərabər olduğu görünür,

Buna görə də, ilkin təsvir *I* steqo−təsvirdən asanlıqla bərpa olunur və məxfi informasiyalar dəqiq şəkildə çıxarılır.

[18, s. 7181-7205] Əhməd Muhammməd interpolyasiyaya əsaslanan hesablanması sadə olan yeni alqoritm təklif etmişdir. Müəlliflərin təklifinə görə bu üsulla gizlədilmiş informasiyanın həcmi böyük olur, konteyner təsvirindəki pozuntular isə minimum olur. Buna nail olmaq üçün iki mərhələdə iş aparılır. Birinci mərhələdə ilkin təsvir kiçildilir və interpolyasiya edilərək yenidən böyüdülür. Sonra ikinci mərhələdə isə məxfi informasiyanın yerləşdirilməsi prosesi aparılır. Müəlliflərin işlədiyi yeni təsvir interpolyasiya alqoritmi birinci addımda təsvirin pozuntularını azaldır, ikinci addımda informasiya gizlədilməsi zamanı baş verən pozuntular müəlliflər tərəfindən işlənilmiş alqoritmə görə minimuma endirilir. Bu alqoritmin fərqləndirici xüsusiyyəti ondan ibarətdir ki, tətbiq edilən alqoritm adaptiv formada gizlədilmiş informasiya tutumu ilə təsvirin keyfiyyəti arasındakı kompromisi tənzimləyir.

Təqdim olunan alqoritmin keyfiyyətini qiymətləndirmək üçün PSNR, WPSNR (Weighted PSNR) istifadə edilib. Bu alqoritmdə gizlədilmiş məxfi informasiya həcmi 1,7 bpp-ə bərabərdir, PSNR 54 dp, WPSNR 78 dp ə bərabərdir.

İstənilən məxfi infromasiya gizlətmə alqoritminin məqsədi informasiya gizlətmə qabiliyyətini artırmaq və eyni zamanda steqo-təsvirin vizual keyfiyyətini qorumaqdır. Təəssüf ki, vizual keyfiyyət və məxfi informasiya gizlətmə qabiliyyəti iki ziddiyyətli tələbdir. Yəni, məxfi informasiyanın gizlədilməsi qabiliyyətinin artırılması təsvirin təhrif olunmasına gətirib çıxarır və təsvirin keyfiyyətinin yaxşılaşdırılması konteyner təsvirində daha az məxfi informasiyanın gizlədilməsinə imkan verir. Burada müəlliflər sadə ədədi hesablamaları saxlayaraq məxfi informasiya gizlətmə qabiliyyətini və steqo−təsvirin vizual keyfiyyətini artıran yeni geri çevrilə bilən

gizlətmə alqoritmi təklif ediblər. Məlumat gizlətmə qabiliyyəti ilə steqo−təsvirin vizual keyfiyyəti arasında məqbul bir uzlaşma əldə etmək üçün yeni interpolyasiya genişləndirilməsi alqoritmi təklif olunub ki, bu da daha çox sayda daxil edilə bilən piksellə əldə olunur. Bunun nəticəsində də məxfi informasiyanın gizlədilməsi qabiliyyətini artırır. Həmçinin təsvirin təhrifini azaltmaq və məxfi informasiyanın gizlədilməsi mərhələsində daşmanın qarşısını almaq üçün yeni adaptiv məxfi informasiya gizlətmə alqoritmi təklif olunub.

[25, s. 271-350]-də Yong Chen və digərləri təsvir interpolyasiyasına əsaslanan effektiv məxfi informasiya gizlətmə alqoritmi təklif edib. Təklif olunan alqoritmdə onluq say sistemində olan məxfi informasiyalar interpolyasiya edilmiş konteyner təsvirinə daxil edilir. Buna görə də, təklif olunan alqoritm yerləşdirilmiş informasiya həcmi ilə təsvir keyfiyyəti arasında nisbi tarazlığı saxlayır ki, bu da steqo−təsvirin keyfiyyətini artırır. İnformasiyanın gizlədilməsi zamanı interpolyasiya edilmiş konteyner təsvir ilə ilkin təsvirin pikselləri müqayisə edilir. Əgər interpolyasiya edilən piksel ilkin pikseldən böyük olarsa, bu zaman məxfi informasiya biti interpolyasiya edilmiş konteyner təsvirinin pikselindən çıxılır, əks halda isə toplanır. Eksperimental nəticələr göstərir ki, təklif olunan alqoritm nisbətən daha böyük həcmdə informasiya gizlədilməsinə və digər alqoritmlər ilə müqayisədə orta hesabla 1,6 dB artım əldə edə bilər. Vizual effekt müxtəlif təsvir interpolyasiyası alqoritmləri ilə istifadə olunduqda üstün olur.

Təklif olunan məxfi informasiya gizlədilməsi alqoritmində ilkin təsvirdəki piksellər istinad üçün istifadə olunur və steqo-təsvir piksellərinin ilkin piksellərə daha yaxın olması üçün müxtəlif situasiyalarda onluq qiymətə malik məxfi informasiya baytları əlavə olunur və ya çıxarılır.

Məxfi informasiyalar blok-blok daxil edildiyindən, verilənlərin daxil edilməsi üçün başlanğıcda daha mürəkkəb teksturalı bloklar seçilərsə, steqo−təsvirin təsvir keyfiyyəti açıq şəkildə yaxşılaşdırıla bilər.

Yüksək tutuma malik informasiya gizlətmə alqoritmi.

[88, s. 20527-20545] Sabeen G. və digərləri yeni gizlətmə alqoritmi təklif etmişdilər. Təklif olunan alqoritmdə ilkin təsvir əvvəlcə NMİ [43, s. 465-470] alqoritmi ilə interpolyasiya edilərək konteyner təsvir yaradılır, daha sonra kvorum funksiyasından istifadə edilərək məxfi informasiya yaradılan konteyner təsvirə gizlədilir və beləliklə steqo-təsvir alınır.

Məxfi informasiyanın gizlədilməsi üçün kvorum funksiyası 3QF (quaroum function) istifadə olunur.

Konteyner təsvirini yaratdıqdan sonra kvorum funksiyası konteyner təsvirinin piksellərinin son 3 əhəmiyyətli bitinə tətbiq olunur. 3 girişli kvorum funksiyasında (3QF) məntiqi AND (∧) və XOR(⊕) istifadə olunur. Kvorum funksiyası [47, s. 2017-2028]-da geniş göstərilmişdir.

1.3. Steqanoqrafiya alqoritmlərinin qiymətləndirilməsi və steqoanaliz alqoritmləri

Təsvir steqanoqrafiyasının inkişafı onun qiymətləndirilmə üsullarının da əhəmiyyətini artırır. Steqanoqrafik alqoritmlərin göstəricilərinin qiymətləndirilməsi zamanı aşağıdakılara diqqət yetirilir [69, s. 12-17]:

- Təsvirin vizual keyfiyyəti;
- Məxfi informasiyanın həcmi ;
- Dayanıqlılığı;
- Aşkarlanmamaq/təhlükəsizlik;
- Alqoritmin hesablama mürəkkəbliyi;

Hər bir göstəriciyə ayrı-ayrılıqda nəzər yetirək.

Vizual keyfiyyətin ölçülməsi.

Buna aid geniş icmal [68, s. 46-66] də verilib. Müxtəlif steqanoqrafik alqoritmlər məxfi informasiyanın gizlədilməsi zamanı konteyner təsvirin vizual keyfiyyəti alqoritmdən asılı olaraq bir-birindən fərqlənir. Lakin insanın görmə sistemi ilə bunun asanlıqla aşkarlanması çox çətindir və bəzən mümkün deyil. Standart ölçü texnikaları vizual modifikasiya səviyyəsini qiymətləndirir. Buna baxmayaraq ədəbiyyatda ste-

qanoqrafiya (MSE, RMSE, PSNR və s.), su nişanı üçün keyfiyyəti ölçən müxtəlif üsullar verilib. Ən çox istifadə edilənlər isə aşağıda göstərilir:

- Orta kvadratik xəta – Mean square error (MSE),
- Kökaltı orta kvadratik xəta – Root mean square error (RMSE),
- Siqnalın küyə nisbəti – Signal to noise ratio (SNR),
- Pik siqnalın küyə nisbəti – Peak signal to noise ratio (PSNR),
- Struktur oxşarlıq indeksi ölçüsü – Structural similarity index measure (SSİM).

Təhlükəsizlik/ Aşkarlanmama.

Təhlükəsizlik və yaxud aşkarlanmama həmçinin təsvir steqanoqrafiyasının mühüm qiymətləndirmə parametrləridir. Ümumiyyətlə, steqanoqrafik sistemlər müxtəlif tip aşkarlama hücumlarına məruz qalırlar. Hücumçuları steqo-təsvirdə məxfi informasiya bitlərinin mövcudluğunun aşkarlanması və hətta onu əldə etməsi imkanı cəlb edir [21, s.142-172].

Dayanıqlılıq

Adətən dayanıqlılıq transform domen metodlarında ölçülür. Lakin son vaxtlar müxtəlif sahə domeni steqanoqrafik alqoritmlərinin yaradılması zamanı da istifadə edilib. Dayanıqlılığın əsas şərti odur ki, steqo−təsvir məxfi informasiyanı qoruyub saxlamağa qadir olsun. Hətta küy əlavəsi şəffaflaşdırmaq, bulanıqlaşdırmaq, miqyaslaşdırmaq, fırlamaq, kəsmək və s. kimi əməliyyatlar aparıldıqda belə informasiyanı qorumağa qadir olmalıdır. Yuxarıda baxdığımız bəzi sahə domeni steqanoqrafik metodlarında dayanıqlılığın təməl səviyyəsi əldə edilir.

Hesablamaların mürəkkəbliyi

Steqanoqrafik yanaşmalarda hesablamaların mürəkkəbliyi gizlədilmə və çıxarılma alqoritmlərinin effektiv işləməsinə təsir göstərir. Bu zaman sərf olunan vaxt və əməliyyatların sayı əhəmiyyət daşıyır. Minimal hesablama mürəkkəbliyi ideal hesab edilir. Normalda sahə domeni əsaslı steqanoqrafik metodlar sadə və az hesablama tələb edir. Buna baxmayaraq bəzi maşın təlimi alqoritminə əsaslanan metodlar çox mürəkkəb hesablamalar tələb edir.

Steqoanaliz alqoritmləri

Steqoanaliz dedikdə şübhəli kompüter fayllarında məxfi informasiyanın mövcudluğu faktını aşkarlamaq üçün aparılan kompleks tədbirlər nəzərdə tutulur [6, s. 204-206, 28, s. 48-53, 21, s. 142-172]. İnformasiyanın steqanoqrafik mühafizəsi zamanı təxmin edilir ki, bədniyyətli ötürmə kanalına nəzarət edərək ona maraqlı olan materialların olmasını yoxlayır. Hücum, müvafiq steqanoqrafik sistem sındırılmış olduqda və hücum edən məxfi informasiyanın mövcudluğunu aşkarlaya bildikdə uğurlu hesab edilir. Ona görə də, steqanoqrafik sistemin istifadəsi zamanı daim onun dayanıqlılığını xarakterizə edən parametrlərini dəyərləndirməli və məxfi informasiyanın ötürülməsindən əvvəl steqoanalizə müraciət edilməlidir.

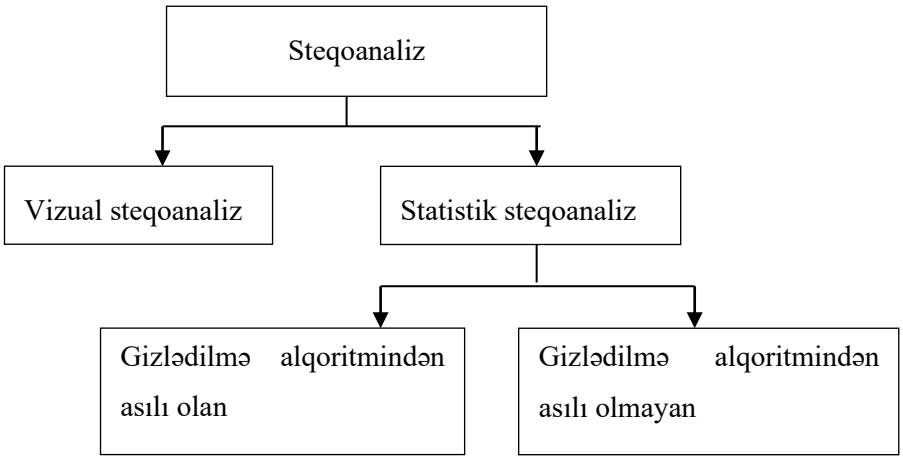
Steqanoqrafiya və steqoanaliz bir–birinə qarşı olan mübarizənin əks qütbləridir. Yeni bir steqanoqrafik alqoritm yaradıldığı zaman, ona əks cavab kimi steqoanaliz alqoritmi də inkişaf edir ki, alqoritmin keyfiyyətini analiz etsin və yaxud da onu pozsun. Adətən steqoanaliz alqoritmləri iki əsas kateqoriyaya bölünür: passiv və aktiv steqoanaliz.

Passiv steqoanaliz məxfi informasiyanın mövcudluğunu və ya olmamasını müəyyən edir yaxud xüsusi gizlədilmə prosesini üzə çıxarır.

Passiv steqoanaliz üsullarına nisbətən aktiv steqoanaliz üsulları daha dərindir. O, məxfi informasiyanı çıxara və ya modifikasiya edə bilər yaxudda məxfi informasiyanın həcmini qiymətləndirə bilər. Bu məqsədə nail olmaq üçün bir çox steqoanaliz alqoritmləri təklif olunur [31, s. 868-882] və biz onların hər birinin incəliklərinə baxmadan steqoanalizin yalnız ümumi prinsiplərini nəzərdən keçiririk.

Steqoanaliz alqoritmləri şəkil 1.3.1-də göstərildiyi kimi, əsasən 2 kateqoriyaya bölünə bilər [6, s. 204-206]:

- Vizual steqoanaliz;
- Statistik steqoanaliz.



Şəkil 1.3.1. Steqoanaliz alqoritmlərinin təsnif edilmə sxemi

Vizual steqoanaliz daha sadə, lakin az effektivdir. Nəzərə alsaq ki, əksər hallarda məxfi informasiya konteynerin ən az əhəmiyyətli bitləri ilə ardıcıl olaraq əvəzlənir və ya ixtiyari gizlədilir onda steqo-təsvirin bit müstəvisini vizual analiz etmək olar. İstənilən halda konteyner təsvirin bit müstəvisinin strukturu informasiyanın gizlədilməsinin nəticəsində pozulmuş olur [57, s. 142-172]. Lakin gizlədilmə prosesi çox diqqətlə yerinə yetirildikdə, pozuntuların vizual müəyyən edilməsi mümkün olmur. Bu da vizual steqoanaliz alqoritmlərinin mənfi tərəfidir.

Digər zəif tərəfi isə ondan ibarətdir ki, böyük miqdarda konteyneri emal etmək mümkün deyil. Konteyner təsviri ilə steqo−təsvirin eynilik dərəcəsini qiymətləndirərkən insana elə gəlir ki, onların arasında heç bir fərq yoxdur, lakin steqoanaliz statistik fərqləri üzə çıxara bilir. Statistik steqoanaliz alqoritminin köməkliyi ilə steqo-təsvirlə konteyner təsvirin arasındakı fərqə əsasən gizlədilmiş informasiyanı aşkarlamaq mümkün olur. Statistik alqoritmləri iki qrupa bölmək olar: gizlədilmə alqoritmindən asılı olanlar - PoVs-qiymətlər cütü (Pair of Values), Xi-kvadrat və digər ən az əhəmiyyətli bit təmayüllü gizlədilmə metodları. [106, s. 147-166]-də TPVD istifadə etməklə məxfi informasiyanı qiymətləndirən gizlədilmə alqoritmi yaradılıb və xüsusi steqoanaliz kimi tanınır. Universal steqoanalizə misal kimi [34, s. 349-353]-də təsvirin sətir və sütunlarının lokal qonşuluqda bir-birindən asılılığı təklif edilib. Konkret gizlədilmə alqoritminə istiqamətləndirilən, xüsusi steqoanaliz alqoritmləri praktikada az istifadə olunur. Çünki informasiyanın konteyner təsvirində

gizlədilmə alqoritmi əvvəlcədən hücum edənə məlum deyil. Gizlədilmə alqoritmindən asılı olmayan universal statistik steqoanaliz xüsusi gizlədilmə alqoritmlərinə yönəldilməyən gizlədilmə alqoritmlərindən ibarətdir. Adətən məxfi informasiyanın təsvirdə mövcudluğunu universal statistik steqoanalizlə yoxlamadan əvvəl məxfi informasiya gizlədilməmiş "boş" konteyner və steqo-təsvirlərdə hər hansı bir statistik steqanoqrafik dəyişiklərin olmasını yoxlamaq lazım gəlir. Bu növ universal alqoritmlərin müsbət tərəfi ondan ibarətdir ki, istənilən, hətta məlum olmayan steqanoqrafik alqoritmlərlə işləmək olur. Statistik alqoritmlər vizual steqoanalizlə müqayisədə daha etibarlıdırlar və yüksək nəticələr verirlər. Belə ki, riyazi alqoritmlər vizual qavrama ilə müqayisədə daha çox həssas və dəqiqdirlər. Müxtəlif universal steqoanaliz alqoritmləri mövcuddur. Buna aid etmək olar: Binar oxşarlığın ölçülməsi alqoritmi (Binary Similarity Measures (BSM), Wavelet əsaslı steqoanaliz, xüsusiyyətə əsaslanan steqoanaliz və digərləri. Ədəbiyyatda xüsusi tip steqoanalizdə istifadə edilən statistik və qeyri-statistik alqoritmlər barədə [37, s. 447-455] və universal tipli steqoanaliz üçün istifadə edilən məlumatlar var. Bu barədə ətraflı məlumat [57, s. 142-172] da tapmaq olar.

Steqoanaliz ilə alqoritmlərin təhlükəsizlik səviyyəsinin qiymətləndirilməsi. Bu hissədə steqoanalizin çox incəliklərinə varmırıq, çünki bunlar [74, s. 1758-1770]-də verilib. Hədəfimiz ədəbiyyatda istənilən steqanoqrafik yanaşmaların təhlükəsizlik səviyyəsini qiymətləndirən test analizlərinin və aşkarlama hücumlarının müzakirə edilməsidir. Aşağıdakı hissələrdə test və analiz üsullarının təməl növləri verilir.

Vizual steqoanaliz. İstənilən steqanoqrafik üsulda insanın görmə sistemi üçün (vizual) görünməzlik ən çox əhəmiyyətli tələblərdən biridir. Gizlədilmə ilə əlaqədar olan vizual artefaktlar gözlə görünməz olur. Çünki insan görmə sisteminin imkanları məhduddur. Vizual keyfiyyətin ölçülməsini qiymətləndirmək üçün müxtəlif keyfiyyət ölçmə üsullarından istifadə edilir. Ümumən MSE, PSNR, SSIM, QINDEX üsulları təsvirlərin vizual bənzərliyini qiymətləndirmək üçün istifadə edilir.

Statistik steqoanaliz. Bu steqoanaliz təsvirlərin struktur xarakteristikalarından istifadə edərək qeyri-adi xassələri aşkarlayır. Həmin xassələrin yaranmasının səbəbi

istənilən steqanoqrafik üsulla əlaqəlidir. Bir çox statistik analiz növləri var, belə ki, histoqram analizi, bit plane analizi, sadə cüt analizi (xi-kvadrat), nizamlı və tək analiz - RS (regular and singular) analiz alqoritmləri. Bu üsullar asanlıqla məxfi informasiyanın mövcudluğunu üzə çıxarır və hətta məxfi informasiyanın ölçüsünü qiymətləndirə bilir.

Histoqram əsaslı steqoanaliz. Bu, həmçinin steqo-təsvirin yoxlanılması üçün effektiv hesab edilir. Piksellərin paylanmasının və yaxud qeyri-adi formaların identifikasiya edilməsi üçün konteyner və steqo−təsvirin histoqramları müqayisə edilir. Bir çox hallarda PVD əsaslı steqanoqrafik üsullar histoqram analizinin müxtəlif dəyişmələri ilə dəyərləndirilir. Misal üçün piksel fərqləri histoqram analizi, histoqram xarakterik funksiya analizi, kütlənin mərkəzi (HCF-Com Characteristic Function-Center of Mass) analizi.

RS steqoanaliz. Nizamlı və tək analiz (Regular and singular) RS üsulu kimi təsadüfi LSB gizlədilmə alqoritmlərində aşkarlama etmək üçün işlənilib. Bu üsul piksellərin LSB-sində kiçik dəyişmələrdən istifadə edir və bu dəyişmələrlə diskriminasiya funksiyasını, piksellərin müntəzəm və tək qruplara bölünməsini təmin edir. Bu qrupların tezliyi steqo-təsvirin içərisindəki məxfi informasiyanın uzunluğunu müəyyən edir. Ədəbiyyatda bir sıra RS steqoanalizinə aid steqanoqrafik üsullar qiymətləndirilir ki, onların təhlükəsizliyini və aşkarlanmamağını isbat edir.

RS steqoanalizinin tətbiqi. Bu analiz, təsvirlərdə fəza korelyasiyası əsasında yaradılmış həssas ikili statistikadan istifadə edir. RS steqoanalizi 24 bit rəngli və 8 bit boz təsvirlərdə istifadə olunur. RS steqoanaliz, təsvir faylları üzərində ən az əhəmiyyətli bitin əvəz edilməsi üsulu əsasında (LSB Insertion Methods) məxfi informasiya gizlənib gizlənmədiyini aşkarlamaq üçün istifadə edilir.

RS steqoanalizində təsvirin pikselləri 3 müstəqil qrupa: nizamlı (regular) piksellər, tək (singular) piksellər və istifadə edilməyən piksellərə ayrılır. Bu steqoanaliz ilk dəfə Fridrich tərəfindən təklif edilmişdir [31, s. 868-882].

Test edilmiş təsvir (R)və Pçoxluğunun qiymətlərinə daxil olan $M \times N$ sayda pikseldən ibarətdir. Məsələn, 8 bitlik boz təsvirdə $P = \{0....255\}$ olur. İlk əməliyyat olaraq (R), n qonşu pikseldən ibarət G ayrı qruplarına bölünür:

$$f(G) = f(x_1, x_2, ...x_n) \in R \tag{1.3.1.}$$

Ayırıcı funksiya aşağıdakı kimidir:

$$f(x_1, x_2, ...x_n) = \sum_{i=1}^{n-1} |x_{i-1} - x_i| \tag{1.3.2.}$$

Misal üçün $n = 6$ olduqda ayırma funksiyası aşağıdakı kimi olacaq:

$$G = (x_1, ...x_6)$$
$$f(x_1, x_2, x_3, x_4, x_5, x_6) = |x_2 - x_1| + |x_3 - x_2| + |x_4 - x_3| + |x_5 - x_4| + |x_6 - x_5| \tag{1.3.3}$$

RS steqoanalizi üçün iki ədəd sürüşdürmə funksiyası istifadə edilir. Bu sürüşdürmə funksiyaları aşağıdakı kimidir:

$$F_1 : 0 \leftrightarrow 1,2 \leftrightarrow 3,4 \leftrightarrow 5,....254 \leftrightarrow 255$$
$$F_{-1} : -1 \leftrightarrow 0,1 \leftrightarrow 2,3 \leftrightarrow 4,.....255 \leftrightarrow 256 \tag{1.3.4}$$

$f(G)$qiymətləri hesablandıqdan sonra maskalama əməliyyatı tətbiq edilir. Maska(M), (-1,0,1) qiymətlərindən təşkil edilmişdir. Bu maska G-yə tətbiq edilir və $F_M(G)$qiymətləri hesablanır. Əgər maskanın qiyməti 1 olarsa, F_1 sürüşdürmə funksiyası, maskanın qiyməti -1 olarsa F_{-1} sürüşdürmə funksiyası istifadə edilir. Daha sonra -M maskası üçün $F_{-M}(G)$qiymətləri hesablanır. Hesablanan bu qiymətlər aşağıdakı şərtlərə görə qiymətləndirilərək $R_M, R_{-M}, S_M, S_{-M}, U_M, U_{-M}$ ədədləri hesablanır.

- Əgər $f(F(G)) > f(G)$ olarsa, G piksel qrupu nizamlıdır (R).
- Əgər $f(F(G)) < f(G)$ olarsa, G piksel qrupu təkdir (S).
- Əgər $f(F(G)) = f(G)$ olarsa, G piksel qrupu istifadə edilməyəndir (U).

Bütün G qrupları üçün pozitiv və neqativ maskalar istifadə edilərək R, S və U qruplarının qiymətləri müəyyən edilir. Daha sonra təsvirin bütün piksellərinin son

bitləri dəyişdirilir və yuxarıdakı əməliyyatlar təkrar edilir. R_M, R_{-M}, S_M və S_{-M} qiymətləri qarşılaşdırılaraq bir nəticə əldə olunur.

$$\begin{aligned} R_M &\cong R_{-M} \\ S_M &\cong S_{-M} \end{aligned} \tag{1.3.5}$$

Sıfır mesaj hipotezinə görə əgər yuxarıdakı şərt ödənirsə, deməli təsvirin içində məxfi informasiya yoxdur. Qiymətlərin 0-a yaxın çıxması təsvirin içində məxfi informasiyanın olmadığını göstərir.

Xi kvadrat analizi. Bu qiymətlər cütlüyü adlanan üsul (pairs of values) statistik analizə əsaslanır və məxfi informasiyanın yerləşdirilməsi zamanı dəyişir (mübadilə edilir). Bu üsul LSB əsaslı yerləşdirmənin aşkarlanması üçün işlənilib. Gizlədilmə alqoritmlərinin sayı Xi kvadrat üsulu ilə aşkarlanır.

Bit müstəvisi analizi. Ümumən təsvirin hər bir bit müstəvisi digər qonşu bit müstəvisi ilə korellyasiya olunur. Steqanoqrafik alqoritm tətbiq edildikdən sonra korellyasiyalar dəyişə bilər və buna görə də bit müstəvisi analizi vasitəsilə görünə bilər. Bit müstəvisi analizi çox əhəmiyyətli dərəcədə əvəzetməyə əsaslanan yerləşdirmə üsulları ilə dəyərləndirilə bilər.

Qeyri-struktur steqoanaliz. Qeyri-struktur steqoanalizdə xüsusiyyətlərin ekstraktoru konteyner təsvirin modelindən istifadə edir və daha sonra steqo və konteyner təsvirin arasındakı pozuntunu qiymətləndirərək məxfi informasiyanın gizlədilməsini aşkarlamaq üçün istifadə edilir. Ümumən maşın təlimi alqoritmlərinə əsaslanan təsnifedici xüsusiyyətlər çoxluğunu öyrədir.

Yüksək göstəricilərə malik mövcud alqoritmlərin tədqiqi

Qarşıya qoyulan məqsəd təsvir steqanoqrafiyasına aid interpolyasiya əsaslı yeni, effektiv, daha böyük həcmdə məxfi informasiya gizlətmə qabiliyyəti (DH) və konteyner təsvirlə steqo-təsvir arasındakı oxşarlıq dərəcəsini təmin edən və steqo-hücumlara qarşı dayanıqlı steqanoqrafiya alqoritmlərinin işlənilməsidir. Ona görə də, son illərdə informasiya gizlətmə sahəsinə aid altı interpolyasiya əsaslı, yüksək göstəricilərə malik metodlar və alqoritmlər seçilərək meyar kimi götürülüb. Hər bir

alqoritm üçün əsas prosedurlar tədqiq edilərək üstün və çatışmayan cəhətləri müəyyən edilib.

Meyar kimi seçilən alqoritmlərin effektivliyini əks etdirən göstəricilər daha geniş və hərtərəfli qaydada yoxlanılaraq analiz edilib. Çünki dərc edilən məqalələrdə yalnız müəlliflərin üstünlük verdikləri parametrlər göstərilir və həmin parametrlər gizlədilmiş informasiyanın həcmindən, seçilmiş konteyner təsvirin növündən asılı olaraq, müxtəlif məqalələrdə eyni müəllifə aid alqoritmlər bir-birindən fərqlənir. Bu reallığı nəzərə alaraq, aparılan tədqiqata uyğun etibarlı nəticələr almaq üçün seçilmiş interpolyasiya əsaslı təsvir steqanoqrafiyası alqoritmləri mütəxəssislər tərəfindən bu gün daha çox istifadə edilən keyfiyyət göstəriciləri ilə yoxlanılıb.

Alqoritmlərin hesablama mürəkkəbliyi, yəni hesablamaların yerinə yetirilmə müddətinin çox olması mənfi hal kimi qəbul edilir. Lakin, araşdırılan bir çox tədqiqatda bu parametrin ölçülməsinə və nəticələrinə aid məlumata çox az rast gəlinir. Gizlətmə üçün istifadə edilən təsvirlərin nümunələri və sayı da fərqli olur. Misal üçün Jung və s. [43, s. 465-470], Chen Y. [25, s. 271-350], Mohəmməd [72, s. 647-654] məqalələrində müxtəlif təsvirlərdən istifadə edilib. Təbii ki, təsvirlərin sayının çox olması nəticələrin daha dəqiq olmasına gətirib çıxarır. Müəlliflərin qiymətləndirməsinə görə Jung və digərləri iki keyfiyyət göstəricisi təqdim ediblər:

- Gizlədilmiş məxfi informasiyanın həcmi-HC;
- Vizual keyfiyyət.

Jana və digərləri işlədikləri 6 addımdan ibarət alqoritmdə gizlədilmiş məxfi informasiyanın həcmi, əldə edilmiş steqo-təsvirin vizual keyfiyyəti və alqoritmin steqo-hücumlara qarşı dayanıqlığı verilib. Ona görə də, seçilən alqoritm barədə tam, dolğun təsəvvür yaratmaq bir qədər çətinləşir.

Deyilənləri nəzərə alaraq, bu işdə yüksək nəticələr əldə edən tədqiqatçıların alqoritmlərinin nəticələrinin daha geniş yoxlanılması aparılıb.

Seçilən alqoritmlərin əsas göstəriciləri yoxlanılarkən müəlliflərinin təsvirlər bazasından götürdükləri və məqalədə göstərdikləri eyni nümunələr konteyner təsvir

kimi istifadə edilib və eyni həcmdə məxfi informasiya gizlədilib. Hər bir alqoritmin özünə aid addımlar ardıcıllığı ilə gizlətmə prosesi həyata keçirilib.

Bütün bunlardan başqa göstərilən tədqiqatlardan görünür ki, bir interpolyasiya metodu müxtəlif illərdə müxtəlif gizlədilmə alqoritmləri ilə birləşdirilərək yeni alqoritmlər təqdim edilib. Buna misal kimi NMI və digər interpolyasiya alqoritmlərini göstərə bilərik. Bu tədqiqatlarda təklif edilən alqoritmləri yoxlamaq məqsədilə eyni təsviri ilkin təsvir kimi və eyni həcmdə məxfi informasiyanı həmin alqoritmlər vasitəsilə gizlətdik. Bundan sonra əldə edilmiş steqo-təsvirin PSNR, MSE, SSIM, HC və ümumi həcmini aşağıda təqdim edilən düsturlar ilə hesabladıq:

Orta kvadratik xəta − MSE (Mean Square Error)

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(C_{i,j} - S_{i,j} \right)^2 \tag{1.3.6}$$

burada M təsvirin eni, N təsvirin uzunluğu, $C(i,j)$ konteyner təsvirinin i,j -ci elementi , $S(i,j)$ isə steqo−təsvirin i,j -ci elementidir.

Kökaltı orta kvadratik xəta − RMSE (Root Mean Square Error)

$$RMSE = \sqrt{MSE} \tag{1.3.7}$$

burada MSE – orta kvadrat səhv (yuxarıdakı kimi), RMSE – MSE-nin kvadrat kökü olub, səhvin ölçüsünü orijinal vahidlərdə göstərir və daha aydın və müqayisə edilə bilən nəticə verir.

Siqnalın küyə nisbəti − SNR (Signal To Noise Ratio)

$$SNR = 10 \times \log_{10} \left(\frac{\sum_{i=1}^{M \times N} (C_i)^2}{\sum_{i=1}^{M \times N} (C_i - S_i)^2} \right) \tag{1.3.8}$$

burada C_i – orijinal siqnalın i -ci elementi; S_i – təxmini siqnalın i -ci elementi, SNR – siqnalın səsə (error-a) nisbətini desibel (dB) ilə ölçür. Yüksək SNR daha yaxşı keyfiyyət deməkdir.

Pik siqnalın küyə nisbəti− PSNR (Peak Signal To Noise Ratio)

$$PSNR = 10 \times \log_{10}\left(\frac{Max^2}{MSE}\right) \tag{1.3.9}$$

burada Max – pikselin ala biləcəyi maksimum dəyərdir (məsələn, 8-bit təsvirlər üçün Max = 255), MSE – orta kvadrat səhvdir, PSNR – pik siqnal dəyəri ilə səhv nisbətini desibellə ölçür. PSNR yüksəkdirsə, şəkil keyfiyyəti daha yaxşıdır.

Struktur oxşarlıq indeksi ölçüsü −SSİM (Structural Similarity Index Measure)

$$SSIM(x,y) = \left(\frac{\left((2\cdot\mu_x\mu_y + C_1)\cdot(2\cdot\sigma_{xy} + C_2)\right)}{\left((\mu_x^2 + \mu_y^2 + C_1)\cdot(\sigma_x^2 + \sigma_y^2 + C_2)\right)}\right) \tag{1.3.10}$$

burada $\mu_x\mu_y -$ x və y təsvirlərinin orta (parlaqlıq) dəyərləri, σ_x^2, σ_y^2 – təsvirlərin dispersiyası (kontrast), σ_{xy} – təsvirlər arasındakı kovarians (struktur komponenti), C_1 və C_2 – sabitlərdir (sıfıra bölünmənin qarşısını almaq üçün), SSIM – iki təsvir arasındakı struktur, parlaqlıq və kontrast oxşarlığını 0 ilə 1 arasında ölçür. 1 – tam eynilik, 0 – heç bir oxşarlıq yoxdur.

Gizlədilmiş məxfi informasiyanın həcmi. Digər steqanoqrafik qiymətləndirmə parametri hər pikselə gizlədilən məxfi informasiya bitlərinin miqdarını göstərir.

$$EC = \frac{tutum}{W \times H} \tag{1.3.11}$$

burada W və H təsvirin eni və hündürlüyüdür.

Aparılan analizin nəticələri Cədvəl 1.3.1-də verilib.

Cədvəl 1.3.1

Müxtəlif interpolyasiya alqoritmlərinin analizi

İnterpolyasiya	**Gizlədilmə alqoritmi**	**Ümumi həcm (bit)**	**Faydalı yük, HC (bpp)**	**PSNR (dB)**	**MSE (dB)**	**SSIM (dB)**
NMI [43, s. 465-470]	Jung [43, s. 465-470]	385124	1,25	29,78	0,012	0,989
	Sabeen G.[88, s.20527-20545]	196608	0,75	47,69	0,016	0,925

Cədvəl 1.3.1-n ardı

İnterpolyasiya	Gizlədilmə alqor-itmi	Ümumi həcm (bit)	Faydalı yük, HC (bpp)	PSNR (dB)	MSE (dB)	SSIM (dB)
ENMİ [105, s. 603-606]	YaThink Chang [105, s. 603-606]	282237	1,06	41,24	0,003	0,949
	Sabeen G. [86, s. 1311-1316]	368557	1,43	30,79	0,023	0,986
INP [58, s. 6712-6716]	Lee [63, s. 6712-6716]	434425	1,6	29,09	0,011	0,973
NIE [18, s. 7181-7205]	Ahmad M. [23, s. 7181-7205]	445644	1,7	24,05	0,017	0,992
Sabeen [87, s. 300-314]	Sabeen G.[92, s. 300-314]	655365	2,5	30,10	0,001	0,989
NIE [18, s. 7181-7205]	Chen Y. [30, s.271-350]	438749	1,6	30,98	0,032	0,985
Jana B. [45, s 239-248]	Jana B. [50, s. 239-248]	778567	2.97	38,03	0,008	0,963

Cədvəldə ən yüksək ümumi həcm göstəricisi NIE [18, s. 7181-7205] interpolyasiya metodu əsasında təqdim edilən məxfi informasiya gizlədilmə alqoritmindədir. Burada ümumi həcm göstəricisi 445644-ə bərabərdir. Lakin, təsvirin vizual keyfiyyəti nəzərə çarpacaq dərəcədə aşağıdır (PSNR 24,05) və orta kvadratik xəta (MSE) qiymətinin qənaətbəxş olmasına baxmayaraq təsvirdə pozuntular daha çoxdur. Buradan belə nəticəyə gəlmək olar ki, vizual pozuntular təklif edilən alqoritmdə daha çox informasiyanın gizlədilməsini məhdudlaşdırır. Cədvəldə ən yüksək PSNR qiyməti Sabeen G. və digərlərinin ENMİ [105, s. 603-606] interpolyasiyası əsasında təqdim etdikləri məxfi informasiya gizlədilmə alqoritmindədir [88, s. 20527-20545]. Bu alqoritmdə təsvirin vizual keyfiyyəti yüksək olduğu halda (47,69) orta kvadratik xəta (MSE) təsvirdə pozuntuların çox olmasını göstərir (0,016), halbuki həmin cədvəldə göstərilən digər alqoritmdə [18, s. 7181-7205] PSNR 24,05 olduğu halda orta kvadratik xəta (MSE) 0,009 qiymətini

alıb. [23, s.271-350] də isə nisbətən yüksək PSNR (30,98) qiymətinin olmasına baxmayaraq, MSE daha aşağı keyfiyyət göstərir -0,032. Ədəbiyyatda istinad edilən bu tədqiqatlarda müəlliflər buna aid məlumat verməyiblər. Buna görə də, yeni alqoritmlər işlənilərkən burada əldə edilən nəticələr nəzərə alınmalıdır.

Bu fəsildə tədqiq edilən işlərin əksəriyyəti təsvirlərin interpolyasiyası metoduna əsaslanır. Çünki təsvir steqanoqrafiyasında məxfi informasiya bitləri bir başa təsvirin piksellərinə gizlədildiyi zaman ciddi vizual pozuntular yarana bilər. Bu problemin həlli olaraq mütəxəssislər təsvirləri interpolyasiya edərək xəyali piksellər yaradırlar və həmin piksellərdə məxfi informasiya bitlərini gizlədirlər. Bu zaman daha çox məxfi informasiya biti yerləşdirmək mümkün olur.

Əldə olunan yeni, hərtərəfli statistik göstəricilər dissertasiya işində nəzərdə tutulan tədqiqatların nəzəri bazasını təşkil edərək daha üstün keyfiyyətlərə malik yeni effektiv steqanoqrafik alqoritmlərin işlənilməsinə zəmin yaradır. Müəyyən edilib ki, alqoritmlərin əksəriyyəti təsvir interpolyasiya əsasında məxfi informasiyanın gizlədilməsi zamanı gizlədiləcək məxfi bitlərin sayını müəyyən etmək üçün piksellər arasındakı fərq qiymətlərinin loqarifması hesablanır və loqarifmin nəticəsinə əsasən gizlədiləcək bit sayı müəyyən edilir. Lakin loqarifmin hesablanması zamanı gizlədiləcək məxfi informasiya biti pikselin tutumundan daha az olur.

Təsvirlərin interpolyasiya metodu adətən təsvirlərin vizuallığını yaxşılaşdırmaq üçün istifadə edilir. Təsvir steqanoqrafiyasında isə təsvir interpolyasiya edilərkən ilkin təsvirdən müəyyən dərəcədə fərqlənir. Bu isə steqanoqrafik alqoritmin keyfiyyətini və steqoanaliz hücumlarına qarşı dayanıqlığını aşağı salır. Qoyulan məqsədə nail olmaq üçün prinsip etibarilə məxfi informasiya gizlədilməsinin yeni fərqli mexanizmləri üzərində işlər aparmaq üçün perspektiv istiqamətlər müəyyən edilib.

1.4. Məxfi informasiyanın gizlədilməsinin aktual problemlərinin müəyyən edilməsi

Steqanoqrafiya sahəsində məxfi informasiyaların gizlədilməsi üçün aktual elmi-tədqiqat problemlərinin [3, s. 51-55] – də hazırkı vəziyyəti geniş analiz edilimşdir.

Aparılan analizlər zamanı steqanoqrafiya sahəsində əsas aktual məsələlərə baxılmışdır. Bu məsələlərə istinadən qeyd etmək lazımdır ki, bu sahədə birinci aktual məsələ kimi konteynerə gizlədilmiş məxfi informasiyanın steqo-hücumlara qarşı dayanıqlı olması və aşkarlanmamasıdır. Çünki informasiya texnologiyaları inkişaf etdikcə yeni hücum növləri yaradılır və beləliklə, məxfi informasiyalar ələ keçirilir. Buna görə də, məxfi informasiyaların gizlədilməsi zamanı belə hücum növünə qarşı daha yüksək dayanıqlılıq təmin edilməlidir.

Bundan başqa məxfi informasiyanın konteyner içərisində gizlədilməsi zamanı konteynerdə müəyyən pozuntular baş verir. Bu da məxfi informasiyanın mövcudluğuna şübhə yaratmaqla yanaşı onun təhrif olunmasına və ələ keçirilməsinə şərait yaradır ki, bu da steqanoqrafiya sahəsində olan aktual məsələlərdən biridir.

Bəzən konteynerə böyük həcmdə məxfi informasiya gizlədilərkən konteynerdə ciddi pozuntular yaranır və yaxud məxfi informasiya bitləri tam yerləşmədiyi üçün təhrif olunur. Buna görə də, vizual pozuntunun az olması ilə böyük həcmdə məxfi informasiya bitlərinin yerləşdirilməsini təmin edən alqoritmlərin yaradılması da aktual məsələdir.

Yuxarıda göstərilən şərtlərin ödənilməsi zamanı alqoritmlərin hesablama mürəkkəbliyi onun realizə müddətinə təsir edir. Belə ki, hesablama vaxtı artır. Bu baxımdan alqoritmlərin sadə, lakin steqanoqrafiyanın əsas keyfiyyət göstəricilərinə uyğun olmasına ehtiyac var. Bu zaman az vaxt ərzində daha çox iş görmək mümkün olacaqdır.

Birinci fəsildə steqanoqrafiya sahəsinə aid alqoritmlər, onların qiymətləndirmə metodları və mövcud problemləri araşdırılıb. Qarşıya qoyulan məqsəd və həll edilməli olan problemlər məxfi informasiyanın rəqəmsal təsvirlərdə gizlədilməsi üçün daha effektiv alqoritmlərin yaradılmasıdır. Müəyyən edilən problemlər aşağıda göstərilib.

1. Steqo-təsvirdə məxfi informasiyanın aşkarlanmasının çətinləşdirilməsi. Konteynerdə məxfi informasiyanın gizlədilməsi olduqca əhəmiyyətli və bir o qədər də problemli məsələdir. Belə ki, steqanoqrafiya sahəsi inkişaf etdikcə, ona qarşı

hücum növləri də öz növbəsində inkişaf etdirilərək təkmilləşdirilir. Ona görə də, məxfi informasiyanın gizlədilməsi faktı, gizli saxlanılmaqla yanaşı, inkişaf etmiş hücum növlərinə qarşı da dayanıqlı olmalı [8, s. 366-370,] və məxfi informasiya üçüncü şəxslər tərəfindən aşkarlanmamalıdır [1, s.60-66].

2. Böyük həcmdə məxfi informasiyanın gizlədilməsi zamanı konteyner təsvir ilə steqo-təsvir arasındakı vizual fərqin minimum olması. Göndərilən məxfi informasiyanın tamlığının qorunması şərti ilə qarşı tərəfə təhrifsiz ötürülməsi olduqca əhəmiyyətli məsələdir. Əgər göndərilən məxfi informasiyanın həcmi böyük olarsa və seçilmiş konteynerin həcmi məxfi informasiyanın həcmindən kiçik olarsa və yaxud da konteynerə məxfi informasiya tam olaraq yerləşdirildikdə konteynerdə dağılmalar və vizual pozuntular baş verərsə, onda istifadə edilən alqoritm keyfiyyətsizdir və bu alqoritmin istifadə edilməsi məqsədəuyğun deyil [75, s. 329-333].

3. Yuxarıda göstərilən amillər nəzərə alınmaqla daha böyük həcmdə məxfi informasiya biti gizlətmək. Məxfi informasiyanın gizlədilməsi zamanı uyğun konteynerin seçilməsi qədər gizlədilmə alqoritmi də böyük əhəmiyyət daşıyır. Çünki seçilən konteynerin həcmi məxfi informasiyanın tam gizlədilməsinə imkan versə də, istifadə edilən alqoritmin düzgün olmaması konteynerdə pozuntular yarada bilər. Bundan başqa məxfi informasiyanın gizlədilməsi zamanı məxfi informasiya bitlərinin təhrif olunmasına gətirib çıxardır [11, s. 465-472].

4. **Konteyner təsvirə məxfi informasiyanın gizlədilməsi və steqo-təsvirdən məxfi informasiyanın çıxarılması üçün aparılan hesablamaların mürəkkəblik dərəcəsini aşağı salmaq.** Aparlan elmi-praktiriki tədqiqatlara nəzər yetirsək görərik ki, bəzən təklif edilən alqoritm dayanıqlığı, yüksək vizual keyfiyyəti və vizual oxşarlığı təmin etməsi ilə yanaşı mürəkkəb hesablamalar tələb edir. Belə olan halda alqoritmlərin realizə müddəti çox olur. Lakin daha sadə hesablamalar ilə daha yüksək dayanıqlılığa malik steqo-təsvir yaradılarsa, onda alqoritmin realizə müddəti azalar [10, s. 39-51, 11, s.465-472, 75, s. 329-333].

Birinci fəsil üzrə nəticələr

1. Dissertasiya işinə uyğun son illər ərzində yazılan məqalələrin icmalı aparılıb və yeni alqoritmlərin yaradılması üçün əsas istiqamətlər müəyyən edilib. Son illərin tədqiqatlarının nəticəsində müəyyən edilib ki, steqanoqrafiya sahəsində əsas nəzər yetirilməli olan istiqamətlər yaradılan alqoritmin steqo hücumlara qarşı dayanıqlı olması, steqo-təsvir ilə konteyner təsvir arasında vizual oxşarlığın tam olması, məxfi informasyanın steqo-təsvir içərisində aşkarlanmaması, məxfi informasiyanın təhrif olmadan yenidən bərpa edilməsi və bununla yanaşı, daha çox məxfi informasiya bitini bir konteyner içərisində gizlədə bilmək kimi göstricilər nəzərə alınmalıdır;
2. Steqanoqrafiya sahəsində xaricdə və ölkədə mövcud olan elmi tədqiqatların müasir vəziyyəti analiz edilib;
3. SIFT alqoritmi və onun tətbiq sahələri araşdırılıb. SIFT alqoritmlərinin steqanoqrafiyaya tətbiq olunması istiqamətləri müəyyən edilib;
4. Təsvir steqanoqrafiyası sahəsində mövcud olan məşhur metodlar, ən az əhəmiyyətli bitlərin əvəz edilməsi metodları və piksellərin fərqinə əsaslanan metodlar tədqiq edilib. Onların üstün və mənfi cəhətləri göstərilib və bu metodlar haqqında mövcud tədqiqatlar araşdılıb. Tədqiqatların nəticəsindən aydın olur ki, bu metodların birlikdə istfadə edilməsi daha effektiv metodların alınmasına gətirib çıxarda bilər;
5. Təsvir steqanoqrafiyası sahəsində təsvirlərin interpolyasiyasına əsaslanan metodlar araşdılıb. Bu metodlara aid bir neçə tədqiqatdan istinadlar verilib və onlar haqqında qısa icmal təqdim olunub. Onların nəticələri və tətbiq olunma sahələri göstərilib;
6. Steqoanaliz alqoritmləri araşdırılıb və bu alqoritmlər haqqında icmal təqdim edilib. Bunun nəitcəsində dissertasiya işində təklif edilən yeni alqoritmlərə uyğun olan steqoanaliz alqoritmləri müəyyən edilib;
7. Aparılın icmalın əsasında mövzunun işlənmə səviyyəsi və dissertasiya işində həll edilməli olan problemlər qoyulub [76, s.427-437];

8. Əsas istiqamət kimi sahə domeyin metodları və təsvirlərin interpolyasiyasına əsaslanan metodlar seçilib;
9. Analiz edilən alqoritmlərin statistik göstəriciləri oriyentir kimi müəyyən edilərək daha üstün keyfiyyətlərə malik alqoritmlərin yaradılması qarşıya məqsəd kimi qoyulub.

II FƏSİL. YENİ STEQANOQRAFİK ALQORİTMLƏRİN İŞLƏNİLMƏSİ

Bu fəsildə steqanoqrafiyanın əsas anlayışları və müddəalarının müzakirələri, rəqəmsal steqo-sistemlərin qurulması prinsiplərinin araşdırılması nəticəsində və əldə edilən biliklər əsasında yeni daha effektiv alqoritmlər təklif olunur.

Steqanoqrafik sistemlərin qurulmasında əsas prinsiplər steqo-təsvirlərin və konteyner təsvirlərin vizual olaraq fərqlənə bilməməsi, həmçinin məxfi informasiya bitlərinin gizlədilməsi həcminin artırılması və bütövlüyünün təmin olunmasıdır. Bütün bunlar nəzərə alınaraq bu keyfiyyətləri özündə birləşdirən, təklif edilən yeni alqoritmlərin izahı növbəti bölmələrdə geniş verilmişdir [4, s. 79-81].

Steqo-sistemlərin qurulması üçün keyfiyyət göstəricilərindən biri də məxfi informasiyanın konteyner təsvirə yerləşdirilməsi üçün istifadə edilən çətin riyazi hesablamaların daha asan üsullarla əvəz edilməsidir ki, bu da təklif edilən alqoritmlərdə öz əksini tapır. Eyni zamanda bu keyfiyyət göstəricisinin olması daha qısa müddətdə steqo-təsvirin emal edilməsini təmin edir.

Bu fəsildə sahə domen metodları üzərində qurulmuş yeni alqoritmlər təqdim olunur. Bizdən əvvəl təklif olunan metodlarla müqayisədə daha yüksək vizual keyfiyyətə, daha çox məxfi informasiya biti gizlətmək qabiliyyətinə və steqo-hücumlara qarşı dözümlü alqoritmlər işlənib. Təklif olunan hər alqoritmin yuxarıda qeyd olunan keyfiyyət paramterləri yoxlanılmış və üstün nəticələr əldə olunmuşdur.

Sahə domen metodları.

Məxfi informasiyanın konteyner təsvir içərisində yerləşdirilməsinin müxtəlif metod və alqoritmləri vardır. Bu alqoritmlər konteynerin seçilməsi, yaradılması və modifikasiya edilməsinə görə ayırd edilir. Konteynerin modifikasiya edilməsinə görə məxfi informasiyanın konteynerə yerləşdirilməsinin iki növü var: sahə domeni və tezlik domeni.

Təklif edilən alqoritmlərdə sahə domeni metodlarından istifadə edilmişdir. Sahə domeni metodunda məxfi informasiyanın konteyner təsvirə gizlədilməsi zamanı məxfi informasiya bitləri konteyner piksellərində hər hansı bir dəyişiklik edilmədən

bir başa yerləşdirilir. Yerləşdirilmənin isə bir neçə yolu vardır. Bizim istifadə etdiklərimiz LSB (ən az əhəmiyyətli bitin əvəz edilməsi) və PVD (piksellərin fərqinə əsaslanan yerləşdirmə) siniflərinə aid olan metodlardır [3, s. 51-55].

Ən az əhəmiyyətli bitin əvəz edilməsi (LSB) – bu zaman konteyner təsvir piksellərinin ən az əhəmiyyətli biti məxfi informasiya biti ilə əvəz olunur. LSB alqoritmi ilə məxfi informasiyanın gizlədilməsi geniş istifadə olunan alqoritm hesab edilir. Çünki, bu üsulda məxfi informasiya bitlərinin yerləşdirilməsi və steqo-təsvirdən həmin informasiyanın çıxarılma prosesi sadə və asandır. Bundan başqa, bu metodda konteyner təsviri çox az zədələnir ki, bu da onun keyfiyyət göstəricisinə demək olar ki, təsir etmir. LSB alqoritminə aid tədqiqatçılar tərəfindən geniş tədqiqatlar aparılmışdır. Bu alqoritmi bir neçə alqoritm ilə kombinə edərək yeni və daha effektiv nəticələr almaq mümkündür. Biz də təklif etdiyimiz yeni alqoritmlərimizdə LSB alqoritminin yeni modifikasiyalarından istifadə etmişik [75, s. 329-333].

Bundan başqa sahə domeni metoduna aid olan digər bir alqoritm isə piksellərin fərqinə əsaslanan PVD (pixel value difference) alqoritmidir. Bu alqoritm LSB alqoritmi ilə müqayisədə daha çox məxfi informasiya biti gizlətmə qabiliyyətinə malikdir.

LSB alqoritmində gizlədiləcək məxfi informasiya bitlərinin həcminin artması təsvirin vizual keyfiyyətinə təsir etdiyi halda PVD alqoritmlərində belə bir problem olmur. Belə ki, LSB alqoritmində konteyner təsvir pikselinin yalnız sonuncu ən az əhəmiyyətli bitlərini dəyişdirə bilərik ki, bu da maksimum 3 bit ola bilər. Əgər biz LSB alqoritmində daha çox bit gizlətmək istəsək, bu zaman təsvirin əhəmiyyət kəsb edən bitlərini dəyişdirmək məcburiyyətində qalarıq. Bu isə vizual keyfiyyətdə ciddi dəyişikliyə səbəb olar. Deməli, biz LSB alqoritmi ilə konteyner təsvirinin bir pikselinə yalnız 3 bit məxfi informasiya gizlədə bilərik. Buradan belə nəticəyə gəlirik ki, təsvirin vizual keyfiyyəti baxımından daha az məxfi informasiya gizlədilməlidir. Bu məsələnin həllini tapmaq üçün biz LSB alqoritmini PVD alqoritmi ilə birlikdə istifadə etdik. Bunun üçün PVD üzərində yeni modifikasiyalar aparılaraq uğurlu

nəticələr əldə edildi. LSB və PVD alqoritmi əsasında təklif etdiyimiz yeni effektiv alqoritmin geniş izahı növbəti bölmədə verilmişdir.

2.1. Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritmi

Bu bölmənin məqsədi böyük həcmdə məxfi informasiya gizlətmə qabiliyyəti, yüksək dayanıqlılıq və steqo-təsvirin vizual keyfiyyətinin qorunması prioriteti ilə məxfi informasiyaların gizlədilmə alqoritminin inkişafıdır. Eyni zamanda, təklif edilən alqoritm konteynerin yenidən bərpa olmasını da təmin edir. Problem iki mərhələdə həll olunur [75, s. 329-333]. İlk addımda məxfi informasiyanın gizlədilməsi üçün məxfi açara əsaslanan ən az əhəmiyyətli bitlərin dəyişdirilməsindən istifadə olunur [15, s. 582].

Ən az əhəmiyyətli bitin əvəz edilməsi (LSB) geniş istifadə olunan və həyata keçirilməsi sadə olan alqoritmdir. Lakin alqoritm diqqətsiz tətbiq olunarsa, məlumat itkiləri baş verir.

LSB alqoritmində təsviri təşkil edən hər baytın son bitlərini məxfi informasiya bitləri ilə əvəzləyirik. Son bitlərin əvəz edilməsi təsvirin əvvəlindən və ya sonundan ardıcıl olaraq edilə bilər, yaxud təsadüfi funksiya generatorundan istifadə edərək müəyyən edilmiş piksellərə tətbiq etməklə reallaşdırıla bilər.

Bəzən steqanoqrafik sistemlərdə gizli açarlardan da istifadə olunur. Bu açarlar aşağıdakı siniflərə bölünür:

Steqanoqrafik açarlar − məxfi informasiyanı təsvirə yerləşdirmək və steqo-təsvirdən məxfi informasiyanın çıxarılması prosesini idarə etmək üçün istifadə olunur.

Kriptoqrafik açarlar − məxfi informasiyanı təsvirə daxil etməzdən əvvəl şifrləmək və deşifrə etmək üçün istifadə olunur.

Son bitlərin dəyişdirilməsi faylın əvvəlindən sonuna qədər ardıcıl olaraq həyata keçirilir, lakin bu alqoritmdə steqo-açar vasitəsilə psevdo təsadüfi funksiya əsasında təsadüfi piksellər seçilir və məxfi informasiya həmin piksellərə gizlədilir. Steqo-

açardan istifadənin məqsədi təhlükəsizliyi artırmaqdır. Şifrənin açılması prosesi zamanı bu açar olmasa, məxfi informasiya əldə edilə bilməz.

İkinci mərhələdə, daxil edilən konteyner təsvir 2x2 bloklara bölünür və hər blok daxilində ən kiçik piksel seçilir. Daha sonra qalan üç piksel və ən kiçik piksel arasındakı fərq hesablanır. Yaranan fərqin onluq say sistemində olan qiymətləri ikilik say sisteminə çevrilir. Təklif edilən alqoritmdə bu əməliyyat konteyner təsvirin bütün 2x2 blokları üzrə aparılır. Sonra minimum piksellər istisna olmaqla psevdo təsadüfi seçilmiş piksellərin ən az əhəmiyyətli bitləri məxfi informasiya biti ilə əvəzlənir. Daha sonra həmin piksel qiymətləri yenidən 10-luq say sisteminə çevrilərək minimum qiymətlə cəmlənir. Beləlikə, bütün məxfi informasiya bitləri konteyner təsvirinin 2x2 bloklarındakı minimum pikselləri istisna olmaqla ixtiyari seçilmiş piksellərinə gizlədilərək steqo-təsviri əmələ gətirir. Məxfi informasiya bitlərinin gizlədilməsi və yenidən bərpa edilməsi steqo-açar vasitəsilə həyata keçirilir.

Məxfi informasiyanın gizlədilməsi təsadüfi piksellərdə olduğu üçün məxfi informasiya bitlərinin bərpası yalnız açar ilə mümkündür. Əks halda məxfi informasiya bitləri ardıcıl gizlədilmədiyi üçün sadəcə məxfi informasiyanın bitləri xaotik sürətdə əldə edilir ki, bu da məxfi informasiyanın təhrif olunmuş forması olur.

Yeni alqoritmin məqsədi daha yüksək dayanıqlılıq qabiliyyətinə və ilkin təsvirin minimal təhrifinə nail olmaqla steqo-təsviri yaratmaqdır.

Təklif olunan alqoritmin daha ətraflı izahı növbəti bölmədə verilir.

Məxfi informasiyanın konteyner təsvirinə gizlədilməsi prosesi.

Addım 1. Burada N - mövcud konteyner bitlərinin sayı P_0^N və 0-dan $N-1$-ə qədər olan ədədlərin permutasiyası olsun. Eyni zamanda, məxfi informasiya bitlərini yerləşdirəcəyimiz piksellər isə $P_0^N(0), P_0^N(1), \ldots\ldots P_0^N(n-1)$ olsun.

İstifadə edəcəyimiz permutasiya funksiyası, gizli K açarına bağlı və təsadüfi olmalıdır. Çünki seçilən bitlər təsadüfi seçilməlidir. Bunun nəticəsində məxfi informasiya bitləri konteynerin içərisində yayıla biləcəkdir. Bunun üçün psevdo təsadüfi permutasiya generatoru olmalıdır. Bu funksiyada K açarı giriş qiyməti olaraq daxil olur və $\{0,\ldots N-1\}$ arasında fərqli nəticələr alır. Bu prosesdə K gizli

açarını bilmədən heç kim məxfi informasiya bitinin harada gizlədildiyini təxmin edə bilməz.

Addım 2. Psevdo təsadüfi permutasiya generatoru yaratmaq üçün psevdo təsadüfi funksiya istifadə edilə bilər. Bunun üçün K gizli açarı ilə $i\{i=0,...n-1\}$ arqumenti sıralanaraq hər hansı bir təhlükəsiz heş funksiyası H ilə asanlıqla edilə bilər

$$f_K(i)=H(K\circ i) \qquad (2.1.1).$$

Burada $(K\circ i)$, K açarı ilə i arqumentinin sıralanmasıdır. Beləliklə, K parametrinə bağlı olan bir $f_K(i)$ psevdo təsadüfi funksiyasını əldə etmiş oluruq.

Psevdo təsadüfi permutasiya generatoru üçün a və b-nin bit və bit 2 moduluna görə cəmi (XOR) və nəticənin a-nın ölçüsünə bərabər olduğu əməliyyatı müəyyən etmək lazımdır$(a\oplus b)$.

Addım 3. Əldə olan $2l$ uzunluğundakı i ikilik say sistemində olan arqumenti $X(sonl)$ və $Y(ilkl)$ olan, l uzunluğuna sahib iki hissəyə bölünür. K açarı da K_1,K_2,K_3,K_4 olaraq 4 hissəyə bölünür.

Addım 4. Aşağıdakı alqoritmin 2^{2l-1} dəfə təkrar işləməsi ilə $\{0,.....2^{2l-1}\}$in psevdo təsadüfi permutasiyası alınır.

$$\begin{aligned} &Y=Y\oplus f_{K1}(X)\\ &X=X\oplus f_{K2}(Y)\\ &Y=Y\oplus f_{K3}(X)\\ &Y=X\oplus f_{K4}(Y)\\ &geri dönüş\ X\circ Y \end{aligned} \qquad (2.1.2)$$

Addım 5. Təkrar edilən X və Y qiymətləri məxfi informasiya bitinin gizlədiləcəyi koordinatları verir.

$$\begin{aligned} &Y=i\ div\ x\\ &X=i \bmod x\\ &Y=(Y+f_{K1}(X)) \bmod y\\ &X=(X+f_{K2}(Y)) \bmod x\\ &Y=(Y+f_{K3}(X)) \bmod y\\ &sonda\ Y*x+X \end{aligned} \qquad (2.1.3)$$

Addım 6. İlkin təsvir 2x2 bloklara bölünür, onların daxilində ən aşağı qiyməti olan piksel, minimal piksel olaraq təyin olunur (şəkil 2.1.1).

I_{11}	I_{12}
I_{21}	I_{22}

Şəkil 2.1.1. Konteyner təsvir bloku

Addım 7. Digər 3 pikselin hər birindən ən kiçik pikselin qiyməti çıxılır. (2.1.4) düsturundan istifadə edərək $D(i,j)$fərq qiyməti hesablanır

$$D(i,j)=I(i,j)-\min \quad (2.1.4)$$

Addım 8. Onluq say sistemində olan $D(i,j)$fərq qiyməti ikilik say sisteminə çevrilir.

Addım 9. Bu addımda məxfi informasiya bitləri, təsadüfi yolla seçilmiş konteyner təsvirinin pikselinin ikilik say sistemində olan $D(i,j)$fərq qiymətlərinin ən az əhəmiyyətli bitləri (LSB) ilə əvəz edilərək gizlədilir.

Addım 10. LSB əməliyyatı tamamlandıqdan sonra hər blokda təyin edilən minimum qiymətlər yenidən digər piksellər ilə cəmlənir.

Məsələnin həllinin ədədi nümunəsi növbəti bölmədə verilmişdir.

Təklif olunan alqoritmin rəqəmsal nümunəsi.

Tutaq ki, konteyner təsvirin ölçüsü 900x700-dür. 2 Kb məxfi informasiyanın 400 bitini gizlədəcəyimiz koordinatları təyin edək.

Konteyner təsvirin piksellərinin ümumi bitlərinin sayı $N=630000$, məxfi informasiyanın ümumi bitlərinin sayı 2048x8=16384, gizli açarın qiymətləri $K_1=123,\ K_2=456,\ K_3=789$, təsvirin ölçüləri $x=900,\ y=700$ olsun. Məxfi informasiyanın 400 bitini gizlədəcəyimiz təsvirdəki pikselin koordinatını tapmaq üçün aşağıdakı əməliyyatları aparmalıyıq:

$$Y = 400 \ \ div \ \ 900 = 0$$
$$X = 400 \ \ \text{mod} \ \ 900 = 400$$
$$Y = \left(0 + H\left(123 \circ 400\right)\right) \text{mod} \ \ 700 = 491$$
$$X = \left(400 + H\ \left(456 \circ 491\right)\right) \text{mod} \ \ 900 = 435$$
$$Y = \left(491 + H\ \ \left(789 \circ 435\right)\right) \text{mod}\, 700 = 557$$
$$Y * x + X = 557 * 900 + 435$$

Beləliklə, məxfi informasiyanın 400 bit y koordinatı 557, x koordinatı 435 olan piksel müəyyən edilir. Piksellər bütün təsvir boyunca bu ardıcıllıq ilə təyin edildikdən sonra, konteyner təsvir 2x2 bloklara bölünür (şəkil 2.1.2). Məxfi steqo-açar ilə təyin edilən hər bir piksel 2x2 bloklarındakı minimum piksel ilə müqayisə edilir. Əgər həmin piksel minimum piksel deyilsə, onda minimum piksel digər piksellərdən çıxılır.

60	85
103	93

Şəkil 2.1.2. Konteyner təsvir bloku

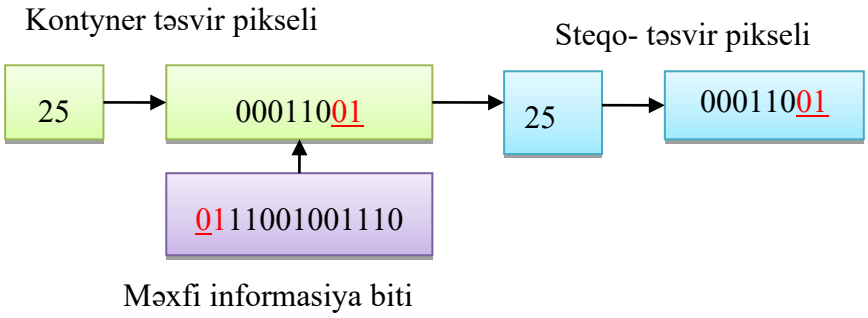
Burada minimum piksel 60-dır. Blokun açar ilə təyin edilən piksellərindən minimum qiymət çıxılır. Tutaq ki, bir blokdan aşağıda göstərilən 3 piksel təyin edilib, onda

$$D_{12} = 85 - 60 = 25$$
$$D_{21} = 103 - 60 = 43$$
$$D_{22} = 93 - 60 = 33$$

Açar ilə təyin edilən piksellərin fərq qiymətləri ikilik say sisteminə çevrilir.

$$D_{12} = 25_{10} = 11001_2$$
$$D_{21} = 43_{10} = 101011_2$$
$$D_{22} = 33_{10} = 100001_2$$

Məxfi informasiya bitləri B1=01110010011100..... kimi verilir və yuxarıdakı ardıcıllığa uyğun olaraq LSB alqoritmi ilə iki ədəd məxfi bit giriş təsvirinin müvafiq ən az əhəmiyyətli bitlərinə daxil edilir (şəkil 2.1.3).



Şəkil 2.1.3. Məxfi informasiya gizlədilmə prosesinin ədədi nümunəsi.

Daha sonra minimum piksellər yenidən digər 3 piksel ilə toplanır.

$$s_{12} = 25 + 60 = 85$$
$$s_{21} = 43 + 60 = 103$$
$$s_{22} = 32 + 60 = 92$$

Beləliklə, aşağıda təsvir olunan steqo-pikselləri alırıq (şəkil 2.1.4)

60	85
103	92

Şəkil 2.1.4. Steqo– piksellər

Konteyner təsvir pikselləri ilə steqo-təsvir piksellərini müqayisə edərkən onların arasında fərqin çox kiçik olduğunu görürük. Bu o deməkdir ki, aralarında çox kiçik fərq var, ona görə də PSNR çox yüksəkdir.

Məxfi informasiyanın steqo-təsvirdən çıxarılma prosesi.

Addım 1. Əvvəlcə steqo-açar ilə məxfi informasiya biti gizlədilmiş piksellər müəyyən edilir. Steqo–təsvir 2x2 bloklara bölünür və blokun minimum pikseli müəyyən edilir (şəkil 2.1.5)

S_{11}	S_{12}
S_{21}	S_{22}

Şəkil 2.1.5. Steqo-təsvir bloku

Addım 2. Steqo-pikseldən minimum piksel çıxılır s_{12}, s_{21}, s_{22}

$$D'(i,j) = S(i,j) - \min \qquad (2.1.5.)$$

Addım 3. Hesablanmış $D'(i,j)$ fərq qiyməti ikilik say sisteminə çevrilir.

Addım 4. Əldə edilən ikilik say sistemində olan fərq qiymətindən ən az əhəmiyyətli bitlər seçilir. Seçilmiş rəqəmsal bitlər ardıcıl olaraq düzülür və beləliklə, məxfi informasiya bitləri yenidən əldə edilir.

Rəqəmsal nümunə.

2x2 ölçüdə olan təsvir blokunun rəqəmsal nümunəsi şəkil 2.1.6-da göstərilib;

60	85
103	92

Şəkil 2.1.6 Steqo-təsvir bloku

$$D'_{12} = 85 - 60 = 25$$
$$D'_{21} = 103 - 60 = 43$$
$$D'_{22} = 92 - 60 = 32$$

Hesablanmış fərq qiymətləri ikilik say sisteminə çevrilir.

$$D'_{12} = 25_{10} = 11001_2$$
$$D'_{21} = 43_{10} = 101011_2$$
$$D'_{22} = 33_{10} = 100001_2$$

Sonra hər pikselin son ən az əhəmiyyətli biti 2 seçilir və ardıcıl düzülür. Beləliklə, B1=01110010011100 kimi bit ardıcıllığını əldə edirik ki, bu da məxfi informasiya bitləri ardıcıllığıdır.

2.2. Təsvir interpolyasiyasına əsaslanan məxfi informasiya gizlədilmə alqoritmi

Kompüter steqanoqrafiyası sahəsində aparılan bir çox tədqiqatlar da ilkin təsvir interpolyasiya edilərək konteyner təsvirə çevrilir [107, s. 9195-9218]. Yaradılan konteyner təsvirin içərisinə məxfi informasiya bitləri gizlədilir.

Təsvirin interpolyasiya edilməsinə əsaslanan metodlara misal kimi 1-ci fəsildə müzakirə edilən metodları göstərə bilərik. Ədəbiyyatlarda təklif edilən interpolyasiya metodlarının tətbiqi zamanı yaradılan konteyner təsvir içərisinə gizlədiləcək məxfi

informasiya bitlərinin sayını müəyyən etmək üçün məxfi informasiya biti gizlədiləcək pikselin və ya onun fərq qiymətinin loqarifması hesablanır. Yəni, gizlədiləcək məxfi informasiya bitlərinin miqdarı Hartli düsturu ilə müəyyən edilir. Alınan nəticə konteyner pikselinə gizlədiləcək məxfi informasiya bitinin sayını müəyyən edir.

Hartli düsturuna əsasən məxfi informasiya bitlərinin gizlədilməsinə aid bir neçə interpolyasiya əsaslı steqanoqrafik alqoritmlər var. Belə alqoritmlərə misal kimi [43, s. 465-470, 35, s. 271-350] ədəbiyyatda verilən tədqiqatları göstərə bilərik.

Konteyner pikselinə gizlədiləcək məxfi informasiya bitinin sayını müəyyən etmək üçün Hartli düsturundan istifadə edilməsi gizlədiləcək bit sayını müəyyən dərəcədə aşağı salır. Gizlədiləcək məxfi informasiya bitlərinin sayını artırmaq məqsədilə yeni alqoritm təklif edirik. Yeni alqoritmdə gizlədiləcək məxfi informasiya bitinin sayını artırmaq məqsədilə konteyner pikselləri üzərində müəyyən hesablamalar apardıqdan sonra əldə edilən qiymətlərin ikilik say sistemində göstərilməsi və alınan bit düzümündəki bitlərin sayı ilə məxfi informasiya bitlərinin sayının müəyyən edilməsi təklif olunur.

Bunun üçün təsvirin piksel qiymətləri 10-luq say sistemindən ikilik say sisteminə çevrilir. Bu zaman alınan bit düzümündəki bitlərin sayına əsasən məxfi informasiya bitləri düzümündən bitləri ardıcıl seçirik və seçilmiş məxfi informasiya bitlərini onluq say sisteminə çevirərək təklif edilən alqoritmə əsasən piksel qiyməti ilə toplayırıq.

Misal üçün konteyner təsvirinin piksel qiyməti 2 olduğu hala baxaq. Tutaq ki, məxfi informasiya bitləri B=1110110101011..... kimi verilib. Pikselin qiyməti 2 olduqda o, binar sistemdə 10-a bərabər olur. 0 və 1-in ümumi sayı 2-yə bərabərdir, buna əsasən məxfi informasiya biti düzümündən iki bit, məsələn ilk iki bit "11" seçilir və 10-luq sistemə çevrilir $11_2=3_{10}$. Daha sonra piksel qiymətinin 10-luq sistemdəki 2 qiyməti ilə toplanır s=2+3=5.

Bu bölmədə təsvirin interpolyasiyasına əsaslanan məxfi informasiya gizlətmək üçün yeni alqoritm təklif edilir. Alqoritmin üstünlüyü təsvirin vizual keyfiyyətini təmin etməklə böyük həcmdə məxfi informasiya bitini gizlətməkdir.

Təklif olunan üsul aşağıdakı mərhələlərdən ibarətdir:

- təsvirin kiçildilməsi
- təsvirin genişləndirilməsi
- məxfi informasiyanın gizlədilməsi
- məxfi informasiyanın steqo-təsvirdən çıxarılması

Təklif edilən alqoritmdə məxfi informasiyanın gizlədilməsi prosesi.

Məxfi bitlərin gizlədildiyi alqoritmin rəqəmsal tətbiqi və təsvirin işlənməsi üçün əməliyyatların addım–addım icrası aşağıda verilmişdir.

Addım 1. İlkin təsvir 3x3 ölçüdə bloklara bölünür və interpolyasiya olunur. Bu məqsədlə düstur 2.2.1. istifadə olunur.

$$\begin{aligned} &C(0,0) = O(0,0) \\ &C(0,1) = (O(0,0) + O(0,2))/3 + (O(2,0) + O(2,2))/6 \\ &C(1,0) = (O(0,0) + O(2,0))/3 + (O(0,2) + O(2,2))/6 \\ &C(1,1) = (O(0,0) + O(0,2) + O(2,0) + O(2,2))/4 \end{aligned} \tag{2.2.1}$$

Burada $O(i,j)$ilkin təsvirin pikselləri, $C(i,j)$isə interpolyasiya ilə yaradılan konteyner təsvirin pikselləridir.

Addım 2. Yaradılan konteyner təsvir 2x2 bloklara bölünür. Təklif olunan məxfi informasiya gizlətmə alqoritminə əsasən, məxfi informasiya bitləri blokun yuxarı sağ hissəsində, solda aşağı hissəsində və sağda aşağı hissəsində yerləşən piksellərə gizlədilməlidir. Koordinatlara əsasən (2.2.2) düsturu istifadə edərək piksellər arasında fərq qiymətləri hesablanır.

$$\begin{aligned} d_1 &= \max\left(\left|C_1(0,1) - C_1(0,0)\right|, \left|C_1(0,1) - C_2(0,0)\right|\right), \\ d_2 &= \max\left(\left|C_1(1,0) - C_1(0,0)\right|, \left|C_1(1,0) - C_3(0,0)\right|\right), \\ d_3 &= \max\left(\left|C_1(1,1) - C_1(0,0)\right|, \left|C_1(1,1) - C_2(0,0)\right|, \left|C_1(1,1) - C_3(0,0)\right|, \left|C_1(1,1) - C_4(0,0)\right|\right) \end{aligned} \tag{2.2.2}$$

Addım 3. Hər bir pikselə daxil ediləcək məxfi bitlərin sayını müəyyən etmək üçün fərq qiymətlərini hesabladıqdan sonra hesablamalardan əldə edilən nəticələrin onluq say sistemində olan qiymətləri ikilik say sisteminə çevrilir. İkilik say sistemində olan qiymətlərdəki 1-lər və 0-ların ümumi sayı konteyner pikselinə daxil ediləcək məxfi bitlərin sayını müəyyən edir.

Addım 4. Addım 3-də bir pikselə daxil ediləcək məxfi bit sayları müəyyən edildikdən sonra (2.2.3) düsturundan istifadə etməklə konteyner pikselinə məxfi bitlər gizlədilir

$$S_1(0,1)=\begin{cases}C_1(0,1)+b_1, C_1(0,1)\le O_1(0,1)\\ C_1(0,1)-b_1\end{cases}$$
$$S_2(1,0)=\begin{cases}C_1(1,0)+b_2, C_1(1,0)\le O_1(1,0)\\ C_1(1,0)-b_2\end{cases} \quad (2.2.3).$$
$$S_3(1,1)=\begin{cases}C_1(1,1)+b_3, C(1,1)\le O_1(1,1)\\ C_1(1,1)-b_3\end{cases}$$

Burada C konteynerin pikselləri, S steqo-təsvirin pikselləri, b_1, b_2, b_3 isə məxfi informasiya bitləridir (Şəkil 2.2.1.).

S(0,0)	S(0,1)
S(1,0)	S(1,1)

C(0,0)	C(0,0)
C(0,0)	C(0,0)

Şəkil 2.2.1. (a) Steqo-təsvir (b) Konteyner təsvir

Digər tədqiqatlarda təklif olunan Hartli düsturu ilə məxfi informasiya gizlədilməsi təklif edilən alqoritmdə qeyd olunduğu kimi, onluq say sistemində alınmış qiymətləri binar sistemə çevirməklə əvəz etdikdə, konteyner təsvirinin pikselinə gizlədiləcək məxfi informasiya bitlərinin sayı daha çox olur ki, bu da yerləşdirmə həcminin artması deməkdir. Bundan başqa, ilkin təsvir ilə steqo-təsviri müqayisə etdikdə dəyişikliyinin az olması səbəbindən PSNR qiymətləri yüksək olur.

Bu tip məxfi informasiyanın gizlədilməsi alqoritmi daşmaya və ya azalma problemlərinə səbəb ola bilər. Konteynerdə bütün dəyərlərin '0' olduğu bir yerləşdirmə xəritəsi (location map) təyin olunur. Daxil edilmiş piksellər 255-dən böyük olarsa, həmin konteyner pikselləri dəyişməz saxlanılır və məlumatlar bu piksellərə daxil edilmir. Bu vəziyyət nadir hallarda baş verdiyi üçün yerləşdirmə xəritəsini sıxlaşdırmaq üçün hesab kodlaşdırma (arithmetic coding) alqoritmi istifadə olunur. Sıxılmış yer xəritəsini isə sonuncu sətir və sonuncu sütundakı piksellərə yerləşdirmək üçün LSB əvəzetmə alqoritmindən istifadə olunur. Qeyd etmək lazımdır

ki, bir LSB piksel əksər hallarda sıxılmış yerləşdirmə xəritəsini daşımaq üçün kifayətdir, lakin bəzi ekstremal hallarda daha uzun sıxılmış yer xəritəsini daşımaq üçün ən çox 5 LSB və ya daha çox piksel istifadə edilə bilər.

Məxfi informasiyanın gizlədilməsinin rəqəmsal nümunəsi.

Tutaq ki, ilkin təsvirin 3x3 ölçüdəki bloku aşağıdakı kimidir (şəkil 2.2.2.)

73	75	70
75	77	93
71	72	92

Şəkil 2.2.2. İlkin təsvir və ilkin təsvir bloku

İlkin təsvir (2.2.1) düsturundan istifadə edərək interpolyasiya yolu ilə konteyner təsvirə çevrilir.

$$C(0,0) = 73$$
$$C(0,1) = (73+70)/3 + (71+92)/6 = 74,7$$
$$C(1,0) = (73+71)/3 + (70+92)/6 = 75$$
$$C(1,1) = (73+70+71+92)/4 = 76,5$$

Sonra d_1, d_2, d_3 fərq qiymətləri hesablanır.

$$d_1 = \max(|75-73|, |75-70|) = 5$$
$$d_2 = \max(|75-73|, |75-71|) = 4$$
$$d_3 = \max(|77-73|, |77-70|, |77-71|, |77-92|) = 15$$

Hesablanmış fərq qiymətləri aşağıdakı kimi ikilik say sisteminə çevrilir.

$$n_1 = 5_{(10)} = 101_{(2)}$$
$$n_2 = 4_{(10)} = 100_{(2)}$$
$$n_3 = 15_{(10)} = 1111_{(2)}$$

d fərq qiymətlərini ikilik say sisteminə çevirdikdən sonra, n-nin bit düzümündəki bitlərin sayı qədər məxfi informasiya bitləri seçilir. Misal üçün məxfi informasiya bitləri B=11001100111100011 olduğunu fərz edək. $n_1 = 5_{(10)} = 101_{(2)}$ qiymətinin bit düzümündəki bitlərin sayı 3-ə bərabərdir, buna görə B-nin ilk 3 məxfi informasiya biti seçilir. Seçilən bitlər onluq say sisteminə çevirilir $b1 = 6$. Sonra

növbəti mərhələdə konteynerin pikselləri və ilkin təsvir pikselləri arasında müqayisə aparılır. Əgər konteynerin pikselləri ilkin təsvirin piksellərindən azdırsa, seçilmiş məxfi bitlər konteynerin pikselinə əlavə olunur. Əks halda, seçilmiş məxfi bitlər konteyner pikselindən çıxarılır. Bu konteyner təsvir ilə steqo-təsvir arasında oxşarlığın maksimum olmasına gətirib çıxarır ki, bu da PSNR-də artım deməkdir.

Hesablama aşağıdakı kimi aparılır.

$$S_1 = 74{,}7 + 6 = 80{,}7$$
$$S_2 = 75 + 3 = 78$$
$$S_3 = 76{,}5 + 3 = 79{,}5$$

Beləliklə, aşağıdakı kimi steqo-təsvir bloklarını almış oluruq (şəkil 2.2.3.)

73	81
78	80

Şəkil 2.2.3. Steqo-təsvir və steqo-təsvir bloku

Konteynerin piksellərini və steqo-təsvirin piksellərini müqayisə etsək, piksellər arasında çox az fərq olduğunu görərik. Bir çox tədqiqatda informasiyanın gizlədilməsi prosesində istifadə olunan Hartli düsturunun bizim təklif etdiyimiz ikilik say sistemindəki bit düzümlərinin sayının əsasında gizlədiləcək məxfi informasiya bitinin sayının müəyyən edilməsi, konteyner təsvirə daxil ediləcək məxfi informasiya bitlərinin sayını artırır. Bu da gizlədiləcək məxfi informasiyanın həcminin artması deməkdir və bu tədqiqatın əsas vəzifəsi olan digər alqoritmlərlə müqayisədə təklif olunan alqoritmin üstünlüyü hesab edilir.

Məxfi informasiyanın steqo-təsvirdən çıxarma mərhələsinin addımları

Steqo-təsvirdən məxfi informasiyanın çıxarılması alqoritmi, gizlədilmə alqoritminin əksi olmaqla, məxfi informasiyanı çıxarmaq və ilkin təsviri bərpa etmək üçün istifadə olunur.

Addım 1. Steqo−təsvir 2x2 bloklara bölünür və interpolyasiya edilmiş konteyner hər bir blokun ilk dəyərinə uyğun olaraq yenidən qurulur və C təsviri 2×2 ölçülü bloklara bölünür.

Addım 2. Steqo−təsvir pikselləri ilə konteyner təsvir piksellərinin fərqi hesablanır

$$\begin{aligned} De1 &= S(1,2) - C(1,2) \\ De2 &= S(2,1) - C(2,1) \\ De3 &= S(2,2) - C(2,2) \end{aligned} \qquad (2.2.4)$$

Məxfi informasiya bitləri bu fərq qiymətləri əsasında bərpa edilir.

Məxfi informasiya bitlərinin steqo-təsvirdən çıxarılma mərhələsinin rəqəmsal nümunəsi.

Konteyner və steqo-təsvirin 2x2 ölçüdə olan bloklarının rəqəmsal nümunəsi şəkil 2.2.4.-də göstərilib.

73	75
75	77

73	81
78	80

Şəkil 2.2.4. Konteyner təsvir Steqo-təsvir

Steqo-təsvir pikselləri ilə konteyner təsvirinin pikselləri arasında fərq hesablanır

$$81_{10}\text{-}75_{10}=6_{10}=110_2$$

$$78_{10}\text{-}75_{10}=3_{10}=11_2$$

$$80_{10}\text{-}77_{10}=3_{10}=11_2$$

Yuxarıdakı fərqdən alınan qiymətlər ardıcıl düzülür və beləliklə, məxfi informasiya bitlərini yenidən bərpa etmiş oluruq.

2.3. Kvorum funksiyasına əsaslanan informasiya gizlədilmə alqoritmi

Məlum olduğu kimi steqanoqrafiyanın əsas şərtlərindən biri odur ki, ilkin təsvir ilə içərisinə məxfi informasiya gizlədilmiş steqo-təsvir arasında vizual oxşarlıq maksimum olmalıdır. Lakin ilkin təsvir üzərində aparılan hər bir dəyişiklik onun

vizual dəyişməsinə səbəb olur. Eyni zamanda ilkin təsvirin interpolyasiya edilərək konteyner təsvirinin yaradılması zamanı da ilkin təsvir üzərində aparılan əməliyyatlar onun müəyyən dərəcədə dəyişilməsinə səbəb olur. Dəyişilmənin səbəbindən ilkin təsvir və steqo-təsvir arasında hesablanan PSNR qiymətləri aşağı olur. Steqo-təsvirdən məxfi informasiya çıxarıldıqdan sonra konteyner təsvirin yenidən bərpa olunması üzrə aparılan tədqiqatlar PSNR və daha çox məxfi informasiya gizlətmə qabiliyyəti baxımından bir-birindən fərqlənən bir çox işlərə həsr edilmişdir. Bu bölmədə təklif etdiyimiz alqoritm mövcud oxşar alqoritmlər ilə müqayisədə yuxarıda qeyd olunan göstəricilər (PSNR və HC) üçün yaxşı nəticələr verir.

Məxfi informasiyanı göndərən tərəf onu konteyner içərisinə gizlətməzdən əvvəl AES alqoritmi ilə şifrləyir. Şifrlənmiş məxfi informasiya bitləri kvorum funksiyası əsasında təklif edilən yeni alqoritm ilə konteyner təsvirinə gizlədilir və beləliklə steqo-təsvir yaranmış olur.

Məxfi informasiyanın steqotəsvirdən çıxarılması prosesi isə gizlədilmə alqoritminin əksi olan alqoritmdən istifadə olunaraq həyata keçirilir. Təklif olunan alqoritm ilkin təsvirin vizual keyfiyyətinə təsir etmədən məxfi informasiyaların daxil edilməsini və ilkin təsvirin yenidən bərpa olunmasını təmin edir.

Aşağıda təqdim edilən bölmələrdə təklif olunan alqoritmin daha geniş izahı, yəni məxfi informasiyanın konteyner təsvirinə gizlədilməsi və yaradılmış steqo-təsvirdən məxfi informasiyanın çıxarılma prosesinin addımları göstərilmişdir.

İşlənilib təklif edilən 3 girişli kvorum funksiyası əsaslı informasiya gizlətmə alqoritminin steqo-hücumlara dayanıqlığını, yəni təhlükəsizliyini təmin etmək məqsədilə məxfi informasiyanın şifrlənməsindən istifadə edilib. Şifrlənmə kriptoqrafiyada özünə geniş yer tapmış AES şifrləmə standartı ilə aparılıb.

AES əsasında məxfi informasiyanı aşağıda göstərilən ardıcıllıqla şifrləyirik:

Şifrləmə addımları.

Məxfi informasiya bitinin ilkin bloku $A(x)$ massivi şəklində verilmişdir və $C(x)$ açar massivimiz var. Bu işdə 128 bit açarın istifadəsi kifayət edir. Bildiyimiz kimi 128 bit açar istifadə edilən zaman dövrlərin sayı 10 olur.

Addım 1. Açarın əlavə edilməsi. $A(x)$ massivi ilə $C(x)$ açar massivinin 2 moduluna görə cəmi (XOR) hesablanır.

$$A(x)=\begin{bmatrix} 32 & 88 & 31 & e0 \\ 43 & 5a & 31 & 37 \\ f6 & 30 & 98 & 07 \\ a8 & 8d & a2 & 34 \end{bmatrix} \qquad C(x)=\begin{bmatrix} 26 & 28 & ab & 09 \\ 7e & ae & f7 & cf \\ 15 & d2 & 15 & 4f \\ 16 & a6 & 88 & 3c \end{bmatrix}$$

$$A(x)=A(x)\oplus C(x)$$

$$A(x)=\begin{bmatrix} 19 & a0 & 9a & e9 \\ 3d & f4 & c6 & f8 \\ 3e & e2 & 8d & 48 \\ be & 2b & 2a & 08 \end{bmatrix}$$

Addım 2. Baytların əvəz edilməsi. Əldə edilən $A(x)$ massivi baytların əvəz edilməsi prosesində istifadə edilir. Bunun üçün bizə S-bloku lazımdır. S -blokundakı elementlər ilə $A(x)$ massivinin elementləri əvəzlənir. S-bloku şəkil 2.3.1. də verilib.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Şəkil 2.3.1. S-bloku

$A(x)$ massivinin birinci elementi 19-dur. Bu element S-blokunun 1-ci sətri ilə 9-cu sütununun kəsişməsində duran elementlə əvəz edilir. Əvəzetmə prosesi bu şəkildə $A(x)$ massivinin bütün elementlərinə tətbiq olunur və növbəti addıma keçirilir.

Addım 3. Sətirlərin sürüşdürülməsi. $A(x)$ massivinin axırıncı üç sətri müxtəlif sayda baytlarla dövri sürüşdürülür. Sətr 1-C_1 bayt, sətr 2-C_2 bayt, sətr 3-C_3 bayt sürüşdürülür. C_1 C_2 C_3 sürüşmələrinin qiyməti blokun uzunluğu N_b-dən asılıdır.

Axırıncı üç sətrin sürüşməsi əməliyyatı **ShiftRows (State)** kimi işarə edilir. Beləliklə, $A(x)$ massivinin elementləri aşağıdakı kimi olacaq.

$$A(x)=\begin{bmatrix} d4 & e0 & b8 & le \\ bf & b4 & 41 & 27 \\ 5d & 52 & 11 & 98 \\ 30 & ae & f1 & e5 \end{bmatrix}$$

Sonra növbəti addıma keçilir.

Addım 4. Sütunların qarışdırılması. Bu addımda $A(x)$ massivinin sütunlarına $GF(2^8)$ meydanı üzərindəki çoxhədlilər kimi baxılır. Çevirmə sütunun x^4+1 moduluna görə müəyyən edilmiş

$$c(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$$

çoxhədlisinə vurulmasından ibarətdir:

$$b(x)=c(x)\cdot a(x)(\mathrm{mod}\, x^4+1) \qquad (2.3.1).$$

Burada $c(x)$ çoxhədlisi x^4+1 ilə qarşılıqlı sadədir və buna görə vurmanın tərsi var. Tərs çevirmə x^4+1 moduluna görə $c(x)$ -in multiplikativ tərsi olan

$$d(x)=\{0B\}x^3+\{0D\}x^2+\{09\}x+\{0E\} \qquad (2.3.2)$$

çoxhədlisinə vurmaqdan ibarətdir.

$A(x)$ massivini $C(x)$ massivi ilə 2 moduluna görə cəmini hesablayırıq. Hesablama zamanı $A(x)$ massivinin sütun elementləri ardıcıl olaraq $C(x)$ massivi ilə 2 moduluna görə cəmlənir .

$$A(x)=\begin{bmatrix} d4 & e0 & b8 & 1e \\ bf & b4 & 41 & 27 \\ 5d & 52 & 11 & 98 \\ 30 & ae & f1 & e5 \end{bmatrix}$$

$$\oplus \qquad B(x)=\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \bullet \begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix} = \begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix}$$

$$C(x)=\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Bu addımın nəticəsində $A(x)$ massivinin elementləri aşağıdakı kimi olacaq.

$$A(x)=\begin{bmatrix} 04 & e0 & 48 & 28 \\ 66 & cb & f8 & 06 \\ 81 & 19 & d3 & 26 \\ e5 & 9a & 7a & 4c \end{bmatrix}$$

Addım 5. Açarın dövrə əlavə edilməsi. Bildiyimiz kimi hər dövrdə açar hesablanaraq yeni qiymətlər alır. Dövrə açarın əlavə edilməsi ilə $A(x)$ state massivinin hər bir açar massivinin uyğun baytı ilə 2 moduluna görə bütün bitlərin toplanması ilə həyata keçirilir. Bu çevirmə öz-özünün tərsidir. Açarın əlavə edilməsi prosesi aşağıdakı kimidir:

$$A(x) = \begin{bmatrix} 04 & e0 & 48 & 28 \\ 66 & cb & f8 & 06 \\ 81 & 19 & d3 & 26 \\ e5 & 9a & 7a & 4c \end{bmatrix}$$

$$\begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix} \oplus \begin{bmatrix} a0 \\ fa \\ fe \\ 17 \end{bmatrix} = \begin{bmatrix} a4 \\ 9c \\ 7f \\ 2f \end{bmatrix}$$

Beləliklə, $A(x)$ massivinin elementlərinə açar əlavə edilir və aşağıdakı qiymətləri alır:

$$A(x) = \begin{bmatrix} a4 & 68 & 6b & 02 \\ 9c & 9f & 5b & 6a \\ 7f & 35 & ea & 50 \\ f2 & 2b & 43 & 49 \end{bmatrix}$$

Bu addımların dövrlərinin sayı 10-dur. Sonuncu dövrdə sütunların qarışdırılması prosesi olmur.

Yuxarıda göstərilən addımlar yerinə yetirilərək Rijindel alqoritmi vasitəsilə məxfi informasiya bitləri tam şifrlənir və növbəti başlıqda təqdim edilən alqoritm vasitəsilə konteyner təsviri içərisinə gizlədilir. Təklif olunan steqanoqrafik alqoritmin yerinə yetirilmə ardıcıllığı aşağıdakı kimidir.

Məxfi informasiyanın konteyner təsvirinə gizlədilməsi.

Addım 1. Rijindel alqoritmindən istifadə edərək məxfi informasiya bitləri şifrlənir

$$B = b_1, b_2 b_3, \ldots\ldots b_n$$

Addım 2. Konteyner təsvir 2x2 bloklara bölünür (Şəkil 2.3.6)

a_{11}	a_{12}
a_{21}	a_{22}

Şəkil 2.3.6. Konteyner təsvir

Addım 3. Ən aşağı dəyəri olan piksel digər 3 pikseldən çıxılır.

$$\begin{aligned} c_{12} &= a_{12} - \min \\ c_{21} &= a_{21} - \min \\ c_{22} &= a_{22} - \min \end{aligned} \quad (2.3.3.)$$

Alqoritmdə məxfi informasiyaların daxil edilməsi və çıxarılması üçün 3 girişli kvorum funksiyasından istifadə edirik. Kvorum funksiyası (QF), Bul cəbrində, heş funksiyasında və s. geniş istifadə olunur. Kvorum funksiyası aşağıdakı kimi verilir [88, s. 20527-20545];

$$QF(x_1, x_2, ...x_n) = \begin{cases} 1, \sum_{i=1}^{n} x_i \geq \dfrac{n}{2}, \\ 0 \end{cases} \quad (2.3.4.)$$

Konteyner təsvirin c_{12}, c_{21}, c_{22} piksellərinin son 3 ən az əhəmiyyətli bitində məxfi informasiyaların yerləşdirilməsi üçün kvorum funksiyasından istifadə edilmişdir. Bunun üçün (3.3.5) düsturu ilə üç girişli kvorum funksiyasını (3QF) istifadə etmək mümkündür.

$$3QF(x_1, x_2, x_3) = (x_1 \wedge x_2) \oplus (x_1 \wedge x_3) \oplus (x_2 \wedge x_3) \quad (2.3.5)$$

Burada $3QF(x_1, x_2, x_3)$ kvorum funksiyasının giriş qiymətləridir. Giriş qiymətləri kimi konteyner təsvirin müvafiq piksellərinin son 3 ən az əhəmiyyətli biti istifadə olunur. Məlumdur ki, bu qiymətlər 0 və yaxud 1 ola bilər. Əgər funksiyanın giriş qiymətləri 1-ə bərabər olarsa, onda kvorum funksiyasının çıxış qiyməti də 1-ə bərabər olur. Əgər giriş qiyməti 0-a bərabər olarsa, kvorum funksiyasının çıxış qiyməti 0-a bərabər olacaqdır. Üç girişli kvorum funksiyasından (3QF) istifadə edərək məxfi informasiyanın gizlədilməsi proseduru aşağıda ətraflı təsvir edilmişdir.

Təklif edilən alqoritmin rəqəmsal nümunəsi.

Kvorum funksiyasından istifadə edərək məlumatların konteynerə daxil edilməsi (3QF).

Konteyner təsvirinin hər 2 × 2 blokunda 4 piksel var. Bu piksellərdən 3 piksel verilənlərin daxil edilməsi üçün istifadə olunur. Piksellərin son üç əhəmiyyətli biti 3 girişli kvorum funksiyasına ötürülür. Məxfi biti piksel qiymətlərinə daxil etmək üçün aşağıdakı prosedurdan istifadə edilmişdir və aşağıdakı hallar nəzərə alınmalıdır [93, s. 20527-20545] (Cədvəl 2.3.1);

Cədvəl 2.3.1

3 girişli kvorum funksiyasının çıxış qiymətlərini əks etdirən cədvəl

[88, s. 20527-20545]

Giriş qiymətləri			**Çıxış qiymətləri**
x_1	x_2	x_3	$3QF(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

1. Məxfi informasiya biti [i] = 0 və 3QF çıxışı = 0. Burada məxfi bit 0-ı gizlətmək lazımdır.

Tutaq ki, konteyner təsvirinin pikselinin son 3 bitinin qiyməti{000,001,010,100} qiymətlərindən biridir. Bunun üçün cədvəl 2.3.1.– ə nəzər yetirmək lazımdır. Göründüyü kimi burada giriş qiymətləri kimi bir neçə variant təqdim edilib. Bu qiymətlərin əsasında məxfi informasiya biti gizlədilir. Belə ki, cədvəldə 4 hal göstərilib ki, onların qiymətli 0-a bərabərdir. Deməli, konteyner təsvirin pikselinin son 3 bitinin

qiyməti təqdim edilən dörd haldan birinə uyğundur və onu steqo-piksel kimi qəbul etmək olar. Bu zaman steqo-təsviri qəbul edən şəxs həmin pikselin son 3 bitinin qiymətini kvorum funksiyası ilə hesabladıqda qiyməti 0-a bərabər olan məxfi informasiya bitini əldə edir.

2. Məxfi informasiya biti [i] = 1 və 3QF-nin çıxışı = 1. Burada məxfi bit 1-i gizlətmək lazımdır. Tutaq ki, konteyner təsvirinin pikselinin son 3 bitinin qiyməti {011,101,110,111} qiymətlərindən biridir. Cədvəldən göründüyü kimi qiyməti 1-ə bərabər olan 4 hal var. Bu zaman yenə eyni əməliyyat təkrar olunur.

3. Məxfi informasiya biti [i] = 0 və çıxışı 3QF = 1. Burada məxfi bit 0-ı gizlətmək lazımdır və konteyner təsvirin pikselinin son 3 biti {011,101,110,111} 3QF-ə giriş dəstindən hər hansı biridir. Bu dörd giriş halı ilə 3QF = 1 çıxışını verir. Qəbuledici bu pikseldən məxfi bit 0 çıxarmaq istəyir. Bu zaman, optimal bit dəyişdirmə əməliyyatı istifadə edilir. Bu bit dəyişdirmə əməliyyatı 3QF çıxışını 0-a çevirəcək ki, qəbuledici məxfi biti düzgün çıxara bilsin. Bunu nəzərə alaraq, 3QF = 1 çıxışı üçün mümkün girişlər {011,101,110,111}-dir. Optimal bit dəyişdirmə əməliyyatı aşağıda verilmişdir.

1– ci hal: 011 010 kimi dəyişdirilir.

2– ci hal: 101 100 olaraq dəyişdirilir.

3– cü hal: 110 100 olaraq dəyişdirilir.

4– cü hal: 111 100 kimi dəyişdirilir.

1-ci və 2-ci halda yalnız sonuncu bit dəyişdirilir, 3-cü halda yalnız ikinci bit dəyişdirilir, lakin 4-cü halda son iki bit dəyişdirilir. Beləliklə, bu optimal bit dəyişdirmə əməliyyatı adlandırılır. Bütün dörd halda, qəbuledici məxfi bit 0-ı düzgün şəkildə çıxara bilər.

4. Məxfi informasiya biti [i] = 1 və 3QF = 0 çıxışı. Burada isə məxfi bit 1-i gizlətmək lazımdır və konteyner təsvirinin pikselinin son 3 biti {000, 001,010,100} dəstindən biridir. Bu dörd giriş halı üçün kvorum funksiyasının çıxış qiyməti 3QF = 0

olur. Qəbuledici konteyner təsvirinin müəyyən edilmiş pikselindən məxfi bit 1-i çıxarmaq istəyir, buna görə, yenə də optimal bit dəyişdirmə əməliyyatı istifadə olunur.

Bu bit dəyişdirmə əməliyyatı 3QF çıxışını 1-ə çevirəcək ki, qəbuledici məxfi biti düzgün çıxara bilsin. 3QF = 0 çıxışı üçün giriş qiymətləri {000, 001,010,100}-dir. Optimal bit dəyişdirmə əməliyyatı aşağıda verilmişdir;

1-ci hal: 000 011 kimi dəyişdirilir.

2-ci hal: 001 011 kimi dəyişdirilir.

3-cü hal: 010 011 kimi dəyişdirilir.

4-cü hal: 100 101 kimi dəyişdirilir.

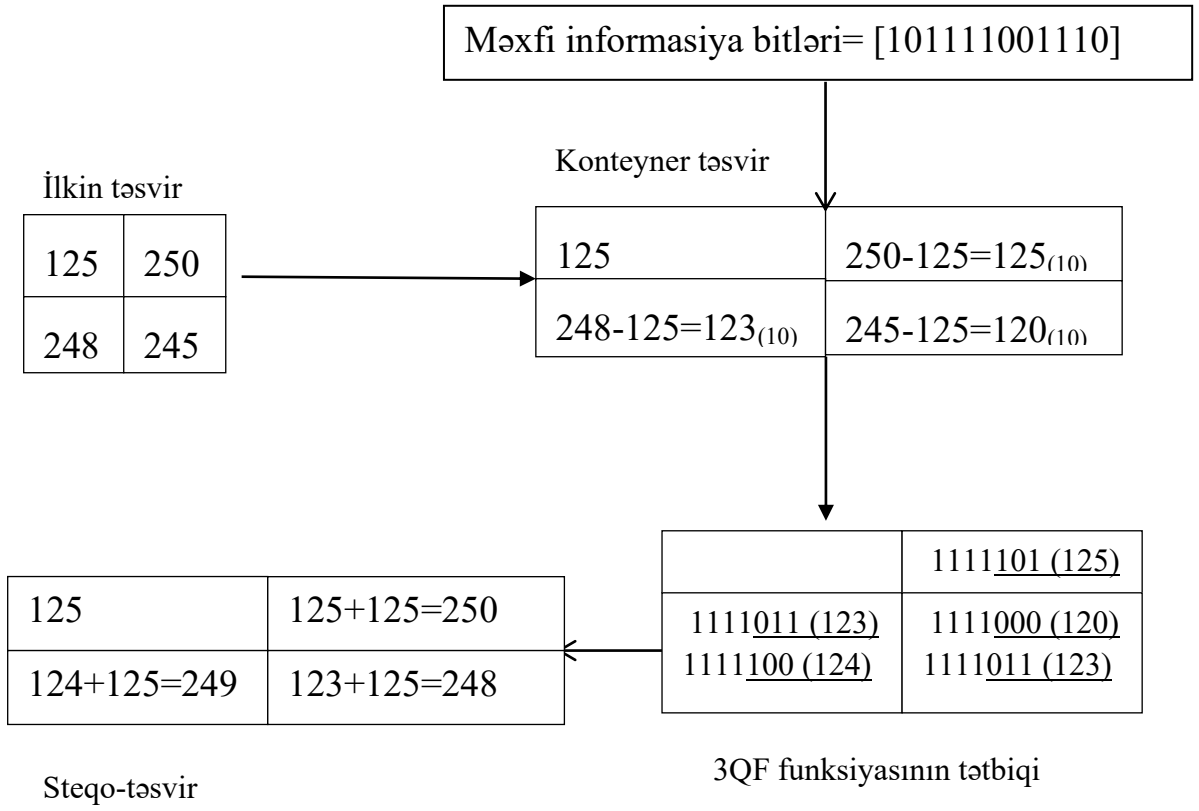
3-cü və 4-cü halda yalnız sonuncu bit, 2-ci halda isə yalnız ikinci bit dəyişdirildi. Lakin, 1-ci halda son iki bit dəyişdirildi. Bütün hallarda, qəbuledici məxfi bit 1-i düzgün şəkildə çıxara bilər.

Fərz edək ki, məxfi informasiya bitləri B=101111001110 verilmişdir. Məxfi informasiyanın birinci biti B [1] =1 bərabərdir. Fərz edək ki, konteyner təsvirin müvafiq pikselinin qiyməti (125=(1111101)) –dir və burada son 3 bitin qiyməti (101)-dir. 3 girişli kvorum funksiyasının qiymətləri cədvəl 2.8.1 [88, s. 20527-20545] verilmişdir. Qiymətlər cədvəlinə əsasən tapırıq ki, giriş qiyməti 101 olarsa, onda 3QF=1 olur. Belə olan halda konteyner pikselinin qiymətini dəyişmədən steqo-təsvir pikseli kimi qəbul edirik. Bu zaman steqo-təsviri qəbul edən şəxs pikselin son 3 qiymətinin kvorum funksiyasına əsasən 1-ə bərabər olduğunu tapır ki, bu da məxfi informasiya biti ilə üst-üstə düşür.

Əks halda, yəni 3QF çıxış qiyməti ilə məxfi bitin qiymətləri arasında bərabərsizlik olarsa, məxfi bitlərin qiymətinə uyğun gələn 3QF-nin məqbul çıxış qiyməti (2) tənliyi ilə müəyyən edilir və müəyyən edilən bitlər konteyner təsvirin müvafiq pikselinin son 3 bitləri ilə əvəz edilir.

Birinci bloka məxfi informasiya bitlərinin bir qismi gizlədildikdən sonra alqoritm növbəti bloku seçir və yuxarıda qeyd olunan prosedur və müvafiq bit

mübadiləsi əməliyyatı başa çatdıqdan sonra blokların piksellərinə minimum piksel əlavə edilir.



Şəkil 2.3.7 Təklif edilən alqoritmin rəqəmsal təsviri

Məxfi informasiyanın steqo-təsvirdən çıxarılması prosesi.

Addım 1. Steqo-təsvir 2x2 bloklara bölünür (şəkil 2.3.8).

S_{11}	S_{12}
S_{21}	S_{22}

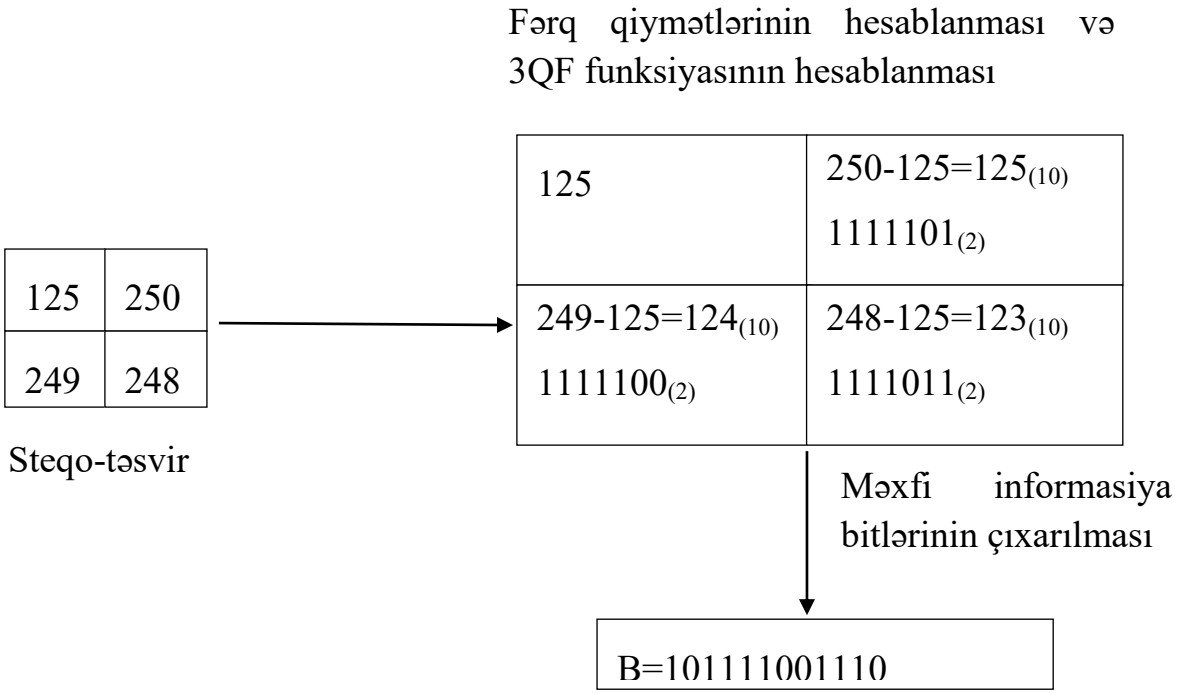
Şəkil 2.3.8 Steqo-təsvir bloku

Steqo-təsvirin hər blokunda birinci pikseldə heç bir məxfi informasiya biti gizlədilməmişdir. Məxfi informasiya bitləri digər üç pikselə gizlədilmişdir.

Addım 2. Digər üç pikseldən minimum piksellər çıxarılır.

$$s'_{12} = s_{12} - \min$$
$$s'_{21} = s_{21} - \min \qquad (2.3.6)$$
$$s'_{22} = s_{22} - \min$$

Addım 3. Fərq qiymətləri s'_{ij} ikilik say sisteminə çevrilir və onların son 3 biti 3QF funksiyasına əsasən hesablanır (3.3.5). Beləliklə, məxfi informasiya bitlərini çıxarmaq mümkün olur (Şəkil 3.3.9).



Şəkil 2.3.9. Təklif olunan alqoritmin rəqəmsal nümunəsinin sxemi

İkinci fəsil üzrə nəticələr

1. İkinci fəsildə 3 müxtəlif məxfi informasiya gizlədilmə alqoritmi işlənilib:
- Təsvirlərin vizual keyfiyyətinə və yüksək dayanıqlılığına əsaslanan məxfi informasiyaların steqanoqrafik gizlədilməsi alqoritmi [75, s. 329-333];
- Təsvirlərin interpolyasiya edilməsinə əsaslanan daha böyük həcmdə informasiya gizlədilmə alqoritmi [11, s. 465-472];
- Kvorum funksiyası əsasında informasiya gizlədilmə alqoritmi [1, s. 60-66].

2. Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritmində məxfi informasiyanın gizlədilməsi iki mərhələdə aprılır. Birinci mərhələdə konteyner təsvirində təsadüfi piksellər seçilir.

Təsadüfi piksellərin seçilməsi steqoaçar vasitəsilə aparılır. Həmin steqoaçarlar olmadan məxfi informasiya bitlərinin yenidən bərpa olunması mümkün olmur. Bu təklif edilən alqoritmin təhlükəsizliyini artırır. İkinci mərhələdə isə məxfi informasiya bitlərinin yerləşdirilməsi təmin edilib. Alınan steqo-təsvirlər steqo hücunlara qarşı dayanıqlı olmaqla yanaşı digər keyfiyyət göstəricilərinin də tələblərini ödəyir.

3. Təsvir interpolyasiyasına əsaslanan məxfi informasiya gizlədilmə alqoritmində mövcud interpolyasiya metodlarında təqdim edilən gizlədiləcək məxfi informasiyanın miqdarını müəyyən etmək üçün istifadə edilən hartli düsturu yeni alqoritm ilə əvəz edilərək daha böyük həcmdə məxfi informasiya biti yerləşdirməyə qadir olan alqoritm təklif edilib. Təklif edilən alqoritm interpolyasiya metodlarının biri ilə birlikdə istifadə edilərək steqo-təsvir yaradılıb. Lakin bu alqoritm sadəcə bu fəsildə təqdim edilən interpolyasiya alqoritmi ilə birlikdə deyil, birinci fəsildə icmalı verilən digər interpolyasiya alqoritmləri ilə birlikdə istifadəsi zamanı da uğurlu nəticələr alınır. Bu da təklif edilən alqoritmin kütləvilik xassəsini təmin etdiyini göstərir. Alqoritmin digər keyfiyyət göstəriciləri və steqo hücumlara qarşı dayanıqlı olması təmin edilib. Bunun daha ətraflı nəticəsi dördüncü fəsildə təqdim edilib.

4. Kvorum funksiyasına əsaslanan informasiya gizlədilmə alqoritmində məxfi informasiya alqoritmi əvvəlcə AES standartı əsasında şifrlənir. Bununla təhlükəsizlik daha gücləndirilir. Daha sonra şifrlənmiş məxfi informasiya bitləri kvorum funksiyası vasitəsilə yeni təklif edilən alqoritm əsasında konteyner təsvirinə gizlədilərək steqo-təsvir yaradılır. Məxfi informasiyanın gizlədilməsi və yenidən əldə olunmasının rəqəmsal nümunəsi verilib. Nümunədən məlum olur ki, məxfi informasiya bitləri tam bərpa olunur. Kriptoqrafik şifrləmə alqoritminin istifadəsi onun təhlükəsizliyini artırır. Təklif edilən yeni alqoritmin keyfiyyət göstəriciləri təmin edilib. Bu göstəricilərin nəticəsi daha geniş dördüncü fəsildə verilib.

5. Təklif edilən hər üç alqoritmin işləməsi üçün məxfi informasiyanın konteyner təsvirinə gizlədilmə və steqo-təsvirdən çıxarılma prosedurlarının rəqəmsal nümunələri verillib. Nümunələrdən məlum olur ki, təklif edilən alqoritmlərdə

mürəkkəb hesablamalar olmadığı üçün sadədir, istifadəsi isə rahatdır. Bu da həmin alqoritmlərin realizəsi üçün az vaxtın tələb olunmasını göstərir.

6. Təqdim edilən alqoritmlər heç bir pozuntu və maneə olmadan məxfi informasiya bitlərinin rəqəmsal təsvirdə gizlədilməsini və çıxarılmasını təmin etməklə yanaşı steqo-hücumlara qarşı dayanıqlı olması üçün də işlər aparılıb. Bu da məxfi informasiyaların icazəsi olmayan şəxslər tərəfindən ələ keçirilməməsini təmin edir.

III FƏSİL. RƏNGLİ TƏSVİRLƏRDƏ MƏXFİ İNFORMASİYANIN GİZLƏDİLMƏ ALQORİTMLƏRİNİN İŞLƏNİLMƏSİ

Bu gün qlobal kompüter şəbəkələrində, sosial mediada dövr etdirilən multimedia vasitələrinin əsas kütləsini rəngli, rəqəmsal təsvirlər təşkil edir. Bu sahədə rəngli təsvirlərin istifadə edilməsi hələ inkişaf mərhələsindədir. Onu da qeyd etmək lazımdır ki, rəngli təsvirlərin steqanoqrafiyada istifadəsi böyük potensiala malikdir.

Rəngli təsvirlərin strukturu daha böyük həcmdə məxfi informasiya gizlədilməsini və bununla yanaşı vizuallığın qorunmasını təmin etməyə imkan verir. Rəngli təsvirlərdə məxfi informasiya gizlədilməsi alqoritmləri tədqiq edilərkən dayanıqlılıq məsələlərinin kifayət qədər öyrənilməməsi nəzərə çarpır.

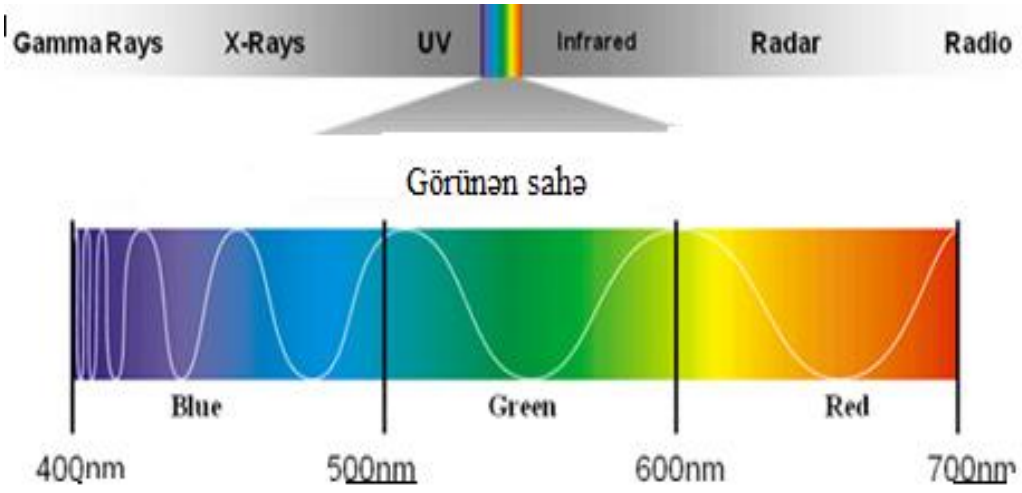
Bu fəsildə yuxarıda deyilənləri nəzərə alaraq dayanıqlığı, vizual keyfiyyəti və daha böyük həcmdə məxfi informasiyanın gizlədilməsini təmin etmək əsas məqsəd kimi qoyulub. Təklif edilən alqoritmlərdə, dayanıqlılıq məsələsini təmin etmək üçün miqyasca dəyişməyən xüsusiyyət çevrilməsi (scale invariant feature transform - SIFT) metodundan istifadə edilib.

Rəngli təsvirlərdə açar nöqtə pikselləri və onların deskriptorlarını SIFT metodu ilə tapmaq mümkündür. Bunun üçün invariantlığı təmin edən aşağıdakı çevrilmələr istifadə olunur. Bu çevirmələrə nəzər yetirək .

1. Sürüşmələr
2. Dönmə
3. Miqyaslama (eyni obyekt müxtəlif təsvirlərdə fərqli ölçülü ola bilər)
4. Parlaqlığın dəyişməsi
5. Kameranın vəziyyətinin (duruşunun) dəyişmələri. Son üç dəyişmələr üçün tam həcmdə invariantlıq almaq olmur. Lakin, heç olmasa qismən bunu etmək mümkündür.

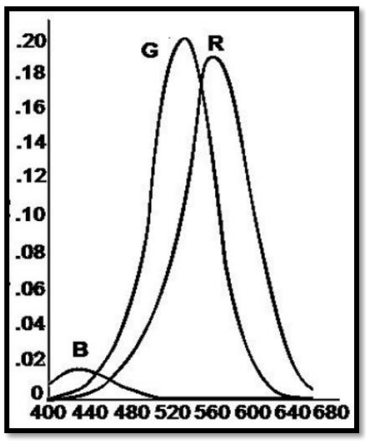
Xüsusi nöqtələrin müəyyən edilməsi və yaxud aşkarlanması üçün Qauss çevirməsi və Qauss fərqi tapılır.

Tədqiqatlar gösərir ki, insan gözü 400 nm (nanometr) ilə 700 nm arasındakı rəng qiymətlərini görə bilir. Mavi rəng isə 400 nm ilə 500 nm arasındadır, bu da görünən sahədə qalan ilk hissədir. Buna görə də, dəyişikliyin digər rənglərlə müqayisədə ən az fərq ediləcəyi rəng mavidir. Məxfi informasiya bitlərini gizlətmək üçün mavi kanal istifadə edilərsə, məxfi informasiyanın bədniyyətli tərəfindən aşkarlanması çətin olar (şəkil 3.1).



Şəkil 3.1. Elektromaqnit spektri

Şəkil 3.1-də üç rəng sxemi və gamma şüalar, X-şüalar, ultrabənövşəyi şüalar, infraqırmızı şüalar, radar və radio şüalar göstərilib. Şəkildən məlum olur ki, mavi rəng kanalı həqiqətən də 400 nm ilə 500 nm intervalında yerləşir. Buna əsasən biz məxfi informasiya bitlərini həmin kanalda gizlətməyi hədəf qoyuruq.



Şəkil 3.2. RGB rəng sxeminin qrafiki

Təklif edilən məxfi informasiya gizlədilmə alqoritmində məxfi informasiya bitləri, konteyner təsvirin mavi kanalının, SIFT alqoritmi ilə seçilmiş piksellərinə gizlədilir. SIFT alqoritmi təsvirdə əsas nöqtə xüsusiyyətlərini müəyyən etmək üçün istifadə edilən alqoritmdir [35, s. 130-134]. SIFT alqoritmi, həm də obyekt və ya səhnənin tanınması, 3D strukturun modelləşdirilməsi, hərəkətin izlənməsi və s. kimi təsvirlər arasında müqayisə üçün istifadə edilə bilən xüsusiyyətlərə malikdir. Bundan başqa o, təsvirlərdən yerli xüsusiyyətləri aşkarlayır və çıxarır. SIFT metodu ilə çıxarılan xüsusiyyətlərə fırlanma, miqyaslama və işıqlandırma təsir etmir, buna görə də səhnənin modelləşdirilməsi, tanınması və izlənilməsi üçün tətbiq olunur [66, s. 1-19].

3.1. Böyük həcmli məxfi informasiya gizlədilmə alqoritmi

SIFT alqoritmi ilə rəngli təsvirin mavi kanalında əsas açar nöqtələrin tapılması MATLAB R2014 proqramında aşağıdakı addımlar ilə hesablanıb:

Miqyas fəzasında ekstremal nöqtələri (minimum-maksimum) axtararaq əsas namizəd nöqtələrin müəyyən edilməsi:

Miqyas fəzasında ekstremal nöqtələrin mövqelərini tapmaq üçün təsvirlərdə adətən müxtəlif standart sapma (σ) qiymətlərini tapmaq lazım gəlir. Bunun üçün təsvir Qauss çevirmələrindən keçirilir.

Təsvirdəki səs-küy (hamarlaşdırma, təkmilləşdirmə və kəskinləşdirmə) müxtəlif standart sapma (σ) ilə, yəni Qauss çevirmələri ilə silinir.

Təsvirlərdə mövcud olan səs-küy dedikdə, əsasən; ətrafdakı hərəkət və ya qeyri-sabitlik səbəbindən bulanıqlıq, təsvirdə yanlış işıq effekti səbəbindən fokusun bulanması, qüsursuz linzaların yaratdığı həndəsi təhriflər və elektron mənbələrdən gələn səhvlər və s. hesab olunur.

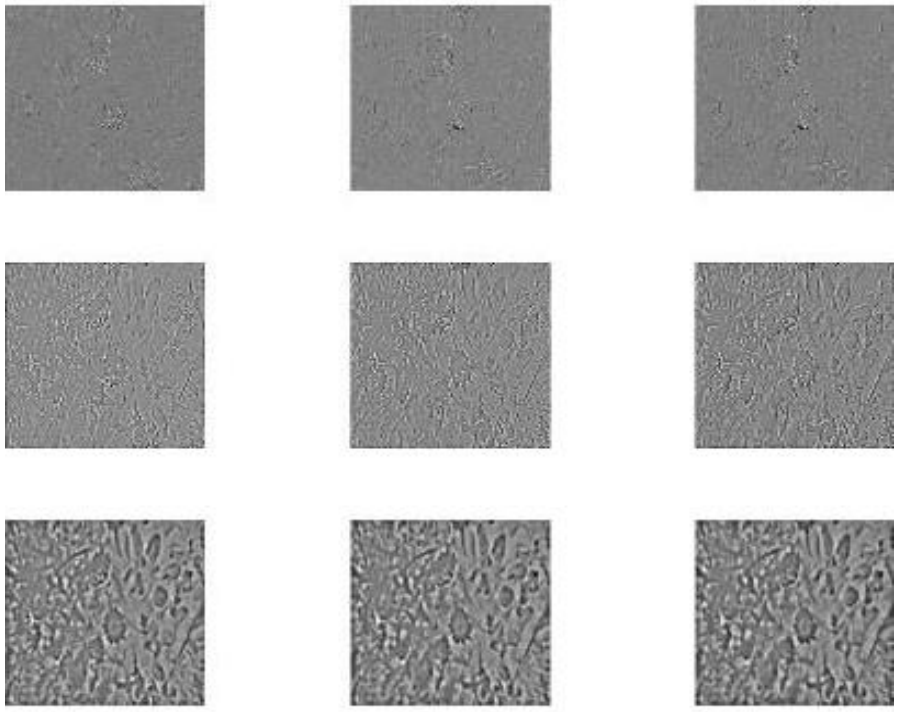
Başqa sözlə, səs-küy, siqnalın kanal üzərindən ötürülməsi zamanı ətraf mühit amillərinin təsiri altında baş verən arzuolunmaz dəyişikliklərdir. Bu xəta həddi səs-küyü yaradan Qauss çevirmələrinin siqma (σ) parametrindən asılıdır. Təsvirdəki əsas namizəd nöqtələr Qauss çevirmələri ilə müəyyən edilir.

İnformasiya gizlədilmə prosesinə keçməzdən əvvəl SIFT alqoritmindən istifadə etməklə rəngli təsvirdə açar nöqtə piksellərinin müəyyən edilməsi verilib. Bu aşağıdakı addımlar ilə edilir.

Addım 1. Fərz edək ki, şəkil 3.1.1-də göstərilən ilkin rəngli təsvir verilib.

Şəkil 3.1.1 İlkin təsvir

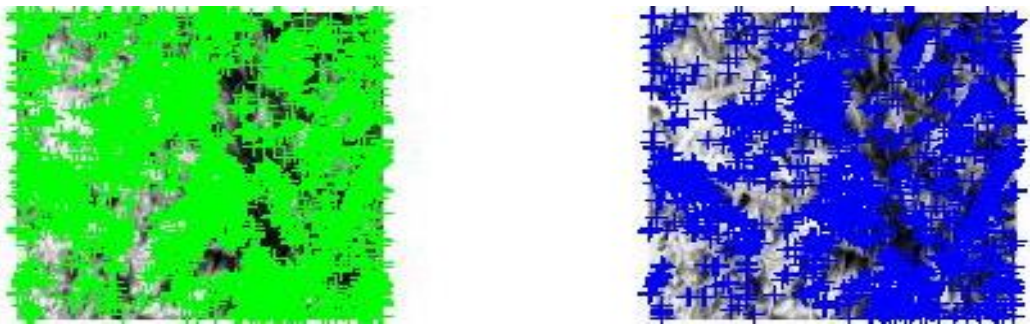
İlkin təsvirin Qauss çevirməsi hesablanır. Qauss çevirməsinin hesablanma qaydası daha ətraflı [56, s. 1150-1157] –də verilib



Şəkil 3.1.2. İlkin təsvirin Qauss fərqi

Sadə boz rəngli təsvirlərdə bulanıq təsvirlər, müxtəlif siqma qiymətlərinə malik Qauss fərqi (Diffrence of Gauss -DoG) funksiyaları ilə ilkin boz tonlu təsvirləri birləşdirməklə əldə edilir. Qauss fərqi (DoG) funksiyası ilkin boz rəngli təsvirdə mövcud olan bütün fəza tezliklərini ləğv edən filtrdir. Qauss fərqi (DoG) funksiyası biri digərinə nisbətən k mütənasib ölçüyə malik, iki Qauss filtrindən keçirilmiş təsvir arasındakı fərq nəticəsində əldə edilir.

Addım 2. Əsas nöqtələrin təkmilləşdirilməsi. Bu addımda əsas namizəd nöqtələr arasından seçim edərək müəyyən edilmiş aşağı keyfiyyətli nöqtələrin aradan qaldırılması (az kontrastlı nöqtələrin aradan qaldırılması və ya yaxşı təsvir olunmadığı üçün kənarda yerləşən nöqtələrin aradan qaldırılması) nəzərdə tutulur. Əsas namizəd nöqtələr arasında seçim edərək əsas nöqtələri üzə çıxarmaq üçün ilk növbədə sabit olmayan, yəni aşağı kontrastlı (küydən daha çox təsirlənən) və ya kənarlarda zəif aşkar edilən əsas nöqtələr aradan qaldırılır. Təsvirdəki az kontrastlı nöqtələrin çıxarılması üçün onun qonşu nöqtələri ilə bağlı namizəd nöqtələrin kontrastının qiymətləndirilməsi müəyyən edilməlidir.



Şəkil 3.1.3 Aşağı kontrastlı nöqtələrin müəyyən olunması

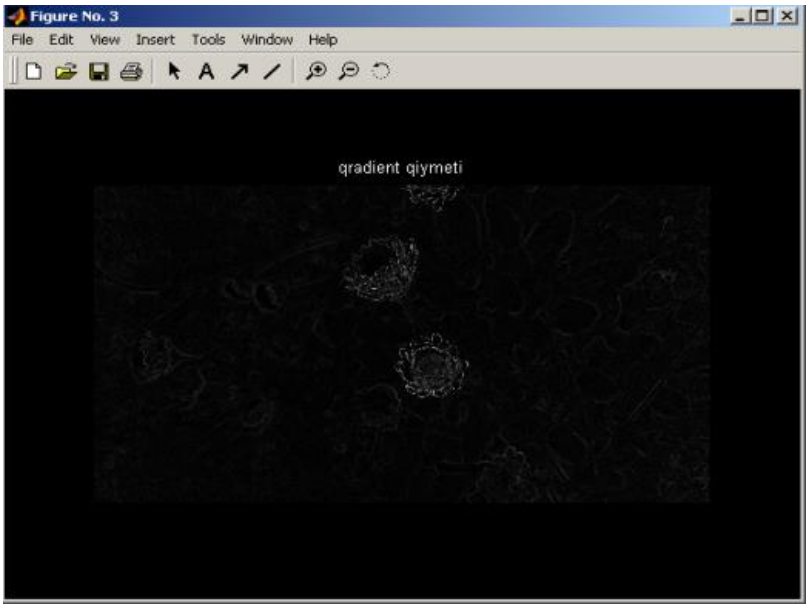
Şəkil 3.1.3-də yaşıl rəng ilə göstərilən nöqtələr təsvirdə seçilmiş ümumi namizəd nöqtələri, göy rəng ilə göstərilən nöqtələr isə aşağı kontrastlı nöqtələri bildirir.

Addım 3. Əsas nöqtələrin dövri dəyişikliyə qarşı davamlılığının hesablanması (nisbətinin aşkarlanması, ölçü və istiqamətin hesablanması) [56, s. 1150-1157].

Əsas nöqtələrin dövri dəyişikliyə qarşı davamlılığının hesablanması üçün cismin iki ölçülü ox ətrafında fırlanmasına, mövqeyinin və bucağının dəyişməsinə qarşı

dövri dəyişikliyə (nisbətin aşkarlanması, ölçü və istiqamətin hesablanması) müqavimət qazanması vacibdir.

Ölçü və istiqamətin hesablanması Qauss filtrindən keçirilmiş, başqa sözlə desək, Qauss fərqi hesablanmış təsvirin bütün əsas nöqtələri hər bir qonşu piksel üçün müəyyən edilir. Əsas nöqtələrin ətrafında hər biri 10° dərəcə istiqaməti əhatə edən 36 dairəvi histoqram yaradılır və histoqrama əlavə edilən hər bir bitişik nümunə nöqtəsi öz qradient qiyməti ilə ölçülür (şəkil 3.1.4) [5, s. 53-57].



Şəkil 3.1.4. Qradient qiyməti hesablanmış təsvir

Addım 4. Əsas nöqtələr üçün identifikatorların yaradılması (128 ölçülü vektor).

Əsas nöqtələr üçün identifikatorların yaradılması və parlaqlıq dəyişiklikləri ilə 3 ölçülü görünüşə qarşı müqavimət əldə edilir. Əsas nöqtə ətrafında qradienti böyük olanlar istifadə olunur. Ayrı-ayrılıqda işlənən hər bir əsas nöqtənin 16x16 ölçüdə qonşusunu ehtiva edən identifikatorlar 4x4 ölçülü sahədə müəyyən edilir. Hər 4x4 ölçülü kvadratın 45° dərəcə olan 8 vektor böyüklüyü var. Bu halda əldə edilən SIFT qiyməti 128 ölçülü vektora bərabə olur [5, s. 53-57].

Addım 5. Yaradılmış identifikator vektorlar arasında Evklid məsafələrinin hesablanması ilə uyğunlaşdırma prosesinin həyata keçirilməsi.

Dövri dəyişməzliyi təmin etmək üçün fırlanma əsas nöqtə identifikatorunun mövqeyinə, qradient bucaqlarına və əsas nöqtə bucağına əsasən həyata keçirilir.

Təsvirin uyğunlaşdırılması prosesi, əsas nöqtə xüsusiyyətlərini müəyyən etdikdən sonra, müəyyən edilmiş əsas nöqtələri bir-biri ilə uyğunlaşdırmaq üçün istifadə olunur (şəkil 3.1.5).

Şəkil 3.1.5. Əsas nöqtələri müəyyən edilmiş təsvir

Şəkil 3.1.5 da konteyner kimi istifadə ediləcək təsvirin SIFT alqoritmi ilə müəyyən edilmiş əsas namizəd nöqtələri, yəni pikselləri aydın göstərilib. Daha sonra isə təklif edilən alqoritm ilə seçilən açar nöqtə piksellərinə məxfi informasiya bitləri gizlədilir.

Müəyyən edilmişdir ki, kompüter prosessorunun sürəti artırıldıqda SIFT əsas nöqtələrini və hədəfi tapmaq vaxtı azalır. Bununla belə, SIFT əsas nöqtələri nə qədər çox taparsa, sistemin doğruluğu və dəqiqliyi bir o qədər yüksək olar [56, s. 1150-1157].

Bu bölmədə təklif edilən alqoritmin əsas məqsədi daha böyük həcmdəki məxfi informasiya bitlərini təsvirin vizuallığını qorumaqla rəngli təsvirə gizlətməkdir.

Təbii ki, burada digər əsas məqam təhlükəsizliyin də təmin olunmasıdır. Eyni zamanda, rəngli təsvirlərdə gizlədilmiş məxfi informasiyanın təhrifinə yönəlmiş bəzi təsvirlərin işlənmə əməliyyatları təsvirdəki məxfi informasiyanın təhrif olunmasına imkan vermir. Bu əməliyyatlar əsasən aşağıda adları sadalananlardır:

- Təsvirin bulanıqlaşdırılması;
- JPEG təsvirlərin kodlanması;
- təsvirin müəyyən bucaq altında döndərilməsi;

- təsvirin sıxılması;
- təsvirin rəng şkalası uyğun gələn başqa təsvir ilə birləşdirilməsi.

Yuxarıda sadalanan hücum alqoritmlərinin nəticələri dördüncü fəsildə təqdim edilib.

Məxfi informasiyanın gizlədilmə ardıcıllığı.

Təklif edilən alqoritmdə məxfi informasiya bitləri RGB (red, green, blue) rəng sxemində olan konteyner təsvirinə gizlətmək üçün təsvirin B (blue) mavi kanalın pikselləri arasında SIFT alqoritmi ilə əsas açar nöqtələr müəyyən edilir və müəyyən edilmiş həmin nöqtədə məxfi informasiya bitləri gizlədilir. Məxfi informasiya bitlərinin gizlədilməsinin xaotik olması alqoritmin vizuallıq və təhlükəsizlik keyfiyyətini yüksəldir.

Məxfi informasiya bitlərinin rəngli təsvirin mavi kanalındakı ixtiyari pikselə və yaxud ardıcıl seçilmiş piksellərinə deyil, SIFT alqoritmi ilə müəyyən edilən açar nöqtə piksellərində gizlədildiyi üçün təhlükəsizlik baxımından etibarlı hesab edilir.

Məxfi informasiya bitləri konteyner təsvirin müəyyən edilmiş piksellərinə gizlədilməsi zamanı səkkizlik say sisteminə çevrilərək konteyner təsvirinə gizlədilməsi nəzərdə tutulur. Çünki, səkkizlik say sistemi əsasında məxfi informasiya bitləri seçilərsə, ikilik say sistemi ilə gizlədilmə alqoritmlərinə nisbətən daha çox məxfi informasiya biti seçib gizlətmiş oluruq. Təklif edilən alqoritmdə SIFT alqoritmi ilə müəyyən edilən açar nöqtə piksellərinə məxfi informasiya bitlərinin gizlədilmə ardıcıllığı aşağıdakı kimidir.

Addım 1. SIFT alqoritmi ilə açar nöqtə pikselləri tapılır.

Addım 2. Müəyyən edilən açar nöqtə pikselləri içərisindən mavi kanalda yerləşən açar nöqtə pikselləri seçilir.

Addım 3. Məxfi informasiya bitləri səkkizlik say sisteminə çevrilərək gizlədilməsi nəzərdə tutulduğuna görə, təklif edilən alqoritmə əsasən (3.1.16) düsturu ilə müəyyən edilmiş piksellərin səkkizə bölünməsindən alınan qalıq hesablanır:

$$n = p_{i,j} \bmod 8 \qquad (3.1.16)$$

burada $p_{i,j}$ konteyner təsvirinin pikselidir.

Addım 4. Addım 3-dən alınan n qalıq qiymət ikilik say sisteminə çevirilir

$$n_{10} \to n_2'.$$

Addım 5. İkilik say sistemində alınan bit düzümünün daxilindəki birlər və sıfırların ümumi sayı qədər məxfi informasiya biti seçilir.

Addım 6. Seçilmiş məxfi informasiya bitləri səkkizlik say sisteminə çevrilir

$$n_2 \to d_8$$

Addım 7. (3.1.17) düsturunda göstərildiyi kimi konteyner təsvirinin pikseli ilə cəmlənir.

$$S_{ij} = p_{i,j} + d_8 \qquad (3.1.17)$$

burada S_{ij} steqo-təsvir pikseli, d_8 isə səkkizlik say sisteminə çevrilmiş məxfi informasiya bitidir.

Beləliklə, məxfi informasiya bitləri konteyner təsvirinə gizlədilir.

Məxfi informasiya bitlərinin steqo-təsvirdən çıxarılması.

Steqo-təsvirdən məxfi informasiya bitlərini çıxarmaq üçün addımlar aşağıdakı ardıcıllıqla yerinə yetirilir.

Addım 1. İnformasiya qəbuledicisi yenidən konteyner təsvirin SIFT alqoritmi ilə açar nöqtələrini tapır.

Addım 2. Həmin nöqtələrin mavi kanala düşən pikselləri müəyyən edilir.

Addım 3. Daha sonra steqo-təsvirin də SIFT alqoritmi ilə açar nöqtələri tapılır.

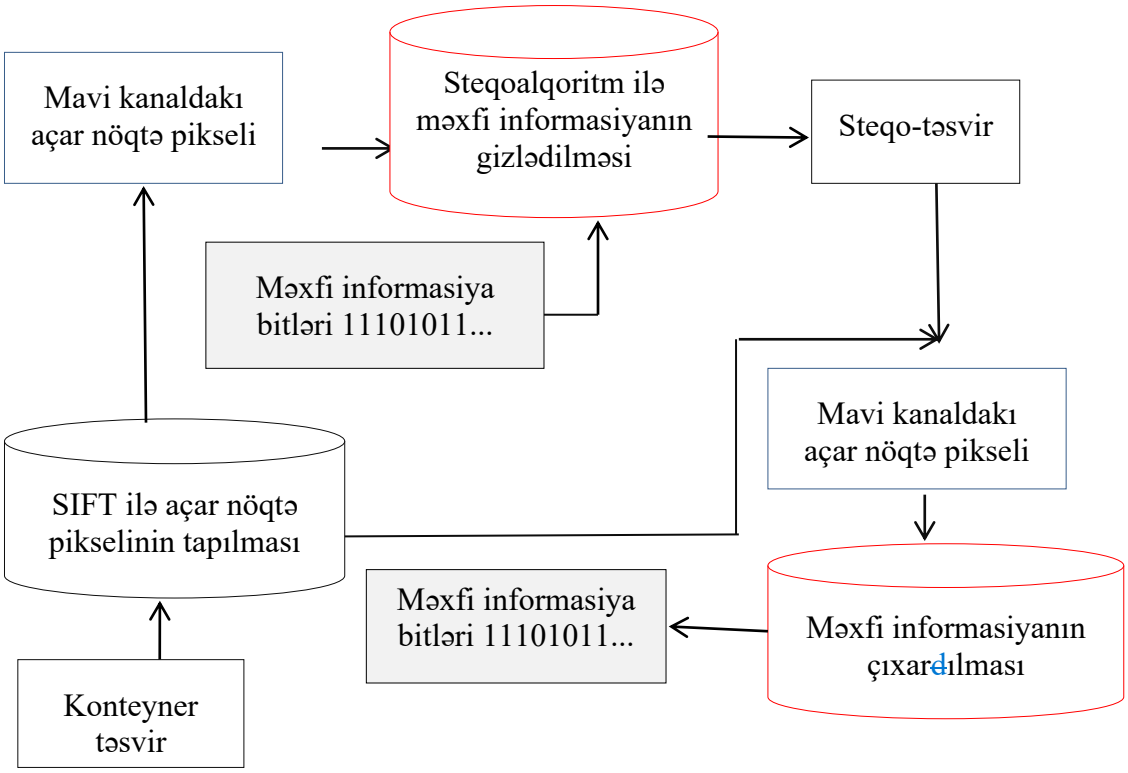
Addım 4. Mavi kanalda yerləşən həmin piksellər müəyyən edilir.

Addım 5. Konteyner təsvirin mavi kanalında müəyyən edilən açar nöqtə pikselləri, steqo-təsvirin mavi kanalında müəyyən edilən açar nöqtə piksellərindən çıxılır (3.1.18)

$$M = S(i, j) - P(i, j) \qquad (3.1.18)$$

burada M məxfi informasiya bitlərini, $S(i, j)$ steqo-təsvirin müəyyən pikseli, $P(i, j)$ isə konteyner təsvirin müəyyən pikselidir.

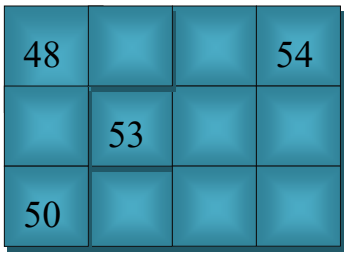
Addım 6. M -in qiymətlərini ikilik say sisteminə çeviririk və alınan qiymətlər ardıcıl olaraq yan-yana düzülür. Beləliklə, məxfi informasiya bitləri yenidən əldə edilir. Təklif edilən alqoritmin ümumi struktur sxemi şəkil 3.1.6-da verilib.



Şəkil 3.1.6. Rəngli təsvirlərdə məxfi informasiyanın gizlədilməsinin və çıxardılmasının ümumi struktur sxemi

Məxfi informasiyanın konteyner təsvirinə gizlədilmə ardıcıllığının rəqəmsal nümunəsi.

Addım 1. Fərz edək ki, mavi kanalın SIFT alqoritmi ilə seçilmiş müvafiq pikselləri şəkil 3.1.7.-dəki kimi verilib.



Şəkil 3.1.7. Konteyner təsvirin mavi kanal bloku və SIFT ilə müəyyən edilmiş açar nöqtə pikselləri

Addım 2. Yuxarıda verilən (3.1.16) düstura əsasən piksellərin səkkizə bölünməsindən alınan qalıq hesablanır.

$$n_1 = 48 \bmod 8 = 0$$
$$n_2 = 54 \bmod 8 = 6$$
$$n_3 = 53 \bmod 8 = 5$$
$$n_4 = 50 \bmod 8 = 2$$

Addım 3. Sonra n-in qiymətləri ikilik say sisteminə çevrilir.

$$n_1 = 48 \bmod 8 = 0$$
$$n_2 = 54 \bmod 8 = 6 = 110$$
$$n_3 = 53 \bmod 8 = 5 = 101$$
$$n_4 = 50 \bmod 8 = 2 = 10$$

Addım 4. Burada n_1-in qiyməti 0-a bərabər olduğu üçün bu pikselə heç bir məxfi informasiya biti yerləşdirilmir. Lakin digər piksellərə nəzər yetirsək, n_2 və n_3-ün nəticəsinə görə 3 bit, n_4-də isə 2 bit məxfi informasiya biti seçilib təklif edilən alqoritmə əsasən səkkizlik say sisteminə keçirərək gizlətmək olar.

Addım 5. Tutaq ki, məxfi informasiya bitləri isə $m = 1011111101$.....kimi verilib. Buna əsasən, məxfi informasiya bitlərindən əvvəlcə ilk üç bit, sonra növbəti üç bit, sonra isə növbəti iki bit seçilir.

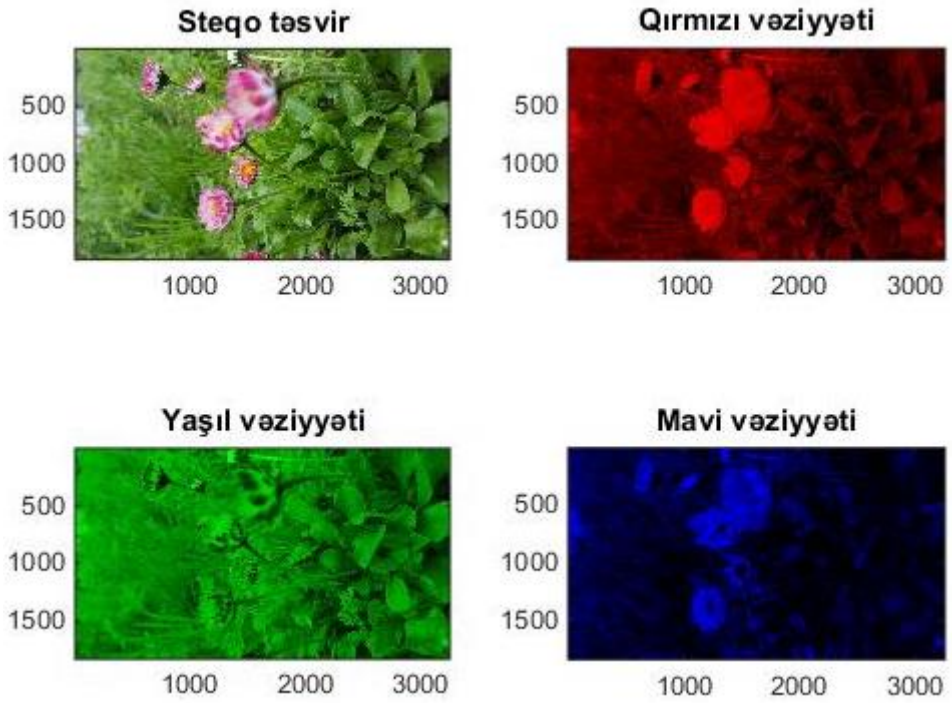
Addım 6. Seçilmiş bitlər səkkizlik say sisteminə çevrilir.

$$m_2 = ''101'' \; onda \;\; d_8 = 5$$
$$m_3 = ''111'' onda \; d_8 = 7$$
$$m_4 = ''11'' \; onda \;\; d_8 = 3$$

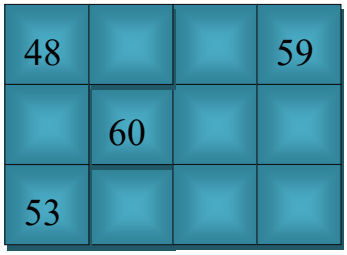
Addım 7. Səkkizlik say sisteminə çevrilmiş məxfi informasiya bitləri rəngli təsvirin B- mavi kanal blokunun müvafiq pikselləri ilə cəmlənir.

$$S_{1,2} = 54 + 5 = 59$$
$$S_{2,1} = 53 + 7 = 60$$
$$S_{2,2} = 50 + 3 = 53$$

Beləliklə, şəkil 3.1.8-də göstərilən steqo-təsvir alınır.



Şəkil 3.1.8. Steqo-təsvir



Şəkil 3.1.9. Steqo-təsvirin mavi kanal bloku və SIFT ilə müəyyən edilmiş açar nöqtə pikselləri

Məxfi informasiya bitlərinin steqo-təsvirdən çıxardılmasının rəqəmsal nümunəsi.

Addım 1. SIFT alqoritmi ilə steqo-təsvirdə müəyyən edilmiş açar nöqtələr yəni, steqo-piksellər $S(i,j)=48,\ 59,\ 60,\ 53$ -ə bərabərdir.

Addım 2. Konteyner təsvirin SIFT alqoritmi ilə açar nöqtə pikselləri müəyyən edilir. Onlarda müvafiq olaraq $p(i,j)=48,\ 54,\ 53,\ 50$-yə bərabərdir.

Addım 3. Belə olduqda yuxarıdakı addımlara əsasən hesablama aşağıdakı kimi aparılacaq;

$$M_1 = 48-48=0$$

burada alınan qiymət sıfıra bərabərdir. Deməli, bu pikseldə heç bir məxfi informasiya biti gizlədilməyib.

Addım 4. Daha sonra növbəti piksellərin hesablanması aparılır,

$$M_2 = 59 - 54 = 5$$
$$M_3 = 60 - 53 = 7$$
$$M_4 = 53 - 50 = 3$$

Addım 5. Addım 4-dən alınan qiymətləri ikilik say sisteminə çevrilir,

$$M_2 = 5 = 101$$
$$M_3 = 7 = 111$$
$$M_4 = 3 = 11$$

Addım 6. Addım 5-dən alınan qiymətləri ardıcıl olaraq aşağıdakı kimi düzülür $M = 10111111.....$ beləliklə, məxfi informasiya bitləri bərpa olunaraq yenidən əldə edilir.

3.2. Yüksək vizual keyfiyyət prioritetli məxfi informasiya gizlədilmə alqoritmi

Yuxarıda təqdim edilən alqoritmin digər bir variantı isə vizuallığı daha da yaxşılaşdırmaq məqsədilə mavi kanalın müvafiq piksellərinin 4-ə bölünməsindən alınan qalığı tapılır. Daha sonra alınan qalıq ikilik say sisteminə çevrilir və oradakı bitlərin sayına uyğun məxfi informasiya bitləri seçilir. Daha sonra seçilən bitləri dördlük say sisteminə çevirib konteyner təsvirin mavi kanalındakı müvafiq piksel ilə cəmləmək olar. Bu zaman səkkizlik say sistemi ilə gizlədilmə alqoritminə nisbətən az, ikilik say sistemi ilə gizlədilmə alqoritmlərinə nisbətən çox miqdarda məxfi informasiya biti gizlədiləcək. Bu alqoritmin əsas məqsədi vizuallıq daha çox tələb olunan sahələrdə tətbiq etməkdir. Belə ki, bu alqoritmdə 3.2 bölməsində təklif edilən alqoritmə nisbətən vizuallıq daha yüksəkdir. Bu alqoritmin addımları aşağıdakı kimidir.

Addım 1. SIFT alqoritmi ilə açar nöqtə pikselləri tapılır.

Addım 2. Müəyyən edilən açar nöqtə pikselləri içərisindən mavi kanalda yerləşən açar nöqtə pikselləri seçilir.

Addım 3. Məxfi informasiya bitləri dördlük say sisteminə çevrilərək gizlədilməsi nəzərdə tutulduğuna görə, təklif edilən alqoritmə əsasən (3.1.16) düsturu ilə müəyyən edilmiş piksellərin dördə bölünməsindən alınan qalıq hesablanır:

$$n = p_{i,j} \bmod 4 \qquad (3.1.16)$$

burada $p_{i,j}$ konteyner təsvirinin pikselidir.

Addım 4. Addım 3-dən alınan n qalıq qiyməti ikilik say sisteminə çevirilir

$$n_{10} \to n_2' .$$

Addım 5. İkilik say sistemində alınan bit düzümünün daxilindəki birlər və sıfırların ümumi sayı qədər məxfi informasiya biti seçilir.

Addım 6. Seçilmiş məxfi informasiya bitləri dördlük say sisteminə çevrilir

$$n_2 \to d_4$$

Addım 7. (3.1.17) düsturunda göstərildiyi kimi konteyner təsvirinin pikseli ilə cəmlənir.

$$S_{ij} = p_{i,j} + d_4 \qquad (3.1.17)$$

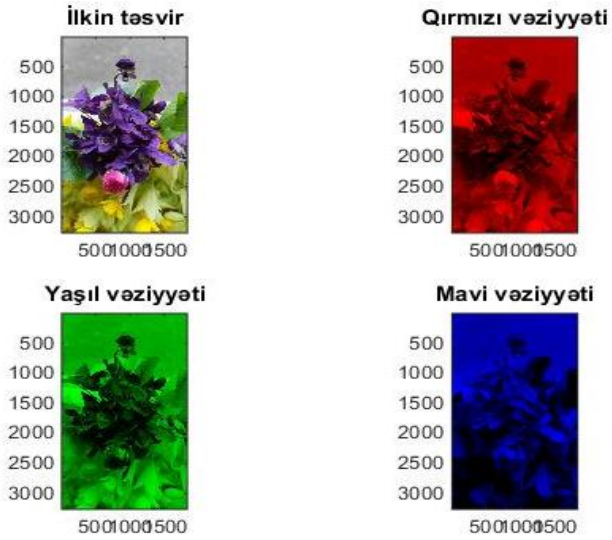
burada S_{ij} steqo-təsvir pikseli, d_4 isə dördlük say sisteminə çevrilmiş məxfi informasiya bitidir.

Beləliklə, məxfi informasiya bitləri konteyner təsvirinə gizlədilir.

Məxfi informasiya bitlərinin steqo-təsvirdən çıxardılması ardıcıllığı əvvəlki alqoritmin ardıcıllığı ilə eyni olacaq. Buna görə də, həmin addımların izahı rəqəmsal nümunədə verilib.

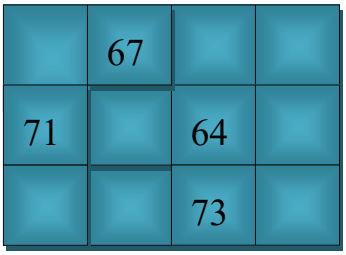
Məxfi informasiya gizlədilmə alqoritminin rəqəmsal nümunəsi.

Fərz edək ki, konteyner təsvir kimi şəkil 3.2.1 təsvir verilib.



Şəkil 3.2.1. Konteyner təsvir

Addım 1. Konteyner təsvirinin pikselləri müvafiq olaraq şəkil 3.2.2 –dəki kimi verilib.



Şəkil 3.2.2. Konteyner təsvirin mavi kanal bloku və SIFT ilə müəyyən edilmiş açar nöqtə pikselləri

Addım 2. Yuxarıda verilən (3.1.16) düsturuna əsasən piksellərin dördə bölünməsindən alınan qalıq hesablanır

$$n_1 = 67 \bmod 4 = 3$$
$$n_2 = 71 \bmod 4 = 3$$
$$n_3 = 64 \bmod 4 = 0$$
$$n_4 = 73 \bmod 4 = 1$$

Addım 3. Sonra n-nin qiymətləri ikilik say sisteminə çevrilir,

$$n_1 = 3_{10} = 11_2$$
$$n_2 = 3_{10} = 11_2$$
$$n_3 = 0_{10} = 0_2$$
$$n_4 = 1_{10} = 1_2$$

Addım 4. Addım 3-də n_3-in qiyməti 0-a bərabər olduğu üçün bu pikselə heç bir məxfi informasiya biti gizlədilmir. Lakin digər piksellərdə n_1 nəticəsinə görə iki bit, n_2-də iki bit və n_4-də bir bit məxfi informasiya biti seçilib təklif edilən alqoritmə əsasən dördlük say sisteminə çeviririk.

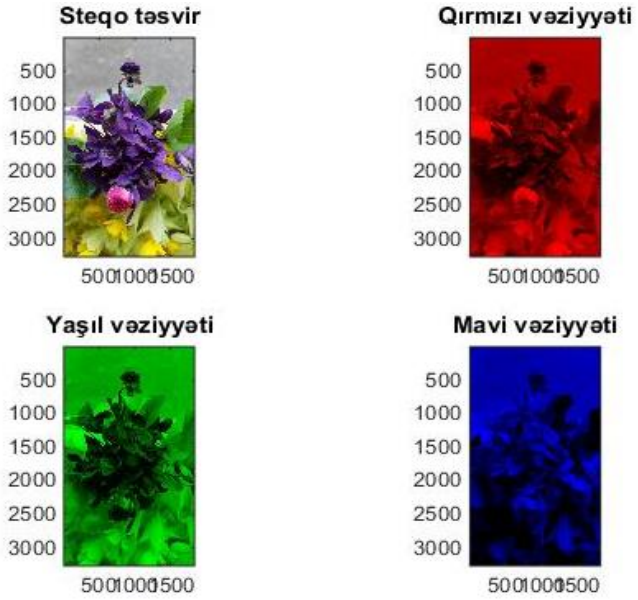
Addım 5. Fərz edək ki, məxfi informasiya bitləri $m = 11101001011.....$kimi verilib.

$$m_1 = ''11_2"onda\ \ d_4 = 3_4$$
$$m_2 = ''10_2"onda\ d_4 = 2_4$$
$$m_4 = ''1_2"onda\ \ d_4 = 1_4$$

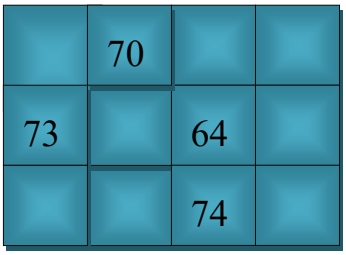
Addım 6. Sonra isə dördlük say sisteminə çevrilmiş məxfi informasiya bitləri rəngli təsvirin mavi kanal blokunun müvafiq pikselləri ilə cəmlənir:

$$S_{1,2} = 67 + 3 = 70$$
$$S_{2,1} = 71 + 2 = 73$$
$$S_{2,2} = 73 + 1 = 74$$

Beləliklə, şəkil 3.2.3. də göstərilən steqo-təsvir alınır.



Şəkil 3.2.3. Steqo-təsvir



Şəkil 3.2.4. Steqo-təsvirin mavi kanal bloku və SIFT ilə müəyyən edilmiş açar nöqtə pikselləri

Məxfi informasiya bitlərinin steqo-təsvirdən çıxarılmasının rəqəmsal nümunəsi.

Addım 1. SIFT alqoritmi ilə steqo-təsvirdə müəyyən edilmiş açar nöqtələr yəni, steqo-piksellər $S(i,j)=70,\ 73,\ 64,\ 74$-ə bərabərdir.

Addım 2. Konteyner təsvirin SIFT alqoritmi ilə açar nöqtə pikselləri müəyyən edilir. Onlar da müvafiq olaraq $p(i,j)=67,\ 71,\ 64,\ \ 73$-ə bərabərdir.

Addım 3. Yuxarıdakı addımlara əsasən hesablama aşağıdakı kimi aparılacaq,

$$M_1 = 70-67=3$$
$$M_2 = 73-71=2$$
$$M_3 = 64-64=0$$
$$M_4 = 74-73=1$$

Addım 4. Addım 3-də alınan qiymətlər yenidən ikilik say sisteminə çevrilir.

$$M_1 = 3_4 = 11_2$$
$$M_2 = 2_4 = 10_2$$
$$M_3 = 0_4 = 0_2$$
$$M_4 = 1_4 = 1_2$$

Burada məxfi informasiya bitinin ilk iki biti “11” daha sonra sırası ilə digər bitlər “10”, “0”, “1” əldə edilir. Göründüyü kimi yalnız $M_3=0$ olur, deməli bu pikseldə heç bir məxfi informasiya biti gizlədilməyib.

Addım 5. Addım 4-dən alınan qiymətlər ardıcıl olaraq aşağıdakı kimi düzülür, beləliklə, məxfi informasiya bitləri $m=11101001011$.....yenidən əldə edilir.

Təklif edilən hər iki alqoritmin nəticələrinə baxsaq, görərik ki, hər iki alqoritmdə də vizual keyfiyyət və gizlədilmiş məxfi informasiya bitlərinin həcmi tələblərə uyğundur. İstifadəçinin istəyinə uyğun olaraq yüksək vizual keyfiyyət tələb olunan zaman dördlük say sisteminin əsasında olan alqoritm, daha çox məxfi

informasiya gizlədilməsi tələb olunan zaman isə səkkizlik say sisteminin əsasında olan alqoritm istifadə edilə bilər.

Bu fəsildə təklif edilən rəngli təsvirdə məxfi informasiya bitlərinin gizlədilmə alqoritmlərinin eksperimental tədqiqi aparılaraq, effektiv olması təsdiq edilib. Eksperimentlərin nəticələri dördüncü fəsildə 4.4. başlığında verilib.

Üçüncü fəsil üzrə nəticələr

1. Rəngli təsvirlərdə məxfi informasiya gizlədilməsi üçün iki alqoritm təklif edilib;

- Böyük həcmli məxfi informasiya gizlədilmə alqoritmi. Bu alqoritmdə əvvəlcə rəngli təsvirin mavi kanalında SIFT alqoritmi vasitəsilə açar nöqtə pikselləri tapılır. Burada SIFT alqoritminin istifadəsi təklif edilən alqoritmdə təhlükəsizliyi artırır. Məxfi informasiyanın gizlədilməsi üçün mavi kanalın seçilməsi steqo-təsvirdə məxfi informasiyanın vizual olaraq aşkarlanmasını çətinləşdirir. Daha sonra məxfi informasiya bitləri yeni alqoritm vasitəsilə konteyner təsvirinə yerləşdirilir. Yerləşdirmə zamanı ənənəvi üsullardan fərqli olaraq səkkizlik say sistemindən istifadə edilir və steqo-təsvir yaradılır. Bu zaman seçilmiş bitlərin sayı digər steqanoqrafik alqoritmlərə nisbətən daha çox olur. Alqoritm keyfiyyət göstəricilərinin tələblərini ödəyərək bir çox steqo hücümlara qarşı dayanıqlı olması aparılan eksperimental analizə görə sübut edilib.
- Yüksək vizual keyfiyyət prioritetli məxfi informasiya gizlədilmə alqoritmində də həmçinin SIFT alqoritmi vasitəsilə rəngli təsvirin mavi kalanındakı açar nöqtə pikselləri aşkar edilərək məxfi informasiyanın yerləşdirilməsi üçün istifadə edilir. Lakin burada məxfi informasiya bitləri dördlük say sistemindən istifadə etməklə konteyner təsvirinin müvafiq pikselinə yerləşdirilir. Burada alqoritmin adından da göründüyü kimi əsasən yüksək vizualılıq əldə etmək əsas götürülüb. Lakin buna baxmayaraq, digər steqoalqorimlərdəki ikilik say sistemi vasitəsilə məxfi informasiyanın yerləşdirilməsinə nisbətən daha çox bit yerləşdirilir. Amma səkkizlik say sistemi ilə seçilən bitlərə nisbətən isə az

bitlər seçilir. Bu alqoritmlərdə də keyfiyyət göstəriciləri, steqo hücumlara qarşı dayanıqlılıq nəzərə alınmışdır və ətraflı olaraq dördüncü fəsildə verilmişdir.

2. Hər iki alqoritmdə məxfi informasiya bitləri gizlədiləcək namizəd piksellərin seçilməsi üçün SIFT alqoritmindən istifadə edilib.

3. Məxfi informasiya biti gizlədilmiş steqo-piksellər SIFT aqloritmi ilə müəyyən edilən açar nöqtələr olduğu üçün məxfi informasiya bitləri ardıcıl deyil, xaotik şəkildə gizlədilir.

IV FƏSİL. TƏKLİF EDİLƏN ALQORİTMLƏRİN EKSPERİMENTAL TƏDQİQİ

Fəsil 2 və Fəsil 3-də təqdim edilən alqoritmlərin effektivliyini qiymətləndirmək üçün bu fəsildə onların eksperimental nəticələri verilmişdir.

Ümumiyyətlə, steqanoqrafik alqoritmlər qiymətləndirilərkən üç kateqoriyaya nəzər yetirilir:

- Konteyner təsvirinə məxfi informasiya gizlədildikdən sonra vizual dəyişməsi;
- Konteyner təsvirinə gizlədilmiş məxfi informasiyanın həcmi;
- Yaradılmış steqo-təsvirin dayanıqlığı.

Bu kateqoriyalara əsasən təklif edilən alqoritmlərin hər birində konteyner təsvirə məxfi informasiya biti gizlədildikdən sonra əldə edilən steqo-təsvir ilə ilkin konteyner təsvir arasındakı vizual oxşarlığı yoxlamaq üçün pik siqnal səs-küyü dərəcəsi olan PSNR (Peak signal noise rate), Orta kvadratik xətanı göstərən MSE (Mean square error), struktur oxşarlıq dərəcəsi SSİM (structural similarity index measure), konteynerə gizlədilmiş məxfi informasiyanın həcmini ölçmək məqsədilə HC qiymətləri və dayanıqlılığı yoxlamaq üçün isə steqoanaliz üsullarından istifadə edilmişdir [77, s. 77-80].

Təklif edilən hər alqoritmin dayanıqlılığı histoqram steqoanaliz üsulu və RS, yəni ikili statistik üsul ilə analiz edilib.

Ümumiyyətlə, steqanoqrafiya sahəsində hər bir alqoritmə uyğun bir steqoanaliz alqoritmləri var. Belə ki, bir alqoritm üçün istifadə edilən steqoanaliz alqoritmi digər alqoritm üçün uğurlu nəticə verməyə bilər. Buna əsasən də təklif edilən alqoritmlər, həmin alqoritmə uyğun olan ikili statistik üsul (RS steqoanalizi) və histoqram steqoanaliz üsulu ilə yoxlanılaraq sınaqdan keçirilib.

Steqoanalitikin steqo-sistemə hücum etməsi üçün müəyyən informasiyaları bilməsi lazımdır. O, bildiyi informasiyalara görə hücum modelini müəyyən edir. Hücum modellərinin beş kateqoriyası var:

- *Steqo-hücum:* analiz üçün sadəcə steqo-təsvir məlumdur. Bu vəziyyətdə steqoanalitik yalnız dəyişdirilmiş bir konteynerə sahibdir, onun vasitəsilə məxfi informasiyanın mövcudluğunu müəyyən etməyə çalışır. Bu tip steqanoqrafik hücum çox rast gəlinən situasiyaların əsasını təşkil edir.

- *Bilinən konteyner hücumu:* təsvirin məxfi informasiya gizlədilmədən əvvəlki və sonrakı vəziyyəti məlumdur. Bilinən konteyner haqqında məlumatlı hücumlar o zaman mümkündür ki, steqoanalitik məxfi informasiyanı gizlətmək üçün hansı konteynerdən istifadə olunduğunu dəqiq bilmək imkanına malik olsun. Bu hücum bir dəfə ələ keçirilmiş konteynerin və məxfi informasiyanın mövcudluğundan asılı olaraq gələcəkdə informasiyaların gizlədilməsi faktının müəyyən edilməsini təmin edir.

- *Məxfi informasiyanın məlum olması halı*: bu halda elə hesab edilir ki, steqoanalitik hansı informasiyanın gizlədiləcəyini müəyyən edə bilir, lakin bunun üçün istifadə olunacaq konteyneri müəyyən etmək imkanı yoxdur. Bu hücum növü, sistemin eyni konteynerdən istifadə edərək, göndərilən informasiyaların tutulmasına və izlənməsinə qarşı müqavimətini xarakterizə edir. Bu tip hücum, həm də istifadə olunan steqanoqrafik sistemlərin növünü müəyyən etməyə imkan verir.

- *Seçilmiş steqo-hücum:* steqanoqrafik alqoritm və steqo-təsvir məlumdur. Əvvəlkilərə bənzər bu hücumlar eyni məxfi informasiyanın müxtəlif konteynerlərlə təkrar istifadəsi halında steqo-sistemin açıqlamaya qarşı müqavimətini təyin etməyə imkan verir.

- *Seçilmiş informasiya hücumu*: steqoanalitik steqo-təsviri analiz edə bilmək üçün müxtəlif informasiyalar toplayır, steqanoqrafik açarlar istifadə edir və bu üsullar ilə alqoritmi tapmağa çalışır.

Yuxarıda sadalanan hücum növlərinə aşağıdakıları da əlavə edə bilərik. Hansı ki, son dövrlərdə steqanoqrafiya sahəsində bu hücum növləri də aktual hesab olunur.

- Saxtakarlıq hücumları: bu hal məxfi informasiyanın mövcudluğunu müəyyən etmək və ya onu çıxarmaq üçün nəzərdə tutulmur, onlar məxfi informasiyaları dəyişdirmək və ya bu cür ötürülməni imitasiya etmək üçün istifadə olunur.

- Məxfi informasiya ötürülməsinə qarşı hücumlar: məxfi informasiyaları məhv etmək və gizli kanalların ötürücülüyünü azaltmaq üçün istifadə olunur.

Təklif edilən alqoritmlərin yoxlanılması üçün konteyner təsvir kimi istifadə edilən bütün təsvirlərə, eləcə dəsteqo-təsvirlərə RS steqoanalizi tətbiq edilib və nəticələri göstərilib.

4.1. Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritminin eksperimental tədqiqi

Bu bölmədə təklif edilən ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritminin eksperimental nəticələri verilib. Bu alqoritm steqo-təsvir ilə konteyner təsvir arasındakı vizual oxşarlıq saxlanılmaqla gizlədiləcək məxfi informasiya bitlərinin sayını artırmağa imkan verir. Alqoritmin həyata keçirilməsində giriş təsviri kimi rəqəmsal təsvirdən istifadə edilib.

Təklif edilən alqoritm iki mərhələdən ibarətdir. Birinci mərhələdə seçilmiş konteyner təsvirində steqo-açar vasitəsilə məxfi informasiya gizlədilməsi üçün piksellər müəyyən edilir, sonra təsviri 2x2 bloklara bölünür. Daha sonra həmin blokda minimum qiymətə malik olan piksel ilə digər piksellər arasında fərq qiyməti hesablanır. Açar vasitəsilə müəyyən edilən minimumdan fərqli olan piksellərə LSB alqoritmindən istifadə edərək məxfi bitlərin daxil edilməsi nəzərdə tutulur.

Təklif olunan alqoritmin eksperimental tədqiqatları ədəbiyyatda təqdim olunan bir neçə alqoritmin eksperimental tədqiqatları ilə müqayisə edilmişdir. İşlənilən alqoritmin üstünlükləri kimi daha çox məxfi informasiya biti gizlətməklə, yüksək vizual keyfiyyətin saxlanılması və hesablama üsullarının digərlərindən asan və qısa zaman ərzində məxfi informasiya gizlətmək qabiliyyətinə malik olmasını və steqo-hücumlara qarşı dayanıqlılığını göstərmək olar.

Konteyner və steqo-təsvirlərin oxşarlıq dərəcəsinin və gizlədilmiş məxfi informasiya həcminin tədqiqi.

İstifadə olunan standart təsvirlərdən asılı olmayaraq, təklif edilən alqoritmdə iki təsvir arasındakı vizual oxşarlıq yəni PSNR 50 dB-dən yuxarıdır. Cədvəl 4.1.1-dən

asanlıqla görmək olar ki, təklif olunan alqoritm müqayisə edilən digər alqoritmlərdən daha üstün keyfiyyət göstəricilərinə malikdir. Sınaqların nəticələri sonrakı tədqiqatlarda gizlədiləcək məxfi informasiya bitlərinin sayının artırılmasına zəmin yaradır.

Alınan tədqiqat nəticələrinin etibarlılığını yoxlamaq üçün USC-SIPI (ABŞ) [99] təsvir bazasından götürülmüş 50 təsvir üzərində eksperimentlər aparılmışdır, onlardan 4-ü cədvəl 4.1.1-də göstərilmişdir. Təcrübələr MATLAB \ R2014b proqramından istifadə etməklə aparılmışdır.

$$PSNR = 10 \times \log_{10}\left(\frac{Max}{MSE}\right) \tag{4.1.1}$$

(4.1.1) düsturu müqayisə edilən steqo-təsvir ilə ilkin təsvir arasındakı oxşarlıq dərəcəsini müəyyən edir. İnsanın görmə sistemi (İGS) 36 dB-dən çox fərqi qəbul edə bilmir. PSNR-in qiyməti steqo-təsvirin vizual keyfiyyəti ilə birbaşa bağlıdır. PSNR-in qiyməti nə qədər yüksək olarsa, müqayisə edilən təsvirlər, yəni ilkin təsvir ilə steqo-təsvir bir o qədər oxşar olar. Test edilən təsvirlərin keyfiyyət göstəriciləri HC və PSNR-in orta qiymətləri bərabərdir: HC- 435202 bit; PSNR- 38.8096 dB.

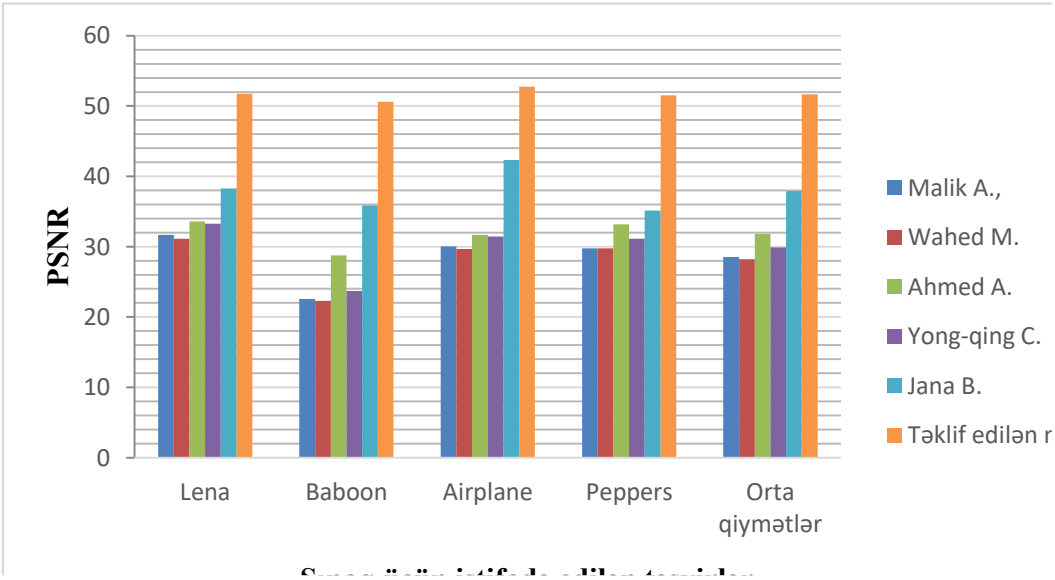
Cədvəl 4.3.1-də sınaqdan keçirilmiş 50 təsvirdən 4-nün nəticəsi, yəni konteyner təsvir və steqo-təsvir arasındakı PSNR qiymətləri, eyni zamanda təklif olunan alqoritmin son illərdə işlənib hazırlanmış yeni alqoritmlər ilə PSNR, alqoritmin yerinə yetirilmə müddəti və steqo-təsvirə gizlədilmiş məxfi informasiya bitlərinin həcmlərinin (HC) müqayisəsi göstərilir.

Daha geniş təsəvvür yaratmaq və ikinci fəsildə araşdırılan alqoritmlərlə məhdudlaşmamaq məqsədilə ədəbiyyatda uğurlu nəticələri olan və müqayisə edilən Malik A. [71, s. 2454-7190] və Wahed M. [101, s. 10795-10819]-in təklif etdikləri alqoritmlərın göstəriciləri də müqayisə üçün cədvələ daxil edilib (Cədvəl 4.1.1).

Cədvəl 4.1.1.

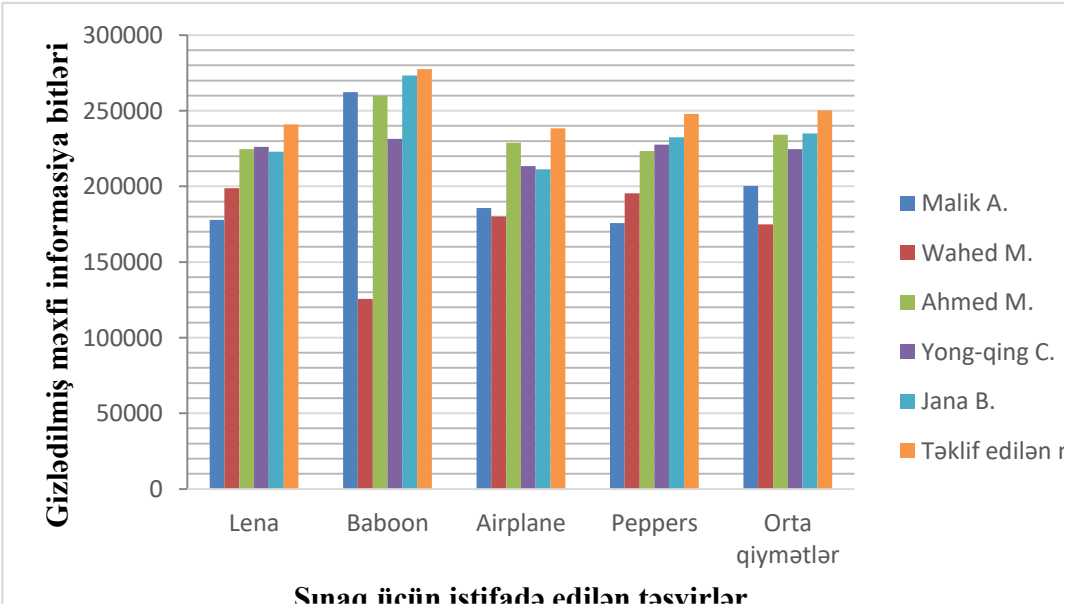
Steqo-təsvirin keyfiyyət göstəricilərinin müqayisəli analizi

Giriş təsvirləri	**Keyfiyyət göstəriciləri**	**Malik A., Sikka G. .** [71, s. 2454-7190], **2018**	**Wahed M.A., Nyeem, H** [101, s. 10795-10819], **2019**	**Ahmad A.M., [18, s. 7181-7205], 2019**	**Yong-qing C. [25, s. 271 - 350] 2020**	**Jana B., Giri D., [45, s.239-248] 2015**	**Təklif edilən alqoritm**
Lena	**HC (bit)**	177777	198902	224528	226085	223031	240962
	PSNR (dB)	31,67	31,14	33,60	33,27	38,25	51,73
Baboon	**HC (bit)**	262272	125562	259737	231401	273235	277492
	PSNR (dB)	22,57	22,29	28,77	23,70	35,85	50,62
Airplane	**HC (bit)**	185676	179961	228863	213460	211321	208392
	PSNR (dB)	30,01	29,66	31,67	31,43	42,34	52,74
Peppers	**HC (bit)**	175669	195490	223295	227493	232563	247864
	PSNR (dB)	29,78	29,78	33,18	31,13	35,12	51,53
Orta qiymətlər	**HC (bit)**	205349	249979	234106	237110	235037	**243677**
	PSNR (dB)	28,50	28,22	31,8	29,88	38,39	**51,65**



Şəkil 4.1.1. PSNR göstəricilərinin müxtəlif təsvirlərdən asılılığı

Şəkil 4.3.1. dən göründüyü kimi təsvirlər bazasından götürülmüş hər 5 təsvirlə aparılan eksperimentlərdə bu fəsildə təklif edilən alqoritm öz göstəricisinə görə müqayisə edilən alqoritmlərdən üstündür.

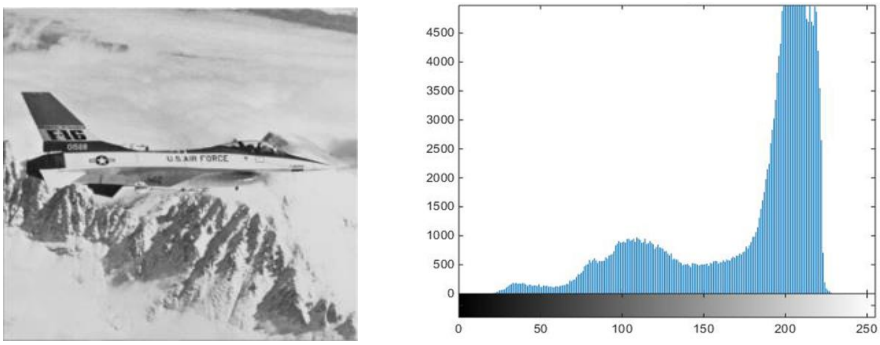


Şəkil 4.1.2. Gizlədilmiş məxfi informasiya bitlərinin müxtəlif təsvirlərdən asılılığı

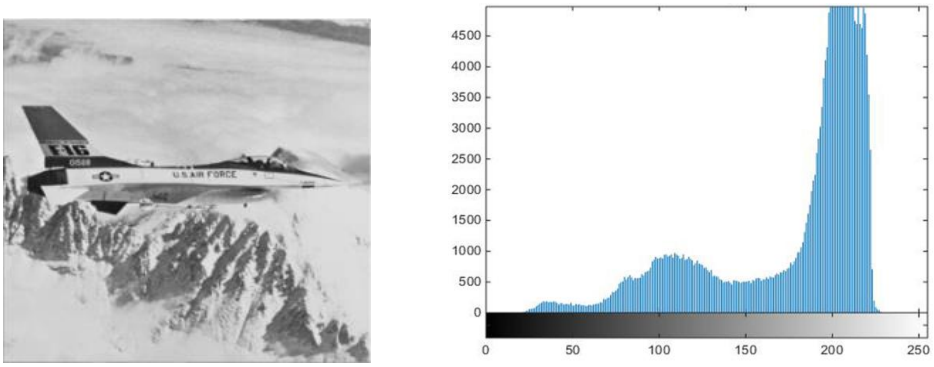
Şəkil 4.1.2.-də müxtəlif təsvirlərdə təklif edilən alqoritm və ədəbiyyatda təklif edilən alqoritmlər əsasında nə qədər məxfi informasiya gizlədilməsinin mümkün olması göstərilmişdir. Şəkildən məlum olur ki, təklif edilən alqoritm müqayisə edilən digər alqoritmlərə nisbətən daha çox məxfi informasiya biti gizlədilməsini təmin edir.

Alqoritmin histoqram steqoanaliz ilə tədqiqi.

Alqoritmin göstəricilərinin etibarlılığını yoxlamaq üçün yenə gizlətmə alqoritmlərinin effektivliyi tətbiq edilən standart təsvirlərdən ilkin təsvir kimi istifadə edilib. İlkin təsvirlər ilə onlara uyğun olan steqo-təsvirlərin histoqram qrafikləri şəkil 4.1.3 və şəkil 4.1.4-də verilib. Şəkillərdən məlum olur ki, müqayisə edilən təsvirlər, əsasən eyni histoqrama malikdirlər. Bu da öz növbəsində müqayisə edilən təsvirlərin yüksək bənzərlik dərəcəsinə malik olması deməkdir.



Şəkil 4.1.3. Konteyner təsvir və onun histoqramı



Şəkil 4.1.4. Steqo-təsvir və onun histoqramı

Təklif edilən alqoritmin ikili statistik steqoanaliz ilə tədqiqi

Təklif edilən alqoritmin dayanıqlılığı histoqram steqoanalizindən başqa həmçinin RS steqoanalizi ilə daha geniş yoxlanılmışdır.

Bu analiz, təsvirlərdə fəza korelyasiyası əsasında yaradılmış həssas ikili statistikadan istifadə edir. RS steqoanalizi 24 bit rəngli və 8 bit boz təsvirlərdə istifadə olunur. RS steqoanaliz təsvir faylları üzərində ən az əhəmiyyətli bitin əvəz edilməsi metodu əsasında (LSB Insertion Methods) məxfi informasiya gizlədilib-gizlədilmədiyini aşkarlamaq üçün istifadə edilir. Bu növ steqoanaliz aşağıdakı qaydada həyata keçirilmişdir.

Bunun üçün əvvəlcə 4 boş konteyner təsvirinə (Lena, baboon, airplane, peppers) RS steqoanalizi tətbiq edilib və nəticələr cədvəl 4.1.2-də göstərilib.

Cədvəl 4.1.2.
Konteyner təsvirlərin RS steqoanalizi

Konteyner təsvir	$\lvert R_m - R_{-m} \rvert$ (dB)	$\lvert S_m - S_{-m} \rvert$ (dB)
Lena	0,0078	0,0088
Baboon	0,0057	0,0067
Airplane	0,0063	0,0065
Peppers	0,0093	0,0083

Daha sonra isə konteyner təsvirinə müxtəlif həcmdə məxfi informasiya bitlərinin gizlədilməsindən sonra (bu halda konteyner təsvir artıq steqo təsvir olur) $|R_m - R_{-m}|$-nin və $|S_m - S_{-m}|$ -i qiymətləri hesablanıb və nəticəsi cədvəl 4.1.3.- də verilib.

Cədvəl 4.1.3

Steqo-təsvirlərin RS steqoanaliz nəticələri

Steqo−təsvir	**RS steqoanalizi (dB)**	**Gizlədilmiş məxfi informasiya həcmi (bayt)**			
		1000	5000	10000	15000
Lena	$\|R_m - R_{-m}\|$	0,0080	0,0087	0,0093	0,0099
	$\|S_m - S_{-m}\|$	0,0091	0,0095	0,0097	0,0099
Baboon	$\|R_m - R_{-m}\|$	0,0064	0,0079	0,0093	0,0052
	$\|S_m - S_{-m}\|$	0,0073	0,0163	0,0031	0,0043
Airplane	$\|R_m - R_{-m}\|$	0,0093	0,0095	0,0099	0,0103
	$\|S_m - S_{-m}\|$	0,0082	0,0086	0,0025	0,0026
Peppers	$\|R_m - R_{-m}\|$	0,0097	0,0098	0,0086	0,0093
	$\|S_m - S_{-m}\|$	0,0085	0,0085	0,0092	0,0098

Yuxarıdakı cədvəldə RS steqoanalizin nəticəsində alınan $|R_m - R_{-m}|$ və $|S_m - S_{-m}|$ fərq qiymətlərinin 0-a yaxın olması alqoritmin dayanıqlılığını təsdiq edir.

Cədvəl 4.1.3.-də verilən nəticələrdən aydın olur ki, tədqiq olunan alqoritmin tətbiqi zamanı heç bir steqoanalitik (bədniyyət şəxs) bu alqoritmlə göndərilən və bu gün məlum olan steqoanaliz alqoritmləri ilə məxfi informasiyanı ələ keçirə bilməz, çünki müxtəlif təsvirlər istifadə edilərək gizlədilən məxfi informasiya həcmindən asılı olmayaraq dayanıqlılıq göstəriciləri təhlükəli həddi keçmirlər və stabil olaraq sıfıra çox yaxın olan qiymətlər alırlar.

Alqoritmin hesablama mürəkkəbliliyinin eksperimental tədqiqi

Hər bir təklif edilən alqoritmin hesablama mürəkkəbliyinin, yəni alqoritmdə istifadə edilən bütün prosedurların yerinə yetirilməsinə sərf edilən zamanın həlledici əhəmiyyəti var. Alqoritmin, hətta çox yüksək göstəriciləri olsa belə, hesablamalara sərf edilən zamanı da həlledici parametrlərdən biri hesab edilir və seçim zamanı iki və ya üç alqoritmdən ən az zaman tələb edən alqoritmə üstünlük verilir. Bu göstərici deyilənlər nəzərə alınaraq experimental tədqiq edilib. Eksperimentlər beynəlxalq təsvirlər bazasından [94, s. 110-119] götürülərək istifadə edilib.

Alqoritmin hesablama mürəkkəbliyini *(*Alqoritmin yerinə yetirilmə müddəti) yoxlamaq üçün aşağıdakı eksperiment aparılmışdır. Bunun üçün MATLAB/ R2014b proqramından istifadə edilmişdir. Müxtəlif konteyner təsvirinə məxfi informasiya gizlədilib və alınan steqo-təsvirdə informasiyanın gizlədilmə və steqo-təsvirdən çıxarılma vaxtı yoxlanılıb. Eksperimentlər aparılarkən müxtəlif standart təsvirlərdən istifadə etməklə konteyner təsvirə müxtəlif həcmli informasiya gizlədilib. Bu, həm informasiyanın gizlədilməsinə, həm də steqo-təsvirdən çıxarılma prosedurlarına aid edilib. Alınan nəticələr cədvəl 4.1.4. -də verilib.

Cədvəl 4.1.4.

Alqoritmin realizə olunma müddəti

Konteyner təsvir	Məxfi informasiya həcmi (bayt)	İnformasiyanın gizlədilmə vaxtı (san)	İnformasiyanın çıxarılması vaxtı (san)
Lena	5000	0,024	0,0204
	10000	0,029	0,0205
	15000	0,029	0,0209
Baboon	5000	0,027	0,0212
	10000	0,026	0,0211
	15000	0,029	0,0230
	15000	0,027	0,0232
Peppers	5000	0,023	0,0213
	10000	0,026	0,0233

	15000	0,029	0,0252

Cədvəldəki nəticələrdən görünür ki, hər iki prosedur həyata keçirilərkən hesablamalara sərf edilən zaman 0,02 san. ətrafında variasiya edilərək 0,03-ə çatmır. Bu isə ədəbiyyatda göstərilən alqoritmlərın hesablanma müddətindən azdır və demək olar ki, daha yaxşı göstərici hesab edilə bilər. Təsvirdən-təsvirə müəyyən fərqlər qeyd olunur, lakin bu, qəbul ediləndir, çünki istifadə edilən təsvirlərin strukturu və xarakteristikaları da eyni deyil. Həmin hal gizlədilən informasiyanın həcminə də aid edilir.

Cədvəl 4.1.5.

Təklif edilən alqoritmin realizə müddətinin digər alqoritmlərlə müqayisəsi.

Təsvirlər	Alqoritmin realizə müddəti (san)	Malik A., Sikka G. [71, s. 2454-7190], 2018	Wahed M.A., Nyeem, H [101, s. 10795-10819], 2019	Ahmad A.M., [18, s. 7181-7205], 2019	Yong-qing C. [25, s. 271-350] 2020	Jana B., Giri D., [45, s.239-248] 2015	Təklif edilən alqoritm
Lena	İnformasiyanın gizlədilməsi	0,031	0,038	0,036	0,033	0,039	0,029
	İnformasiyanın çıxarılması	0,031	0,04	0,0039	0,035	0,036	0,021
Baboon	İnformasiyanın gizlədilməsi	0,042	0,046	0,039	0,035	0,041	0,026
	İnformasiyanın çıxarılması	0,042	0,043	0,037	0,034	0,039	0,021
Airplane	İnformasiyanın gizlədilməsi	0,037	0,029	0,041	0,038	0,039	0,026
	İnformasiyanın çıxarılması	0,037	0,025	0,039	0,035	0,034	0,027
Peppers	İnformasiyanın gizlədilməsi	0,042	0,033	0,036	0,037	0,048	0,028
	İnformasiyanın çıxarılması	0,034	0,031	0,033	0,035	0,046	0,023

Cədvəl 4.1.5.-dəki nəticələr göstərir ki, hər alqoritmin və istifadə edilən hər konteyner təsvirin zaman göstəriciləri bir-birindən fərqlidir. Belə ki, informasiyanın

gizlədilmə mərhələsində çox zaman 0,048 saniyə Papper təsvirində [45, s. 239-248] qeyd olunur. Həmin təsvirdə təklif edilən alqoritmdə isə bu göstərici 0,028 saniyəyə bərabərdir. İnformasiyanın çıxarılması mərhələsində isə maksimal göstərici 0,046 saniyədir. Yenə də Papperdə təkrarlanır, halbuki müəllifin işindəki məxfi informasiyanın konteyner təsvirdən çıxarılmasına aid göstərici Airplane təsviri üçün 0,034 saniyəyə bərabərdir.

Ümumilikdə isə görünən odur ki, orta qiymətləri nəzərə alanda burada təklif edilən alqoritmin hesablama mürəkkəbliyini əks etdirən zaman göstəricisi alqoritmlərdən, prosedurlardan, təsvirlərdən asılı olmayaraq ən minimaldır.

Steqo-alqoritmlərin keyfiyyət göstəricilərinə alqoritmin işləmə müddətini də əlavə edə bilərik. Belə ki, təklif edilən alqoritmin realizəsi üçün minimum vaxt tələb olunur. Bunun əyani sübutu cədvəl 4.1.4 və cədvəl 4.1.5-də göstərilib.

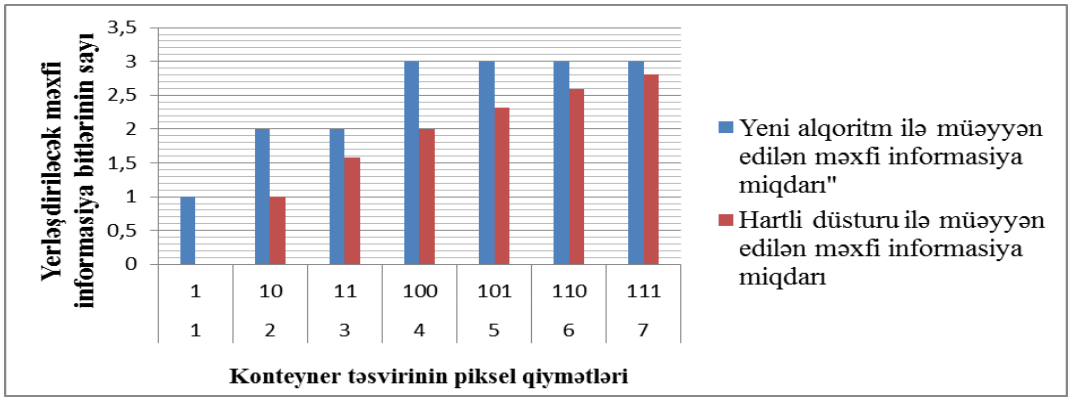
Burada rəqəmsal təsvirlərdə informasiyanın gizlədilməsi üçün yeni steqanoqrafik alqoritm təqdim edilir. Müəlliflər adətən təsvirin vizual keyfiyyətini yaxşılaşdırmaq üçün interpolyasiya texnikasından istifadə edirlər. Bunun əksinə olaraq, təklif edilən yeni alqoritmdə minimum piksel bitinin müəyyən edilməsi və istifadəsi üsulu ilə birlikdə məxfi informasiyanın gizlədilməsi alqoritmindən istifadə edilir.

4.2. Təsvir interpolyasiyasına əsaslanan steqanoqrafik məlumat gizlətmə alqoritminin eksperimental tədqiqi

Təcrübələr müxtəlif gizlətmə üsullarının effektivliyini qiymətləndirmək üçün təsvirlər bazasından [99] götürülmüş 512x512 ölçülü 8 standart təsvir üzərində aparılmışdır. Bu təsvirlər təklif olunan məxfi informasiyanın gizlədilməsi alqoritmini yoxlamaq üçün ilkin təsvir kimi istifadə edilmişdir. Hər bir təsvir burada təklif olunan alqoritmə uyğun işlənmişdir.

İlk olaraq təklif edilən alqoritmin Hartli düsturu ilə gizlədiləcək məxfi informasiya miqdarının müəyyən edilməsi ilə müqayisədə daha çox məxfi bit gizlədilməsinə imkan yaradan eksperimentlərin nəticələrinə nəzər salaq. İşlənilən

alqoritmin digər alqoritmlər ilə müqayisəsinin eksperimental nəticələrinin qrafiki Şəkil 4.2.1.-də verilir. Burada interpolyasiya edilmiş konteyner təsvirinin piksellərinin 1÷7 intervalında qiymətləri və həmin qiymətlərə uyğun piksellərə yerləşdiriləcək məxfi informasiya bitlərinin sayı diaqramlar əsasında göstərilmişdir.



Şəkil 4.2.1 Konteyner pikselinin 1÷7 intervalındakı qiymətlərində məxfi informasiya bitlərinin yerləşdirilməsinin müqayisəsi

Şəkil 4.2.1-dən göründüyü kimi konteyner təsvirin piksellərinin 1÷7 intervalındakı qiymətlərində pikselin qiymətindən asılı olmayaraq gizlədilən məxfi bitlərin sayı 3-ə bərabərdir və buna baxmayaraq təsvirin vizual keyfiyyəti pozulmur. Konteyner təsvirinin piksel qiymətlərinin müxtəlif qiymət intervallarında yerləşdirilmiş bitlərin miqdarından asılılıqlarını əks etdirən digər qrafiklər dissertasiyaya əlavədə verilmişdir. Digər qrafiklərdə konteyner təsvirinin piksel qiymətinin müxtəlif qiymət intervallarında qiymət artdıqca daha çox məxfi informasiya biti gizlətmək imkanının olması təsdiqlənir. Təqdim edilən diaqramlardan məlum olur ki, yeni alqoritmə əsasən daha çox məxfi informasiya biti gizlətmək mümkündür.

Hazırlanmış alqoritmin səmərəliliyini qiymətləndirmək üçün burada təklif olunan məxfi informasiyanın gizlədilməsi alqoritminin eksperimental göstəriciləri son dövrdə işlənib hazırlanmış uğurlu nəticələri olan iki alqoritmlə müqayisə edilib [25, s. 271-350, 71, s. 7181-7205].

Yeni alqoritmin məqsədi daha yüksək həcmdə məxfi informasiya bitlərini yerləşdirmək və steqo-təsvirin minimal təhrifinə nail olmaqdır. Cədvəl 4.2.1-də təklif edilən alqoritmin digər alqoritmlərlə müqayisəsi verilmişdir. Cədvəldən məlum olur

ki, təklif olunan alqoritm digər müqayisə edilən alqoritmlər ilə demək olar ki, eyni həcmdə məxfi informasiya biti gizlətdiyi təqdirdə konteyner təsvir ilə steqo-təsvir arasında daha yüksək oxşarlıq qiymətləri (PSNR) əldə edir. Böyük həcmdə məxfi informasiya bitləri daxil edildikdən sonra konteyner təsvir ilə steqo-təsvirin yüksək oxşarlıq dərəcəsi təklif olunan alqoritmin üstünlüyü hesab edilə bilər.

Konteyner və steqo-təsvirlərin oxşarlıq dərəcəsinin və gizlədilmiş məxfi informasiya həcminin tədqiqi.

Burada əvvəlki gizlədilmə alqoritminin tədqiqi zamanı istifadə edilən təsvirin vizual keyfiyyətinin ölçülməsi tədqiq edilir. İki müqayisə edilən rəqəmsal təsvirlərin bənzərlik dərəcəsi müəyyən olunur. Ona görə də, bu barədə geniş izah tələb olunmadığından qısa məlumat verməyə üstünlük veririk. Vizual keyfiyyəti ölçmək üçün yenə də PSNR istifadə edilir. Təklif edilən alqoritmin digər alqoritmlərlə müqayisəsi Cədvəl 4.2.1.-də verilmişdir. Sınaqdan keçirilmiş 50 təsvirdən səkkizinin nəticəsi, yəni konteyner təsvir və steqo-təsvir arasındakı PSNR qiymətləri, eyni zamanda təklif olunan alqoritmin son illərdə işlənib hazırlanmış yeni alqoritmlər ilə PSNR və steqo-təsvirə gizlədilmiş məxfi informasiya bitlərinin həcmlərinin (HC) müqayisəsi göstərilib.

Cədvəl 4.2.1.

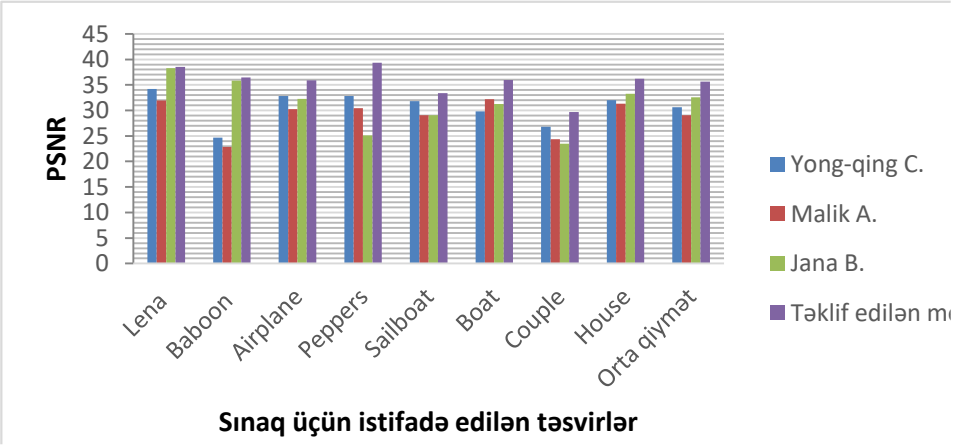
Steqo-təsvirlərin keyfiyyət göstəricilərinin müqayisəsi

Giriş təsvirləri	**Keyfiyyət göstəriciləri**	**Yong-qing C. [25, s. 271-350] 2020**	**Malik A., Sikka G. [71, s. 7181-7205], 2018**	**Jana B., Giri D., [45, s.239-248] 2015**	**Təklif olunan alqoritm**
Lena	PSNR (dB) HC (bit)	34,18 369715	31,93 144887	38,25 223031	38,56 564744
Baboon	PSNR (dB) HC (bit)	24,69 651710	22,85 187141	35,85 273235	36,47 676791
Airplane	PSNR (dB) HC (bit)	32,84 334328	30,26 151269	32,24 241232	35,88 524719
Peppers	PSNR (dB) HC (bit)	32,82 374589	30,42 144177	35,12 232563	39,32 656611
Sailboat	PSNR (dB) HC (bit)	31,80 364589	29,04 175183	29,03 236132	33,36 378123
Boat	PSNR (dB) HC (bit)	29,82 343589	32,22 124236	31,26 295325	35,93 369563

Couple	PSNR (dB) HC (bit)	26,82 381589	24,36 354137	23,48 378256	29,68 400021
House	PSNR (dB) HC (bit)	32,02 236589	31,32 235325	33,27 217482	36,21 282753
Orta qiymətlər	**PSNR (dB) HC (bit)**	**30,62 382087**	**29,05 189544**	**32,31 262157**	**35,67 465390**

Test edilən təsvirlərin keyfiyyət göstəriciləri HC və PSNR-in orta qiymətləri HC- 465390 bit; PSNR- 35,67 dB bərabərdir. Cədvəldən məlum olur ki, təklif olunan alqoritm digər müqayisə edilən alqoritmlərlə demək olar ki, eyni həcmdə məxfi informasiya biti gizlətdiyi təqdirdə konteyner təsvir ilə steqo-təsvir arasında daha yüksək oxşarlıq qiymətləri (PSNR) əldə edilir. Böyük həcmdə məxfi informasiya bitləri daxil edildikdən sonra konteyner təsvir ilə steqo-təsvir arasında yüksək oxşarlıq dərəcəsinin əldə edilməsi təklif olunan alqoritmin üstünlüyü hesab edilə bilər.

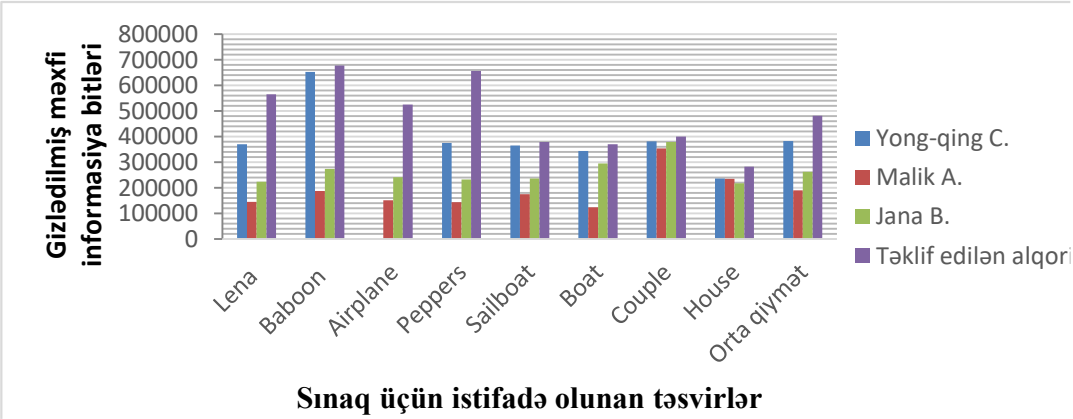
Alınan nəticələrin doğruluğunu bir daha təsdiq etmək üçün PSNR qiymətlərinin test edilən təsvirlərin növündən asılılığının müxtəlif müəlliflərin alqoritmləri ilə müqayisəsi şəkil 4.2.2.-də göstərilib. Təklif edilən alqoritmin PSNR göstəricilərinin üstünlüyü qeyd olunub.



Şəkil 4.2.2. PSNR göstəricilərinin müxtəlif təsvirlərdən asılılığı

Bütün təsvirlərdə PSNR qiymətləri yuxarıdır, bu, o deməkdir ki, məxfi informasiya bitlərinin gizlədilməsi ilə bağlı qaçılmaz pozuntular insan gözü üçün görünməz olaraq qalır. PSNR-ə əlavə olaraq, giriş təsviri və steqo-təsvirin

müqayisəsində, eləcə də alqoritmin dayanıqlılığını daha dəqiq yoxlamaq üçün histoqram steqoanalizindən istifadə olunub.



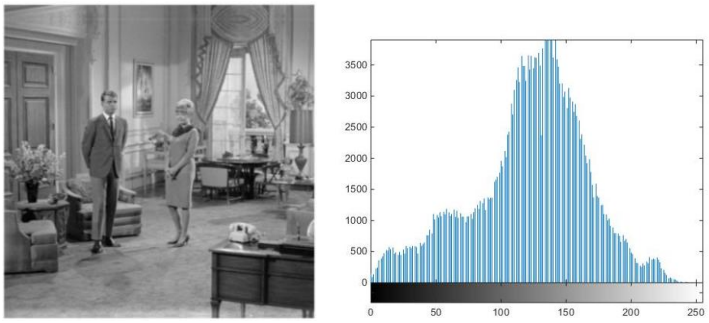
Şəkil 4.2.3. Gizlədilmiş məxfi informasiya bitlərinin müxtəlif təsvirlərdən asılılığı

PSNR-in daha yüksək qiymətləri və steqo-təsvirdə olan gizlədilmiş məxfi informasiya bitlərinin həcmi təklif olunan alqoritmin digər müqayisə olunan alqoritmlərdən üstün olduğunu göstərir (şəkil 4.2.3).

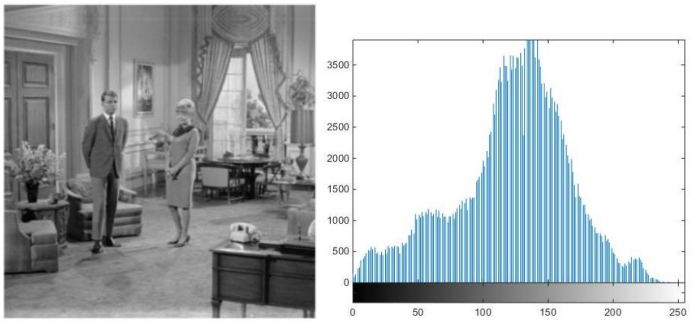
Təklif edilən alqoritmin histoqram steqoanalizi ilə tədqiqi.

Histoqram steqoanalizi səkkiz etalon konteyner və steqo-təsvirlər üzərində aparılıb. Onlardan birinin nəticəsi şəkil 4.2.4 və şəkil 4.2.5-də veirlib. Yerdə qalan 7 etalon təsvirin nəticəsi və histoqramı əlavədə verilib.

Aşağıdakı təsvirlərdə konteyner təsvirin və steqo-təsvirin histoqramları göstərilmişdir. Müqayisə edilən bütün təsvirlər demək olar ki, eyni histoqramlara malikdir. Bu da məxfi informasiyaların mövcudluğunun aşkar edilməsinin qeyri-mümkün olduğunu sübut edir**.** Göstərilən histoqramlarda steqo-təsvirlərin effektiv yoxlanılması təmin edilib və konteyner təsvir histoqramları ilə müqayisədə ciddi dəyişiklik nəzərə çarpmayıb. Müqayisə edilən təsvirlərin histoqramları identik olduğuna görə, steqo-alqoritm etibarlı və keyfiyyətlidir. Steqo-təsvir müvəffəqiyyətlə açıq kommunikasiya kanalı ilə görünməz halda ötürülə bilər.



Şəkil 4.2.4 Konteyner təsvir və onun histoqramı



Şəkil 4.2.5 Steqo-təsvir və onun histoqramı

Müqayisə edilən eksperimental təsvirlərdə heç bir vizual fərq qeyd olunmur, bu da, o deməkdir ki, vizual steqoanaliz vasitəsi ilə məxfi informasiyanın təsvirə gizlədilməsini aşkarlamaq mümkün deyil. Aşkarlanma yalnız daha dəqiq nəticə verən statistik steqoanaliz üsulları vasitəsilə mümkün ola bilər.

Təklif edilən alqoritmin ikili statistik steqoanaliz ilə tədqiqi.

Təklif edilən alqoritmin dayanıqlılığının daha dəqiq yoxlanılması üçün histoqram steqoanalizindən başqa RS steqoanalizindən istifadə edilmişdir. 4-cü fəslin əvvəlində bu statistik steqoanaliz barədə geniş məlumat verildiyinə görə təkrarlamamaq üçün bilavasitə nəticələrə diqqət yetiririk. RS steqoanalizinin nəticələri 4.2.2 və 4.2.3 cədvəllərində təqdim edilib. Tədqiqatlar yenə standart etalon təsvirlər üzərində aparılıb.

Yenə əvvəlcə boş konteyner təsvirlərinə RS steqoanalizi tətbiq edilib. Bu analizin nəticələri cədvəl 4.2.2-də göstərilib.

Cədvəl 4.2.2.

Konteyner təsvirlərin RS steqoanalizi

Konteyner təsvir	$\lvert R_m - R_{-m}\rvert$ (dB)	$\lvert S_m - S_{-m}\rvert$ (dB)
Lena	0,0078	0,0088
Baboon	0,0057	0,0067
Airplane	0,0063	0,0065
Peppers	0,0093	0,0083
Sailboat	0,0045	0,0049
Boat	0,0041	0,0043
Couple	0,0052	0,0059
House	0,0021	0,0031

Göründüyü kimi hər bir təsvirdə RS göstəriciləri sıfırdan çox azdır və bir-birinə çox yaxındır. Bu da öz növbəsində alqoritmin dayanıqlılığını təşkil edən əsas amildir.

Daha sonra konteyner təsvirinə müxtəlif həcmdə məxfi informasiya bitləri müvafiq alqoritm vasitəsilə gizlədildikdən sonra RS steqoanalizi tətbiq edilərək dayanıqlılığı test edilib. Steqoanalizin nəticələri cədvəl 4.2.3-də göstərilib.

Cədvəl 4.2.3

Steqo-təsvirlərin RS steqoanaliz nəticələri

Steqo-təsvir	**RS steqoanalizi (dB)**	**Gizlədilmiş məxfi informasiya həcmi (bayt)**			
		1000	5000	10000	15000
Lena	$\lvert R_m - R_{-m}\rvert$	0,0080	0,0087	0,0093	0,0099
	$\lvert S_m - S_{-m}\rvert$	0,0091	0,0095	0,0097	0,0099
Baboon	$\lvert R_m - R_{-m}\rvert$	0,0064	0,0079	0,0093	0,0052
	$\lvert S_m - S_{-m}\rvert$	0,0073	0,0063	0,0023	0,043
Airplane	$\lvert R_m - R_{-m}\rvert$	0,0093	0,0095	0,0099	0,0103
	$\lvert S_m - S_{-m}\rvert$	0,0082	0,0086	0,0098	0,0110
Peppers	$\lvert R_m - R_{-m}\rvert$	0,0097	0,0098	0,0100	0,0109
	$\lvert S_m - S_{-m}\rvert$	0,0085	0,0085	0,0092	0,0098
Sailboat	$\lvert R_m - R_{-m}\rvert$	0,0048	0,0051	0,0058	0,0063
	$\lvert S_m - S_{-m}\rvert$	0,0052	0,0055	0,0062	0,0065
Boat	$\lvert R_m - R_{-m}\rvert$	0,0044	0,0047	0,0053	0,0058

	$\lvert S_m - S_{-m}\rvert$	0,0046	0,0049	0,0057	0,0064
Couple	$\lvert R_m - R_{-m}\rvert$	0,0056	0,0059	0,0062	0,0069
	$\lvert S_m - S_{-m}\rvert$	0,0062	0,0065	0,0069	0,0073
House	$\lvert R_m - R_{-m}\rvert$	0,0025	0,0028	0,0036	0,0049
	$\lvert S_m - S_{-m}\rvert$	0,0034	0,0037	0,0045	0,0056

Cədvəl 4.2.3 R və S göstəricilərinin gizlədilmiş məxfi informasiyanın həcmindən asılılığı aydın nəzərə çarpır. Bu məlum qanunauyğunluq bir daha rəqəmlər vasitəsilə eksperimental surətdə təsdiq edilərək hesablamaların düzgün aparılmasını göstərir. Baboon təsvirində artım bir qədər fərqlidir, bu da təsvirin strukturu və teksturası ilə izah edilə bilər. Alqoritmin tədqiqindən məlum olur ki, onun dayanıqlılığı yüksək olduğundan bədniyyətli bu alqoritmlə yaradılan steqosistemə müdaxilə edə bilməz. Məxfi informasiya görünməz olduğuna görə açıq kommunikasiya kanalı ilə ötürülə bilər. Gizlədilən məxfi informasiya həcmindən asılı olmayaraq tədqiq edilən alqoritmin cədvəldə verilən həddi dayanıqlılıq dərəcəsinə təsir etmir.

Alqoritmin hesablama mürəkkəbliyinin eksperimental tədqiqi

Bu bölmədə tədqiq edilən alqoritmin də öz növbəsində ayrıca alqoritmlərin keyfiyyətinin və işə yararlılığının dəyərləndirilməsi zamanı əhəmiyyətli göstərici hesab edilən hesablanmanın mürəkkəbliyi parametri tədqiq edilib. Tədqiqat zamanı 8 konteyner və steqo-təsvirlərə müxtəlif həcmdə informasiya gizlədilib. Eyni zamanda həm gizlədilmə, həm də çıxarılma prosedurlarında zaman hesablanıb. Müxtəlif konteyner təsvirinə müxtəlif həcmlərdə məxfi informasiya gizlədilib və alınan steqo-təsvirdə informasiyanın gizlədilmə və steqo-təsvirdən çıxarılma vaxtı yoxlanılıb. Alınan nəticələr aşağıdakı 4.2.4 cədvəlində verilib.

Cədvəl 4.2.4
Alqoritmin işləmə müddəti

Konteyner təsvir	**Məxfi informasiya həcmi (bayt)**	**İnformasiyanın gizlədilmə vaxtı (san)**	**İnformasiyanın çıxarılma vaxtı (san)**
Lena	5000	0,0310	0,0310
	10000	0,0298	0,0296

	15000	0,0369	0,0363
Baboon	5000	0,0326	0,0316
	10000	0,0372	0,0369
	15000	0,0378	0,0369
Airplane	5000	0,0360	0,0354
	10000	0,0379	0,0362
	15000	0,0383	0,0377
Peppers	5000	0,0336	0,0330
	10000	0,0363	0,0330
	15000	0,0393	0,0390
Sailboat	5000	0,0369	0,0358
	10000	0,0382	0,0380
	15000	0,0394	0,0392
Boat	5000	0,03332	0,0329
	10000	0,0342	0,0340
	15000	0,0356	0,0352

Cədvəl 4.2.4-ün ardı

Konteyner təsvir	**Məxfi informasiya həcmi (bayt)**	**İnformasiyanın gizlədilmə vaxtı (san)**	**İnformasiyanın çıxarılma vaxtı (san)**
Couple	5000	0,0321	0,0319
	10000	0,0363	0,0360
	15000	0,0398	0,0394
House	5000	0,0364	0,0362
	10000	0,0379	0,0374
	15000	0,0382	0,0378

Cədvəldə verilən zaman göstəriciləri 4.2 bölməsində verilən alqoritmin göstəricilərindən bir qədər çox olsa da, ümumiyyətlə, mürəkkəb hesab edilməyə bilər. Sıfıra çox yaxındır və təhlükəli həddi keçmir. Alınan göstəricilər digər çox istinad edilən müəlliflərin alqoritmləri ilə müqayisə edilib və cədvəl 4.2.5-də verilib.

Cədvəl 4.2.5.

Təklif edilən alqoritmin realizə müddətinin digər alqoritmlərlə müqayisəsi.

Təsvirlər	**Alqoritmin realizə müddəti (san)**	**Chen Y., [25, s. 271-350]**	**Malik A., [71, s. 7181-7205]**	**Təklif edilən alqoritm**
Lena	İnformasiyanın gizlədilməsi	0,036	0,038	0,0298
	İnformasiyanın	0,033	0,035	0,0296

	çıxarılması			
Baboon	İnformasiyanın gizlədilməsi	0,045	0,048	0,0372
	İnformasiyanın çıxarılması	0,045	0,047	0,0369
Airplane	İnformasiyanın gizlədilməsi	0,041	0,049	0,0379
	İnformasiyanın çıxarılması	0,041	0,046	0,0362
Peppers	İnformasiyanın gizlədilməsi	0,048	0,043	0,0363
	İnformasiyanın çıxarılması	0,046	0,041	0,0330
Sailboat	İnformasiyanın gizlədilməsi	0,044	0,044	0,0382
	İnformasiyanın çıxarılması	0,042	0,042	0,0380

Cədvəl 4.2.5-in ardı

Boat	İnformasiyanın gizlədilməsi	0,049	0,047	0,0342
	İnformasiyanın çıxarılması	0,047	0,045	0,0340
Couple	İnformasiyanın gizlədilməsi	0,039	0,042	0,0363
	İnformasiyanın çıxarılması	0,037	0,041	0,0360
House	İnformasiyanın gizlədilməsi	0,048	0,049	0,0379
	İnformasiyanın çıxarılması	0,046	0,047	0,0374

Cədvəldə verilən zaman göstəriciləri sıfıra çox yaxın qiymətlər alır və tələb edilən həddi keçmir. Alınan göstəricilər məqalələrinə çox istinad edilən müəlliflərin alqoritmləri ilə müqayisə edilib. Cədvəllərdən məlum olur ki, alqoritmin realizəsi minimum vaxt tələb edir. Bu da təklif edilən alqoritmin üstün cəhəti hesab olunur. Hazırlanmış alqoritm təsvirin interpolyasiyası konsepsiyasına əsaslanır. Məlumdur ki, yüksək görüntü keyfiyyəti təmin edilməsi ilə məxfi informasiyaların miqdarının artırılması bir-birinin əksinədir. Bu işin məqsədi steqo-təsvirlərdə təsvirin keyfiyyətini qorumaqla yanaşı böyük həcmdə məxfi informasiya biti gizlətmək qabiliyyətinə malik alqoritm yaratmaq idi. Bunun üçün yeni gizlədilmə alqoritmi təklif edilib. Təklif edilən alqoritmdə Hartli düsturuna əsasən informasiya miqdarının müəyən edilməsi əvəzinə verilənləri onluq say sistemindən ikilik sistemə çevirməklə alınan bit düzümünün sayı əsasında məxfi informasiya bitlərinin sayını müəyyən etdikdən sonra gizlədərək əvəz edilməsi istifadə edilmişdir. Təklif olunan alqoritmin effektivliyi müxtəlif test təsvirləri üzərində aparılan eksperimental tədqiqatlarla, ilkin və steqo-təsvirlərin oxşarlığı PSNR və təsvirə gizlədilmiş məxfi informasiya tutumunun hesablanması, histoqram steqoanaliz və RS steqoanaliz ilə təsdiq edilmişdir. Yuxarıda göstərilənlərdən belə nəticəyə gələ bilərik ki, təklif olunan informasiya gizlətmə alqoritminin istifadəsi, ədəbiyyatda verilmiş digər alqoritmlər ilə müqayisədə daha üstün vizual görüntüyə və dayanıqlılığa malik steqo-təsvir və daha böyük həcmdə məxfi informasiya biti gizlətmə qabiliyyətinə malikdir.

4.3. Kvorum funksiyasına əsaslanan məlumatların gizlədilməsi alqoritminin eksperimental tədqiqi

Təklif olunan alqoritmin səmərəliliyini yoxlamaq və etibarlı nəticələr əldə etmək üçün təsvir üzərində müxtəlif gizlədilmə alqoritmləri üzrə testlər aparılmışdır, onlardan 4-ü Cədvəl 4.3.1.-də təqdim edilmişdir. Təcrübələr USC-SIPI təsvir verilənlər bazasından götürülmüş standart təsvirlər üzərində aparılmışdır. Bu təsvirlər təklif olunan məxfi informasiya gizlədilmə alqoritmi ilə sınaq aparmaq üçün giriş təsvirləri kimi istifadə edilmişdir. Hər bir təsvir təklif olunan alqoritmə uyğun işlənmişdir. Təklif edilən alqoritmin keyfiyyəti ədəbiyyatda təqdim edilən digər alqoritmlər ilə müqayisə edilib və müqayisənin nəticələri cədvəldə göstərilmişdir.

Konteyner və steqo-təsvirlərin oxşarlıq dərəcəsinin və gizlədilmiş məxfi informasiya həcminin tədqiqi.

Konteyner təsvir ilə steqo-təsvirin oxşarlıq dərəcələri yenə PSNR qiymətlərinin hesablanması ilə tədqiq edilib.

Təklif edilən alqoritmin keyfiyyətini xarakterizə edən digər vacib göstərici olan konteynerə gizlədilmiş məxfi informasiya həcmi HC isə ədəbiyyatda təqdim edilən digər alqoritmlər ilə müqayisə edilib və müqayisənin nəticələri cədvəl 4.3.1-də göstərilmişdir.

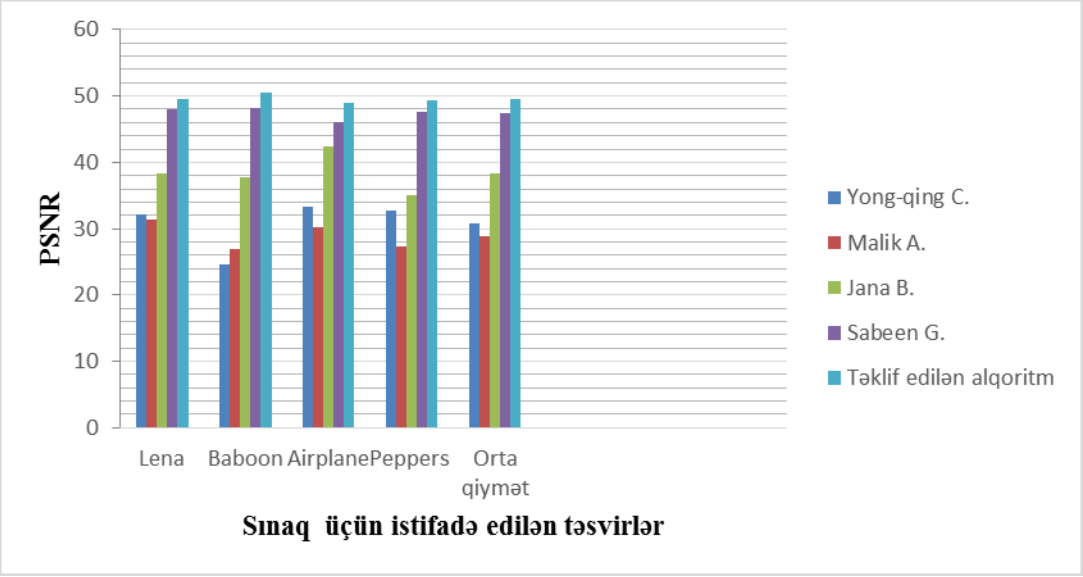
Cədvəl 4.3.1.

Steqo-təsvirlərin keyfiyyət göstəricilərinin müqayisəsi

İlkin təsvir	**Keyfiyyət göstəriciləri**	**Yong-qing C. [25, s. 271-350]**	**Malik A. [71, s. 7181-7205]**	**Jana B., [45, s. 239-248]**	**Sabeen G.[93, s. 20527-20545]**	**Təklif edilən alqoritm**
Lena	PSNR (dB) HC (bit)	32,18 99615	31,33 214571	38,25 222822	48,01 9318	49,56 301465
Baboon	PSNR (dB) HC (bit)	24,69 120586	26,85 117721	37,85 272629	48,21 191365	50,47 283115
Airplane	PSNR (dB) HC (bit)	33,32 96993	30,26 255362	42,34 209715	46,05 112721	48,88 256982
Peppers	PSNR (dB) HC (bit)	32,82 204472	27,39 238826	35,12 230686	47,69 96993	49,32 393216
Orta qiymət	**PSNR (dB) HC (bit)**	**30,75 130417**	**28,95 206620**	**38,39 233963**	**47,49 102599**	**49,55 308695**

Cədvəl 4.3.1. -dən göründüyü kimi hər iki göstərici üçün təklif olunan alqoritm daha yüksək keyfiyyət göstəricilərinə malikdir. Lena təsviri üzərində sınaqlar aparılarkən gizlədilmiş məxfi informasiyanın həcmi [25, s. 271-350]-də 99615, [71, s. 7181-7205- də 214571, [45, s. 239-248]-də 222822, [88, s. 20527-20545]-də 9318 olduğu halda təklif edilən alqoritmdə bu göstərici 301465-ə bərabərdir. Eyni zamanda, belə üstünlük digər əhəmiyyətli parametr olan steqo-təsvirin vizual keyfiyyətində (həmin müqayisə halı üçün) nəzərə çarpır -32,8,31,33,38,25,48,01-ə qarşı 49,56 dB. Bu da təqdim olunan alqoritmin üstünlüyünün birbaşa sübutudur. Nəzərə almaq lazımdır ki, təklif edilən məxfi informasiya biti gizlədilmə alqoritminin məqsədi steqo-təsvirin minimal təhrifi ilə daha çox məxfi informasiya biti gizlətmə qabiliyyətinə nail olmaq idi.

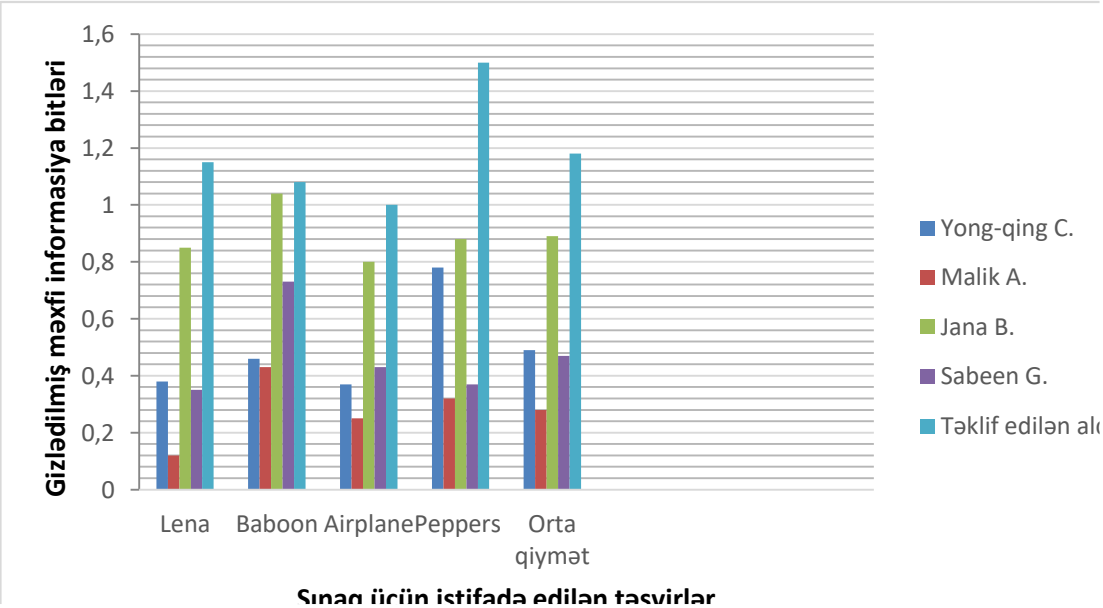
Vizual keyfiyyət parametrinin nəticələrinin istifadə edilən etalon təsvirlərdən asılılığı təsdiq edir ki, PSNR qiymətləri etalon kimi istifadə edilən təsvirin növündən asılı olmayaraq stabil bəyan edilən qanunauyğunluğa tabe olur. Deməli, təklif edilən alqoritmin göstəriciləri etibarlı kimi qəbul edilə bilər.



Şəkil 4.3.1. PSNR göstəricilərinin müxtəlif təsvirlərdən asılılığı

Eyni zamanda, digər mühüm göstərici olan məxfi informasiya bitləri ilə istifadə edilən etalon təsvirlər arasındakı asılılıq da öyrənilib (Şəkil 4.3.2). Qrafikin analizindən məlum olur ki, gizlədilən bitlərin həcminin etalon təsvirdən asılılığı

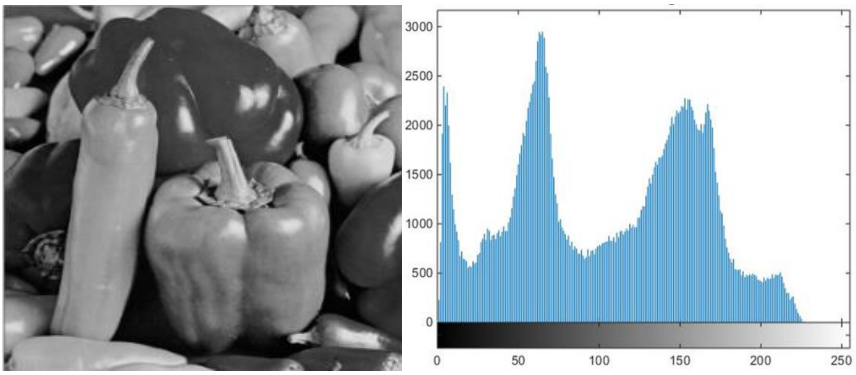
alqoritmin işlənilməsi zamanı əldə edilən qanunauyğunluqla ziddiyət yaratmır və alqoritmin göstəricilərinin dürüstlüyünü bir daha subuta yetirir.



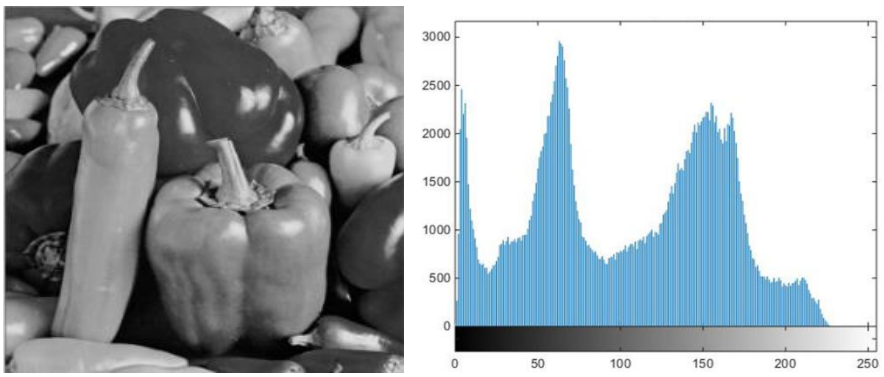
Şəkil 4.3.2. Gizlədilmiş məxfi informasiya bitlərinin müxtəlif təsvirlərdən asılılığı

Alqoritmin histoqram steqoanalizi ilə tədqiqi.

Alqoritmin göstəricilərinin etibarlılığını yoxlamaq üçün giriş təsviri kimi standart təsvirlərdən istifadə edilib. Şəkil 4.3.3.-də konteyner təsvir ilə ona uyğun histoqram, şəkil 4.3.4-də isə steqo-təsvir və həmin təsvirin histoqramı verilib. Cədvəldən görünür ki, müqayisə edilən təsvirlər, əsasən eyni histoqrama malikdirlər. Bu da öz növbəsində müqayisə edilən təsvirlərin yüksək bənzərlik dərəcəsinə malik olması deməkdir.



Şəkil 4.3.3. Konteyner təsvir və onun histoqramı



Şəkil 4.3.4. Steqo-təsvir və onun histoqramı

Tədqiq edilən alqoritmin steqo-hücumlara qarşı dayanıqlılığının analizi:

Bu alqoritmin dayanıqlılığının yoxlanılması üçün histoqram steqoanalizi ilə yanaşı yenə də RS steqoanalizi istifadə edilib. Əvvəlki alqoritmlərdə olduğu kimi bu alqoritmdə də əvvəlcə boş konteynerlərə RS steqoanalizi tətbiq edilib və nəticəsi cədvəl 4.3.2-də verilmişdir.

Cədvəl 4.3.2.

Konteyner təsvirlərin RS steqoanalizi

Konteyner təsvir	$\lvert R_m - R_{-m} \rvert$ (dB)	$\lvert S_m - S_{-m} \rvert$ (dB)
Lena	0,0078	0,0088
Baboon	0,0057	0,0067
Airplane	0,0063	0,0065
Peppers	0,0093	0,0083

Daha sonra alqoritmin prosedurlarına uyğun olaraq təklif edilən alqoritm ilə konteyner təsvirə müxtəlif həcmdə məxfi informasiya gizlədilərək steqo-təsvirlərə müvafiq olan PSNR və gizlətmə həcmləri qeydə alınıb. Eksperimental göstəricilər cədvəl 4.3.3-də verilib. Eksperimental verilənlərin təhlili göstərir ki, müxtəlif həcmdə gizlədilmə RS toplananlarının qiymətləri çox kiçik intervalda dəyişir və yüksək dayanıqlılıq qiymətləri həddi aşmır. Buna görə də, təklif edilən alqoritm ilə informasiya gizlədilərsə, onun açıq kommunikasiya kanalı ilə ötürülməsi zamanı steqosistem bədniyyətlinin hücumlarından tam qorunmuş olur.

Cədvəl 4.3.3.

Steqo-təsvirlərin RS steqoanaliz nəticələri

Steqo−təsvir	**RS steqoanalizi (dB)**	**Gizlədilmiş məxfi informasiya həcmi (bayt)**			
		1000	5000	10000	15000
Lena	$\lvert R_m - R_{-m}\rvert$	0,0086	0,0087	0,0103	0,0108
	$\lvert S_m - S_{-m}\rvert$	0,0095	0,0098	0,0098	0,0099
Baboon	$\lvert R_m - R_{-m}\rvert$	0,0074	0,0083	0,0097	0,0752
	$\lvert S_m - S_{-m}\rvert$	0,0077	0,0083	0,0094	0,0099
Airplane	$\lvert R_m - R_{-m}\rvert$	0,0086	0,0089	0,0095	0,0097
	$\lvert S_m - S_{-m}\rvert$	0,0084	0,0089	0,0095	0,0099
Peppers	$\lvert R_m - R_{-m}\rvert$	0,0097	0,0098	0,0100	0,0109
	$\lvert S_m - S_{-m}\rvert$	0,0090	0,0094	0,0098	0,0100

Məxfi informasiya üç girişli kvorum funksiyasından istifadə etməklə konteyner təsvirə daxil edilir və eyni funksiya ilə əks halda steqo-təsvirdən çıxarılır. Təklif edilən alqoritmin effektivliyi 50 standart təsvir üzərində sınaqdan keçirilmişdir. Təsvirin vizual keyfiyyəti Peak Signal Noise Ratio (PSNR) ilə sınaqdan keçirilib. Bundan başqa alqoritmin dayanıqlılığının qiymətləndirilməsini daha etibarlı etmək üçün histoqram steqoanaliz və RS steqoanalizdən istifadə edilmişdir. İşlənmiş alqoritmin göstəriciləri interpolyasiyaya əsaslanan alqoritmlərlə müqayisə edilib. Alqoritm istər vizual, istərsə də dayanıqlılıq baxımından müəyyən üstünlüklərə malikdir. Son illərdə mövcud olan alqoritmlərlə müqayisənin nəticələri gizlədilmiş məxfi informasiya bitlərinin həcmi və PSNR-in yüksək olması baxımından təklif olunan alqoritmin üstünlüyünü göstərir.

4.4. Rəngli təsvirlərdə məxfi informasiya gizlədilmə alqoritmlərinin eksperimental tədqiqi

Eksperimentlərin doğruluğunu təmin etmək üçün müqayisə edilən alqoritmlərdə istifadə edilən rəngli standart təsvirlər tədqiq edilib. Bu alqoritmdə məxfi informasiya

bitləri rəngli təsvirin mavi kanalında SIFT alqoritmi ilə seçilmiş piksellərə gizlədilmişdir. Təklif edilən alqoritmin dayanıqlılığını yoxlamaq üçün təsvirin bulanıqlaşdırılması prosesi həyata keçirilib. Bunun üçün təsvir 5x5 ölçüdə bloklara bölünür. Blokun qonşu piksellərinin qiymətləri seçilmiş pikselin qiymətləri ilə dəyişdirilməklə həyata keçirilir. Bu prosesdə təklif edilən alqoritm ilə yaradılan steqo-təsvirdə gizlədilmiş məxfi informasiya bitləri təhrif olunmadı və həmin bitlər düzgün şəkildə yenidən əldə edildi. Buna görə də, bu prosesdən uğurla keçmiş hesab olunur. Daha sonra JPEG formatlı təsvirlərin sıxlaşdırılması hücumuna qarşı dayanıqlılığını yoxlamaq məqsədilə yaradılan JPEG formatlı steqo-təsvir 75% sıxlaşdırılıb və gizlədilmiş məxfi informasiya bitləri yoxlanılıb. Yoxlanılma zamanı məxfi informasiya bitlərinin təhrif olunmadığı aşkarlanıb. Bunlardan başqa təsvirlərin döndərilərək məxfi informasiyanın təhrif olunmasına yönəlmiş hücum növü yoxlanılıb. Bunun üçün isə yaradılan steqo-təsvir 70 dərəcə bucaq altında sol istiqamətdə döndərilib. Döndərilmə əməliyyatından sonra gizlədilmiş məxfi informasiya bitləri tam şəkildə, yəni təhrif olunmadan, yenidən bərpa olunub.

Bu hücum növlərinin yoxlanılmasından sonra belə qənaətə gəlmək olar ki, təklif edilən alqoritmdə SIFT alqoritminin istifadəsi bu növ hücumlara qarşı dayanıqlığı təmin edir. Bu hücum növlərindən başqa təklif edilən alqoritm steqanoqrafiya alqoritmlərinin yoxlanılması və qiymətləndirilməsi alqoritmlərinə uyğun olaraq aşağıdakı bölmədə təqdim edilən analiz növləri ilə yoxlanılıb.

Konteyner və steqo-təsvirlərin oxşarlıq dərəcəsinin və gizlədilmiş məxfi informasiya həcminin tədqiqi

Müqayisə edilən iki rəqəmsal təsvirin oxşarlıq dərəcəsi müəyyən olunur. Ona görə də, bu barədə geniş izah tələb olunmadığından qısa verilib. Vizual keyfiyyəti ölçmək üçün PSNR istifadə edilib.

Təklif edilən alqoritmin digər mövcud alqoritmlərlə müqayisəsi cədvəl 4.4.1. -də verilmişdir. Sınaqdan keçirilmiş təsvirlərin göstəriciləri, yəni konteyner təsvir və steqo-təsvir arasındakı PSNR fərq qiymətləri, eyni zamanda təklif olunan alqoritmin

son illərdə işlənilən yeni alqoritmlər ilə PSNR və steqo-təsvirə gizlədilmiş məxfi informasiya bitlərinin həcmlərinin (HC) müqayisəsi göstərilib.

Cədvəl 4.4.1.

Steqo-təsvirlərin keyfiyyət göstəricilərinin müqayisəsi

Giriş təsvirləri	**Keyfiyyət göstəriciləri**	**Yong-qing C. [25,s.271-350]**	**Malik A., Sikka G. [71, s. 2454-7190],**	**Jana B., Giri D., [45, s.239*+/-248]**	**Təklif olunan alqoritmlər**	
					IV alqoritm [5, s. 53-57]	**V alqoritm [5, s. 53-57]**
Lena	PSNR (dB) HC (bit)	34,18 369715	31,93 144887	38,25 223031	41,03 464744	43,23 398562
Baboon	PSNR (dB) HC (bit)	24,69 651710	22,85 187141	35,85 273235	40,43 663791	45,32 593652
Barbara	PSNR (dB) HC (bit)	32,84 334328	30,26 151269	32,24 241232	43,08 423719	48,03 412356
Peppers	PSNR (dB) HC (bit)	32,82 374589	30,42 144177	35,12 232563	39,32 399511	42,02 386592
Orta qiymətlər	**PSNR (dB) HC (bit)**	**30,62 382087**	**29,05 189544**	**32,31 262157**	**40,96 487941**	**44,65 447791**

Qeyd: IV alqoritm - Böyük həcmli məxfi informasiya gizlədilmə alqoritmi.

V alqoritm- Yüksək vizual keyfiyyət prioritetli məxfi informasiya gizlədilmə alqoritmi.

Test edilən təsvirlərin keyfiyyət göstəricilərinin orta qiymətləri HC- 40,96-ya və PSNR-in 44,65-ə bərabərdir. Cədvəldən məlum olur ki, təklif olunan alqoritmlərin digər müqayisə edilən alqoritmlərdən daha böyük həcmdə məxfi informasiya biti gizlədildiyi təqdirdə konteyner təsvir ilə steqo-təsvir arasında daha yüksək oxşarlıq qiymətləri (PSNR) əldə edilir. Böyük həcmdə məxfi informasiya bitləri daxil edildikdən sonra konteyner təsvir ilə steqo-təsvir arasında yüksək oxşarlıq dərəcəsinin əldə edilməsi təklif olunan alqoritmlərin üstünlüyü hesab edilə bilər.

Bundan başqa təklif edilən alqoritmdə PSNR qiymətinin yüksək olması mavi kanalda gizlədilən məxfi informasiya bitlərinin sayının çox olması halında vizual keyfiyyəti qoruduğunu bir daha sübut edir.

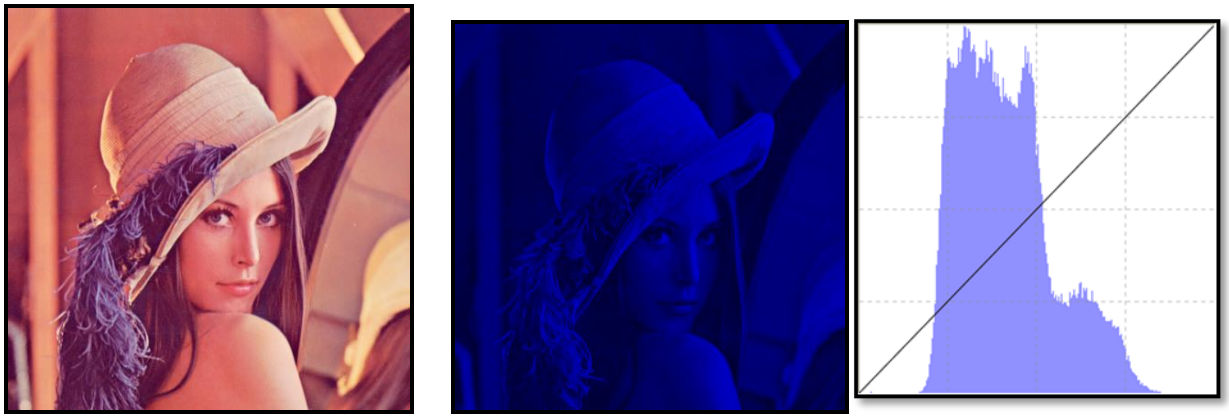
PSNR qiymətlərinə əlavə olaraq giriş təsvirin və steqo-təsvirin müqayisəsində və alqoritmlərin dayanıqlılığını daha dəqiq yoxlamaq üçün histoqram steqoanalizindən istifadə edilir.

Təklif edilən alqoritmlərin histoqram steqoanalizi

Histoqram məlumat sahəsindəki hər bir elementin tezliyinin ölçüsüdür. Çox tez–tez istifadə edilən bu statistika rəqəmsal görüntü təhlükəsizliyi sahəsində olduğu kimi kompüter görmə və görüntü emal sahələrində də tez-tez istifadə edilən bir üsuldur. Histoqramı əldə etmək üçün əvvəlcə hər bir sıfır elementi olan 256 elementli massiv müəyyən edilir (bu rəqəm təsvirin neçə bitlə ifadə olunmasından asılı olaraq dəyişə bilər). Rəqəmsal təsvirin hər pikseli skan edilir və massivin piksel qiymətinə uyğun elementin qiyməti vahid qədər artır. Aşağıda nümunə təsvir və təsvirin boz səviyyəsinin histoqram qrafiki göstərilib.

Histoqram steqoanalizi etalon təsvir və steqo-təsvirlər üzərində aparılıb aşağıda bir təsvirin konteyner (şəkil 4.4.1) və steqo-təsvir (şəkil 4.4.2) fomasının mavi rəng kanalı üzrə histoqramı verilib. Müqayisə edilən digər təsvirlərin histoqramları əlavələrdə verilib.

Müqayisə edilən bütün təsvirlər demək olar ki, eyni histoqramlara malikdir. Bu da məxfi informasiyaların mövcudluğunun aşkar edilməsinin qeyri-mümkün olduğunu sübut edir**.** Göstərilən histoqramlarda steqo-təsvirlərin effektiv yoxla-nılması təmin edilib və konteyner təsvir histoqramları ilə müqayisədə ciddi dəyişiklik nəzərə çarpmayıb.



Şəkil 4.4.1. Konteyner təsvir və konteyner təsvirin mavi kanal üzrə histoqramı

Şəkil 4.4.2. Steqo-təsvir və steqo-təsvirin mavi kanal üzrə histoqramı

Histoqramda hər hansı bir rəng qiymətlərinə malik neçə pikselin daxil edildiyinə görə bu piksel qiymətlərindəki dəyişiklik histoqram fərqi ilə asanlıqla başa düşülə bilər.

Təklif edilən alqoritmlərin dayanıqlılığının ikili statistik steqoanaliz ilə tədqiqi

Təklif edilən alqoritmlərin dayanıqlılığının yoxlanılması üçün yuxarıda təqdim edilən steqoanalizlərdən başqa RS steqoanalizindən istifadə edilmişdir. RS steqoanalizinin nəticələri 4.4.2 və 4.4.3 cədvəllərində təqdim edilib. Tədqiqatlar yenə standart etalon təsvirlər üzərində aparılıb.

Əvvəlcə boş konteyner təsvirlərinə RS steqoanalizi tətbiq edilib. Bu analizin nəticələri cədvəl 4.4.2-də göstərilib.

Cədvəl 4.4.2.

Konteyner təsvirlərin RS steqoanalizi

Konteyner təsvir	$\lvert R_m - R_{-m} \rvert$ (dB)	$\lvert S_m - S_{-m} \rvert$ (dB)
Lena	0,0077	0,0086
Baboon	0,0052	0,0057
Barbara	0,0063	0,0065
Peppers	0,0075	0,0087

Göründüyü kimi hər bir təsvirdə RS göstəriciləri sıfırdan azdır və bir-birinə çox yaxındır. Bu da öz növbəsində alqoritmin dayanıqlılığını təşkil edən əsas amil hesab olunur.

Daha sonra konteyner təsvirinə müxtəlif həcmdə məxfi informasiya bitləri müvafiq alqoritmlər vasitəsilə gizlədildikdən sonra RS steqoanalizi tətbiq edilərək dayanıqlılığı test edilib. Steqoanalizin nəticələri cədvəl 4.4.3.-də göstərilib.

Cədvəl 4.4.3.

Steqo-təsvirlərin RS steqoanaliz nəticələri

Steqo-təsvir	RS steqoanalizi (dB)	Gizlədilmiş məxfi informasiya həcmi (bayt)							
		1000		5000		10000		15000	
		IV alqoritm	V alqoritm	IV alqo-ritm	V alqo-ritm	IV alqo-ritm	V alqo-ritm	IV alqo-ritm	V alqo-ritm
Lena	$\lvert R_m - R_{-m}\rvert$	0,0090	0.0089	0,0091	0.0089	0,0095	0.0092	0,0099	0.0095
	$\lvert S_m - S_{-m}\rvert$	0,0101	0.0101	0,0097	0.0095	0,0099	0.0096	0,0096	0.0093
Baboon	$\lvert R_m - R_{-m}\rvert$	0,0073	0.0073	0,0080	0.0079	0,0086	0.0083	0,0073	0.0090
	$\lvert S_m - S_{-m}\rvert$	0,0082	0.0080	0,0078	0.0076	0,0094	0.0091	0,0078	0.0089
Barbara	$\lvert R_m - R_{-m}\rvert$	0,0078	0.0076	0,0093	0.0093	0,0097	0.0099	0,0093	0.0091
	$\lvert S_m - S_{-m}\rvert$	0,0073	0.0071	0,0089	0.0088	0,0089	0.0094	0,0095	0.0088
Peppers	$\lvert R_m - R_{-m}\rvert$	0,0091	0.0089	0,0099	0.0095	0,0082	0.0085	0,0089	0.0086
	$\lvert S_m - S_{-m}\rvert$	0,0088	0.0086	0,0095	0.0093	0,0078	0.0081	0,0093	0.0082

Təqdim edilən nəticələrdən məlum olur ki, informasiyanın həcminin artırılması təklif edilən alqoritmlərin dayanıqlılığına təsir etmir. Məxfi informasiya görünməz olduğuna görə açıq kommunikasiya kanalı ilə ötürülə bilər.

Alqoritmlərin hesablama mürəkkəbliyinin eksperimental tədqiqi

Bu bölmədə tədqiq edilən alqoritmlərin hesablanmasının mürəkkəbliyi parametri tədqiq edilib. Tədqiqat zamanı konteyner və steqo-təsvirlərə müxtəlif həcmdə informasiya yerləşdirilib. Eyni zamanda, həm məxfi informasiya bitlərinin gizlədilməsi, həm də steqo-təsvirdən məxfi informasiya bitlərinin çıxarılması üçün tələb olunan zaman hesablanıb. Alınan nəticələr aşağıdakı cədvəl 4.4.4-də verilib.

Onu da qeyd etmək lazımdır ki, rəngli təsvirlərdə məxfi informasiya gizlədilmə alqoritmlərinin hər ikisində də gizlədilmə müddəti eynidir.

Cədvəl 4.4.4.

Alqoritmlərin işləmə müddəti

Konteyner təsvir	**Məxfi informasiya həcmi (bayt)**	**İnformasiyanın gizlədilmə vaxtı (san)**	**İnformasiyanın çıxarılması vaxtı (san)**
Lena	5000	0,0231	0,0313
	10000	0,0248	0,0325
	15000	0,0369	0,0337
Baboon	5000	0,0261	0,0339
	10000	0,0273	0,0352
	15000	0,0296	0,0386
Barbara	5000	0,0326	0,0286
	10000	0,0344	0,0303
	15000	0,0363	0,0328
Peppers	5000	0,0235	0,0278
	10000	0.0263	0,0293
	15000	0,0285	0,0299

Cədvəldə verilən zaman göstəricilərindən məlum olur ki, təklif edilən alqoritmlərin realizəsi az vaxt tələb edir. Əgər parametrləri güclü kompüterlərdən istifadə edərək alqoritmlər realizə edilərsə, onda zaman göstəriciləri daha da azala bilər, bu da alqoritmlərin digər üstün cəhəti hesab olunur. Alınan göstəricilər digər müəlliflərin alqoritmləri ilə müqayisə edilib və cədvəl 4.4.5-də verilib.

Cədvəl 4.4.5.

Təklif edilən alqoritmlərin realizə müddətinin digər alqoritmlərlə müqayisəsi

Təsvirlər	**Alqoritmin realizə müddəti (san)**	**Chen Y., [25, s.** 271–350**]**	**Malik A., [71, s. 7181-7205]**	**Təklif edilən alqoritm**
Lena	İnformasiyanın gizlədilməsi	0,023	0,028	0,035
	İnformasiyanın çıxarılması	0,029	0,032	0,028
Baboon	İnformasiyanın gizlədilməsi	0,053	0,038	0,043
	İnformasiyanın çıxarılması	0,042	0,030	0,042

Cədvəl 4.4.5-in ardı

Təsvirlər	**Alqoritmin realizə müddəti (san)**	**Chen Y., [25, s.** 271–350**]**	**Malik A., [71, s. 7181-7205]**	**Təklif edilən alqoritm**
Barbara	İnformasiyanın gizlədilməsi	0,035	0,029	0,029
	İnformasiyanın çıxarılması	0,051	0,046	0,031
Peppers	İnformasiyanın gizlədilməsi	0,027	0,039	0,024
	İnformasiyanın çıxarılması	0,035	0,048	0,036

Cədvəldə verilən zaman göstəriciləri sıfıra çox yaxın qiymətlər alır və tələb edilən həddi keçmir. Cədvəllərdən məlum olur ki, alqoritmlərin realizəsi minimum vaxt tələb edir.

Yuxarıda göstərilənlərdən belə nəticəyə gələ bilərik ki, təklif olunan rəngli təsvirlərdə məxfi informasiya gizlətmə alqoritminin istifadəsi, ədəbiyyatda verilmiş digər alqoritmlər ilə müqayisədə daha yaxşı vizual görüntüyə və dayanıqlılığa malik steqo-təsvir və daha böyük həcmdə məxfi informasiya biti gizlətmə qabiliyyətinə malikdir.

4.5. Təklif edilən alqoritmlərin müqayisəsi

Dissertasiya işində işlənilən alqoritmlər müxtəlif xassələrə və göstəricilərə malikdirlər və bununla da onların təyinatı müəyyən olunur. Hər alqoritmin eksperimental göstəriciləri müqayisə üçün cədvəl 4.5.1-də verilib. Əvvəlki tədqiqat işlərində əsas məqsəd məxfi informasiyanın həcminin artırılması olurdusa, hazırda steqoanaliz alqoritmlərının inkişafı ilə əlaqədar olaraq steqo-təsvirin vizual keyfiyyətinə və alqoritmlərin hücumlara qarşı dayanıqlılığına daha çox diqqət yetirilir. Son illərin tendensiyasını nəzərə alaraq işlənilən vizual keyfiyyət prioritetli informasiya gizlətmə alqoritmində əsas diqqət məhz təsvirin keyfiyyətinə və dayanıqlılığının yüksək olmasına yönəldilibdir. Gizlədilən məxfi informasiya bitlərinin kifayət qədər çox olduğu halda vizual keyfiyyəti xarakterizə edən göstərici

PSNR və ona bənzər metrikaların qiymətləri nəzərə çarpan dərəcədə yüksəkdir. Bu da təbii ki, birinci alqoritm ilə gizlədilən informasiyanın heç bir maneəyə rast gəlmədən müvəffəqiyyətlə görünməz halda açıq şəbəkələr ilə ötürülərək informasiyanın alıcısına çatmasını təmin edir. Deməli, bu alqoritmin təyinatı yüksək konfidensiallıq tələb edilən hallara uyğundur.

Cədvəl 4.5.1.

Təklif edilən alqoritmlərin keyfiyyət göstəricilərinin müqayisəsi

Keyfiyyət göstəriciləri	I alqoritm [75, s. 329-333]	II alqoritm [11, s. 465-472]	III alqoritm [1, s. 60-66]	IV alqoritm [5, s. 53-57]	V alqoritm [5, s. 53-57]
HC (bit)	243677	465390	308695	487941	447791
PSNR (dB)	51,65	35,67	49,55	40,96	44,65
MSE (dB)	0,008	0,016	0,012	0,015	0,015
SSIM (dB)	0,073	0,081	0,089	0,081	0,081
Dayanıqlılıq	Yüksək	Orta	Yüksək	Yüksək	Yüksək

Qeyd:

I alqoritm- Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiya gizlədilmə alqoritmi

II alqoitm - Təsvir interpolyasiyasına əsaslanan məxfi informasiya gizlədilmə alqoritmi

III alqoritm - Kvorum funksiyasına əsaslanan informasiya gizlədilmə alqoritmi

IV alqoritm - Böyük həcmli məxfi informasiya gizlədilmə alqoritmi

V alqoritm - Yüksək vizual keyfiyyət prioritetli məxfi informasiya gizlədilmə alqoritmi

Təsvir interpolyasiyasına əsaslanan məxfi informasiya gizlədilmə alqoritmi [9] konteynerə daha çox məxfi informasiya biti gizlətmə imkanına malikdir. Bununla yanaşı nisbətən az vizual keyfiyyəti və orta səviyyəli dayanıqlılığı ilə fərqlənir. Lakin qeyd etmək olar ki, həmin keyfiyyət göstəriciləri aşağı səviyyəli alqoritm kimi qəbul edilə bilməz və həmin PSNR qiyməti ədəbiyyatda təqdim edilən uğurlu nəticələri olan steqanoqrafik alqoritmlərlə müqayisə edilən səviyyədədir. Bu alqoritm

vasitəsilə daha çox məxfi informasiya bitlərinin gizlədilməsi nisbətən az konfidensiallıq tələb edilən hallarda istifadə edilə bilər.

Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritmi [75, s. 329-333] digər alqoritmlərdən öz imkanlarına və göstəricilərinə görə fərqlənir və demək olar ki, digər boz təsvirlər üzərində işlənmiş alqoritmlərin müsbət xassələri onda cəmlənib. Əgər kvorum funksiyasına əsaslanan informasiya gizlədilmə alqoritmində [1, s. 60-66] vizual keyfiyyət və dayanıqlılıq, təsvir interpolyasiyasına əsaslanan məxfi informasiya gizlədilmə alqoritmində daha çox məxfi informasiya bitinin gizlədilməsi üstünlük təşkil edirdisə, ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritmində hər üç əsas göstərici gizlətmə həcmi, vizual keyfiyyət və yüksək dayanıqlığı ilə seçilir. Vizual keyfiyyəti əks etdirən digər göstəricilərin də qiymətləri PSNR ilə ziddiyət təşkil etmir. Deməli, bu alqoritm çox geniş profilli olaraq daha çox məqsədlər üçün tətbiq edilə bilər.

Təklif edilən böyük həcmli məxfi informasiya gizlədilmə alqoritmi və yüksək vizual keyfiyyət prioritetli məxfi informasiya gizlədilmə alqoritmi [5, s. 53-57] digər üç alqoritmdən bəzi xüsusiyyətlərinə görə fərqlənir. Bu xüsusiyyətlərdən birincisi bu alqoritmlərin digərlərindən fərqli olaraq konteyner təsviri kimi rəngli təsvirlərdən istifadə olunmasını, ikinci xüsusiyyəti kimi təhlükəsizliyin təmin olunması üçün SIFT alqoritmlərindən istifadə edərək açar nöqtə piksellərində məxfi informasiyanın gizlədilməsini, üçüncü fərqli xüsusiyyəti isə konteyner və steqo-təsvir arasında vizual oxşarlığı təmin etmək üçün məxfi informasiya bitlərinin mavi kanalın müvafiq piksellərində gizlədilməsini misal göstərmək olar.

Təklif edilən alqoritmlərin effektivliyi standart təsvirlər üzərində yoxlanılaraq təsdiq edilib.

Təklif edilən alqoritmlərin hər biri informasiyanın gizlədilmə həcmi və steqo-təsvirin vizual keyfiyyət göstəricilərinin tədqiqi ilə yanaşı gizlədilmə həcminin alqoritmdən alqoritmə dəyişən asılılıqları da qrafiki olaraq təqdim edilib. Qrafiklərdən nəzərə çarpan odur ki, təsvirlərin növündən asılı olmayaraq təklif edilən

alqoritmlərin göstəriciləri müqayisə edilən alqoritmlərın göstəricilərindən üstündür. Gizlədilmə həcminin miqdarı ayrı-ayrı təsvirlərdə eyni qanunauyğunluğa tabedir. Misal üçün ən çox gizlədilmə həcmi hər bir müqayisə edilən alqoritmdə, Baboon təsvirində müşahidə edilir. Lakin burada ən az göstərici [101, s. 10795-10819]-də təqdim edilən alqoritmə məxsusdur. Deyilənlərdən belə nəticəyə gəlmək olar ki, steqo-sistemlər və alqoritmlər seçilərkən mütləq təsvirlərin xüsusiyyətləri də nəzərə alınmalıdır.

Dördüncü fəsil üzrə nəticələr

Təklif edilən alqoritmlərin hər birində konteynerin vizual dəyişimini yoxlamaq üçün PSNR, konteynerə gizlədilmiş məxfi informasiyanın həcmini müəyyən etmək məqsədilə HC qiymətləri və dayanıqlığı yoxlamaq üçün isə RS steqoanalizindən istifadə edilmişdir.

Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiya gizlədilmə alqoritmi [75, s. 329-333]:

- Yüksək PSNR təmin edilməsinə baxmayaraq verilənlərin gizlədilmə həcmi kifayət qədər çox olur və müqayisə edilən alqoritmlərin göstəricilərindən üstün olduğu təsdiqlənir.
- Standart təsvirlərin çeşidindən asılı olmayaraq PSNR-in qiymətləri zəmanətli şəkildə 50dB-dən yüksək olur.
- Alqoritmin hücumlara dayanıqlılığını yüksəltmək üçün steqo-açardan istifadə edilib.
- Eksperimentlərin göstəricilərinə əsasən demək olar ki, təklif edilən alqoritm, məxfi informasiyanın görünməz şəkildə açıq kommunikasiya kanalları ilə ötürülməsini təmin edir [77, s. 77-80]..

Təsvir interpolyasiyasına əsaslanan steqanoqrafik informasiya gizlətmə alqoritmi [11, 465-472]:

- İnformasiya gizlədilən təsvirin vizual keyfiyyətini qoruyub saxlamaq şərtilə böyük miqdarda informasiyanı gizlətmək imkanına malik alqoritm işlənilib

- Məsələ prinsip etribarilə yeni gizlətmə mexanizminin tətbiq edilməsi ilə Hartli düsturuna əsaslanan gizlədiləcək məxfi informasiya miqdarının müəyyən edilməsi əvəzinə verilənlərin onluq say sistemindən ikilik sistemə keçilməsi ilə əvəz edilməsi nəticəsində həll olunub.
- Təklif edilən informasiya gizlətmə alqoritmi informasiya gizlədilən təsvirin vizual keyfiyyətini təmin etməklə yanaşı ədəbiyyatda təklif olunan alqoritmlərlə müqayisədə daha çox miqdarda verilənlərin gizlədilməsini təmin edir.

Kvorum funksiyasına əsaslanan məxfi informasiya gizlətmə alqoritmi [1, s. 60-66]:

- Bu alqoritmdə daha yüksək PSNR təmin edilir və buna baxmayaraq verilənlərin gizlədilmə həcmi kifayət qədər çox olmaqla yanaşı müqayisə edilən alqoritmlərin göstəricilərindən əskik deyil və ya az fərqlənir.
- Standart təsvirlərin çeşidindən asılı olmayaraq PSNR-in qiymətləri 50 dB-dən yüksək idi. Həmin göstərici məxfi informasiyanın görünməz şəkildə açıq kommunikasiya kanalları ilə ötürülməsini təmin edir.
- Alqoritmin təhlükəsizlik səviyyəsini yüksəltmək üçün AES şifrləmə standartı ilə məxfi informasiya şifrlənmişdir. Şifrləmə standartının tətbiqi nəticəsində təhlükəsizlik dərəcəsi yüksək səviyyədə təmin edilib.
- Əhəmiyyətli miqdarda çox məxfi informasiya bitlərinin gizlədilməsinə rəğmən müqayisə edilən alqoritmlərdən daha yüksək PSNR və gizlədilən informasiyanın miqdarı təmin edildi [77, s. 77-80]..

Rəngli təsvirlərdə məxfi informasiyanın gizlədilməsi [5, s. 53-57].

Bu məqsədlə iki müxtəlif məxfi informasiya gizlədilmə alqoritmləri təklif edilib.

- RGB rəngli təsvirlərin mavi kanalında məxfi informasiya gizlədilmə alqoritmi işlənilərək sınaqdan çıxarılıb.
- Hər iki alqoritmin PSNR və HC göstəriciləri yoxlanılaraq cədvəldə göstərilib. İşlənilən hər iki alqoritm PSNR və HC göstəricilərinə görə experimental tədqiq edilib [77, s. 77-80].

- Alqoritmlərin dayanıqlılığı RS steqoanalizi və histoqram steqoanalizi ilə tədqiq edilib.
- Rəngli təsvirin bulanıqlaşdırılması, sıxlaşdırılması, təsvirin döndərilməsi kimi məlum hücum növlərinə qarşı dayanıqlığı da yoxlanılaraq müsbət nəticələr əldə olunub.

NƏTİCƏ

Dissertasiya mövzusu üzrə aparılan tədqiqatlar prosesində qarşıya qoyulan məsələlər həll edilərək aşağıdakı nəticələr əldə edilib:

- Təsvir steqanoqrafiyasına aid xarici elmi ədəbiyyatda təklif edilən informasiya gizlətmə alqoritmlərinin geniş icmalı aparılıb [3, s. 51-55, 4, s. 79-81, 6, s. 204-206, 12, s. 34-36, 11, s. 465-472]. Aparılın icmalın əsasında mövzunun işlənmə səviyyəsi və dissertasiya işində həll edilməli olan problemlər müəyyən edilib [76, s. 427-437] və son illərdə təsvir steqanoqrafiyası sahəsində aparılan tədqiqatlar içərisindən yüksək göstəricilərə malik və dissertasiya mövzusuna oxşar alqoritmlər nümunə kimi seçilərək geniş tədqiq edilib [7, s. 29-33].

- Təsvirin vizual keyfiyyəti prioritetli, steqo-hücumlara qarşı yüksək dayanıqlılığa malik, böyük həcmdə məxfi informasiya gizlədilməsini təmin edən steqanoqrafik alqoritm işlənilib [75, s. 329-333].

- Konteyner təsvirin, heç bir pozuntu baş vermədən, yenidən bərpa olunmasını təmin edən, interpolyasiya əsaslı steqanoqrafik alqoritm işlənilib [1, s. 60-66].

- Yüksək göstəricilərə malik üç girişli kvorum funksiyasına əsaslanan steqanoqrafik alqoritm işlənilib [1, s. 60-66, 3, s. 51-55, 12, s. 34-36]. Alqoritmin yüksək dayanıqlılığını təmin etmək üçün AES şifrləmə standartı tətbiq edilib [8, s. 366-370, 9, s. 5-7,].

- Rəngli RGB rəng sxemində olan təsvirlərdə SIFT alqoritmindən istifadə etməklə açar nöqtə piksellərində məxfi informasiyanın gizlədilməsi üçün iki yeni effektiv alqoritm təklif edilib [5, s. 53-57].

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT SİYAHISI

1. Nağıyeva, A.F. Məxfi informasiyanın ötürülməsində informasiya gizlədilmə metodu // – Bakı: Elmi əsərlər, Azərbaycan Texniki Universiteti, – 2023. № 2,– s. 60 – 66.
2. Nağıyeva, A.F. İnformasiya təhlükəsizliyində steqanoqrafik metodlar // – Gəncə: Elmi xəbərlər məcmuəsi, Azərbaycan Texnologiya Universiteti , – 2023. № 4, – s. 98 – 104.
3. Nağıyeva, A.F., Verdiyev, S.Q., İnformasiyanın steqanoqrafik gizlədilməsi metodlarının eksperimental analizi // İnformasiya təhlükəsizliyinin aktual problemləri III respublika elmi – praktik seminarının əsərləri, – Bakı: İnformasiya Texnologiyaları, – 8 dekabr, – 2017, – s. 51–55.
4. Nağıyeva, A.F., Verdiyev, S.Q., Kompüter Steqanoqrafiyası və onun əsas prinsipləri // Proqram mühəndisliyinin aktual elmi-praktiki problemləri üzrə II Respublika konfransı, – Bakı: İnformasiya Texnologiyaları, – 17 may, – 2017,– s. 79-81.
5. Nağıyeva, A.F., Verdiyev, S.Q., Rəqəmli təsvirlərin watershed üsulu ilə seqmentləşdirilməsi // İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri,– Bakı: İnformasiya Texnologiyaları, – 14 dekabr, – 2018, – s. 53-57.
6. Nağıyeva, A.F., Verdiyev, S. Q., Hüseynova, R.Y., Hüseynov, Z. N., Steqoanaliz üsullarının icmalı // İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri V respublika konfransı, – Bakı: İnformasiya Texnologiyaları, – 29 noyabr, – 2019,– s. 204-206.
7. Алмадатова А.Ф., Вердиев С.К., Нагиева А.Ф. Защита информации криптографическим методом разделения секрета // VII Международная научно-техническая и научно-методическая конференция, – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций, -28 февраля-1 марта, – 2018, – с. 29-33.
8. Вердиев, С.Г., Нагиева, А. Ф. О возможностях использования стандарта AES в Корпоративных сетях для защиты информации //– Самара: Инфокоммуникационные технологии,– 2017. 15(4),–с. 366-370.
9. Нагиева, А. Ф., Вердиев, С. К., Гусейнов, З. Н. Симметричное (одноключевое) шифрование данных при защите информации в компьютерных сетях // Технические науки в России и за рубежом: материалы VII Международная научная конференция, – Москва: Молодой ученый –31 ноябрь, – 2017, – с. 5-7.

10. Нагиева А.Ф., Вердиев С.К., Реверсивный метод сокрытия информации основанный на использовании кворум функции // E-Scio, –2022. 72 (9), – с.39-51.
11. Нагиева А.Ф., Вердиев С.К. Реверсивный стеганографический метод сокрытия информации основанный на интерполяции изображений //– Москва: Компьютерная оптика,– 2022. 46 (3),– с. 465-472.
12. Нагиева А.Ф. Корпоративные сети и проблемы безопасности //- Казанъ: Молодой ученый,– 2016. 133 (29),–с. 34-36.
13. Нагиева А.Ф. A review on image interpolation based data hiding techniques //E-Scio, – 2022. 66 (3), – с. 51-58.
14. Нагиева А.Ф.Observe of Data Hiding Techniques used in Image steganography// E-Scio, – 2022. 66 (3), – с. 378-386.
15. Шелухин О.И. Steganography:[в 44 томах]. / С. Д.Канаев. Москва: Горячая линия - Телеком, -2017.-582 с.
16. Abbas, C, Digital image steganography: Survey and analysis of current methods / C. Joan, C. Kevi, K. Paul // Signal processing,– 2010, № 90, -p. 727-752.
17. Aziz, F. Reversible data hiding techniques with high message embedding capacity in images / T. Ahmad, A. Malik, M. Uddin, S. Ahmad, M. Sharaf // PLoS One, – 2020. №15, – p.1-24.
18. Ahmad, A. M., Al-.Haj, A., Mahmoud, F. An improved capacity data hidin technique based on image interpolation // Multimedia Tools and Applications, Springer,– 2019. № 78, – p.7181-7205.
19. Abdelwahab, A. A., Hassan, L. A. A discrete wavelet transform based technique for image data hiding // Proceedings of 25th National Radio Science Conference,– 2008. № 36, – p. 1–9.
20. Al-Husainy, M. A. Image steganography by mapping pixels to letters // Journal of Computer Sciences,– 2009. № 5, – p. 33-38.
21. Bin, L. A Survey on Image Steganography and steqanalysis / H. Janhui, H. Jiwu, S. Yun // Journal of Information Hiding and Multimedia Signal Processing,– 2011. № 2, – p.142-172.
22. Bai, J. A high payload steganographic algorithm based on edge detection / Chang, C. Nguyen, T. Zhu, C. Liu, Y. // Displays, – 2017. № 46, – p.42–51.
23. Chen, W.J., Chang, C.C. High payload steganography mechanism using hybrid edge detector // Expert System Application,– 2010. № 37,– p. 3292–3301.
24. Chauhan, D. Quantization based m watermarking for secure e-health / A. K. Singh, B. Kumar, J. Saini // Multimedia Tools and Applications, – 2017. № 32, – p.1-13.

25. Chen, Y., An efficient general data hiding scheme based on image interpolation / W. Sun, L. Li, X. Chang, C. Wang, // Journal of Information Security and Applications, – 2020. № 54, – p. 271–350.
26. Chin, Y., Shen, H., Cheonshik K. Improving stego image quality in image interpolation based data hiding // Computer Standards & Interfaces,–2017. № 10,– p. 209-215.
27. Chuang, G., Fangxiu, J., Wei, T., Pan, H. A Fast Method for Image Matching and Registration Based on SIFT Algorithm and Image Pyramid // 2nd International Symposium on Power Electronics and Control Engineering (ISPECE 2019) ,– Tianjin, China: IOP Publishing,– 22-24 November,– 2019, – p. 1-7.
28. Denemark, T., Selection-channel-aware rich model for steganalysis of digital images / V. Sedighi, V. Holub, R. Cogranne, J. Fridrich, // IEEE International Workshop on Information Forensics and Security, WIFS, IEEE, – 2014,– p.48–53.
29. Das, P., Kar, N. ILSB: Indicator-based LSB steganography // Intelligent Computing, Communication and Devices, Springer, – 2015. – p. 489–495.
30. Eltyeb, E, Elgabar, A. Comparison of LSB Steganography in BMP and JPEG Images // International Jurnal of Soft Computing and Engineering (IJSCE), – 2013. № 3,– p. 91-95.
31. Fridrich, J., Kodovsky, J. Rich models for steganalysis of digital images // IEEE Trans. Inf. Forensics Secur,– 2012. № 7, – p. 868–882.
32. Gasimov, V.A., The Modified Method of the Least Significant Bits for Reliable Information Hiding in Graphic Files // International journal of information security science, – 2019. 8(1), – p.1-10.
33. Gasimov, V.A., Mammadov, J.I., Mustaphayeva, E.A. Intersymbol interval method for hiding secret information based on pseudo-random number sequences // Проблеми нформатизации та управління,– 2022. 1, (69) – p.18-23.
34. Gul, G., Kurugollu, F. SVD-based universal spatial domain image steganalysis // IEEE Transactions on Information Forensics and Security,– 2010. № 5,– p. 349-353.
35. Guo, F., Yang, J., Chen, Y., Yao, B. Research on image detection and matching based on SIFT features // 3rd International Conference on Control and Robotics Engineering (ICCRE),– Nagoya: IEEE,–20-23 April,– 2018,- pp. 130-134.
36. Hedieh, S., Mansour, J. Evolutionary Rule Generation for Signature-based Cover Selection Steganography // Computer and Information Technology Workshops. IEEE 8th International Conference on, – Neural Network World, – 21 Februrary, – 2016, – p. 297-316.

37. Hu, J. Li, T. Reversible steganography using extended image interpolation technique// Comput. Electric. Eng., – 2015. № 46,– p. 447-455.
38. Hussain, M., Recursive information hiding scheme through LSB, PVD shift, and MPE/ A. Wahab, K.Jung, J. Noman // IETE Technical Review– 8 February, – 2017,– p.1–11.
39. Hong, W. A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification / T. Chen, Y. Chang, C. Shiu // Signal Process,– 2010. № 90,– p. 2911-2922.
40. Hany, F. A survey of image forgery detection // IEEE Signal Processing Magazine,– 2009. № 26 – p.16-25.
41. Imamverdiyev, Y.N., Abdullayeva, F.D., Deep Learning in Cybersecurity: Challenges and approaches // international journal of cyber warfare and terrorisim.– 2020. № 10,–p. 82-105.
42. Imamverdiyev, Y., Teoh, A.B.J., and Kim, J. Biometric cryptosystem based on discretized fingerprint texture descriptors // Expert systems with Applications, – 2013. № 40,– p. 1888-1901.
43. Jung, K.H, Yoo, K.Y. Data hiding method using image interpolation // Comput Stand Interfaces,– 2009. № 31, – p. 465-470.
44. Junying, Y., Haishan, C. Embedding Suitability Adaptive Cover Selection for Image Steganography // International Conference on e Education, e-Business and Information Management (ICEEIM), – 2014. № 12, – p. 36-39.
45. Jana, B. Giri, D. Mondal, S. K. Weighted Matrix based Reversible Data Hiding Scheme using Image Interpolation // Computational Intelligence in Data Mining, Springer,– 2015. № 2, – p. 239-248.
46. Jassim, F. A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method // International Journal of Computer Applications, – 2013. № 72,– p. 39-44.
47. Joshi, K. Gill, S. Yadav, R. A new method of image steganography using 7th bit of a pixel as Indicator by introducing the successive temporary pixel in the gray scale image // – London: Journal Comput Networks Commun, – 2018, – p.10.
48. Jung, K.H. A survey of interpolation-based reversible data hiding // Multimedia Tools and Applications, –2017. № 39, – p. 7795-7810.
49. Jung, K.H., Yoo, K.Y. Steganographic method based on interpolation images// Multimedia Tools and Application, – 2015. № 74,– p. 2143-2155.
50. Jian, F. L., A Coverless Information Hiding Method Based on Constructing a Complete Grouped Basis with Unsupervised Learning / Jin, B.N., Li L., Ting, L., // Journal of Network Intelligence, – China: – 2021. № 6, – p. 29-39.

51. Khosravi, M. R. Yazdi, M. A lossless data hiding scheme for medical images using a hybrid solution based on IBRW error histogram computation and quartered interpolation with greedy weights // Neural. Comput&Applic,– 2018. № 30,– p. 2017–2028.
52. Kim, S., histogram shifting for reversible data hiding using a pair of extreme predictions / X. Sachnev, V. Kim, HJ. Skewed // IEEE Trans Circuits Syst Video Technol, – 2019. № 29,– p. 3236–3246.
53. Kumar, R. Kim, D. Jung, K. Enhanced AMBTC based data hiding method using hamming distance and pixel value differencing // Journal Information Security Application,– 2019. № 47,– p. 94–103.
54. Kumar, R. Rattan, M. Analysis of various quality metrics for medical image processing // Int. J. Adv. Res. Computer. Sci. Softw. Eng,– 2012. № 2,– p. 137–144.
55. Lai, G. Zhang, Z.Y. Dai. Improved LSB Matching Steganography for Preserving Second Order Statistics // Journal of Multimedia,–2010. № 5,– p. 485–463.
56. Lowe, D.G., Object Recognition from Local Scale-Invariant Features // The Proceedings of the Seventh IEEE International Conference on Computer Vision,– Kerkyra, Greece, IEEE,– 20-27 September, –1999,– p. 1150-1157.
57. Li, B. A Survey on Image Steganography and steqanalysis/ J. He, H. Jiwu, Q. Shi. // Journal of Information Hiding and Multimedia Signal Processing,– 2011. № 2,– p.142-172.
58. Lee, C., Huang, Y. An efficient image interpolation increasing payload inreversible data hiding// Expert Syst. Appl.,– 2012. № 39,– p. 6712 – 6719.
59. Luo, L., Reversible image watermarking using interpolation technique / Z. Chen, M. Chen, X. Zeng, Z. Xiong. // IEEE Trans.Inf. Forens. Secur,– 2010. № 5,–p. 187–193.
60. Lakshmanan, S. Rani, M.M. Reversible data hiding in medical images usingedge detection and difference expansion technique // Journal of Computational and Theoretical Nanoscience,– 2018. № 15,– p. 2400–2404.
61. Lin, Y. A data hiding scheme based upon DCT coefficient modification // Computer standards & interfaces,–2014. № 36, – p. 855–862.
62. Liu, L., A reversible data hiding method mean interpolation and random-block division/ T. Chen, S. Zhu, W. Hong // Information Technologic,– 2014. № 13,– p. 2374-2384.
63. Lu, T.C., Reversible data hiding based on Image interpolation with a Secret message reduction strategy / M.C. Lin, C.H. Huang, K.M. Deng // International Journal of Computer & Software Engineering,–2016. № 1,– p. 102-112.

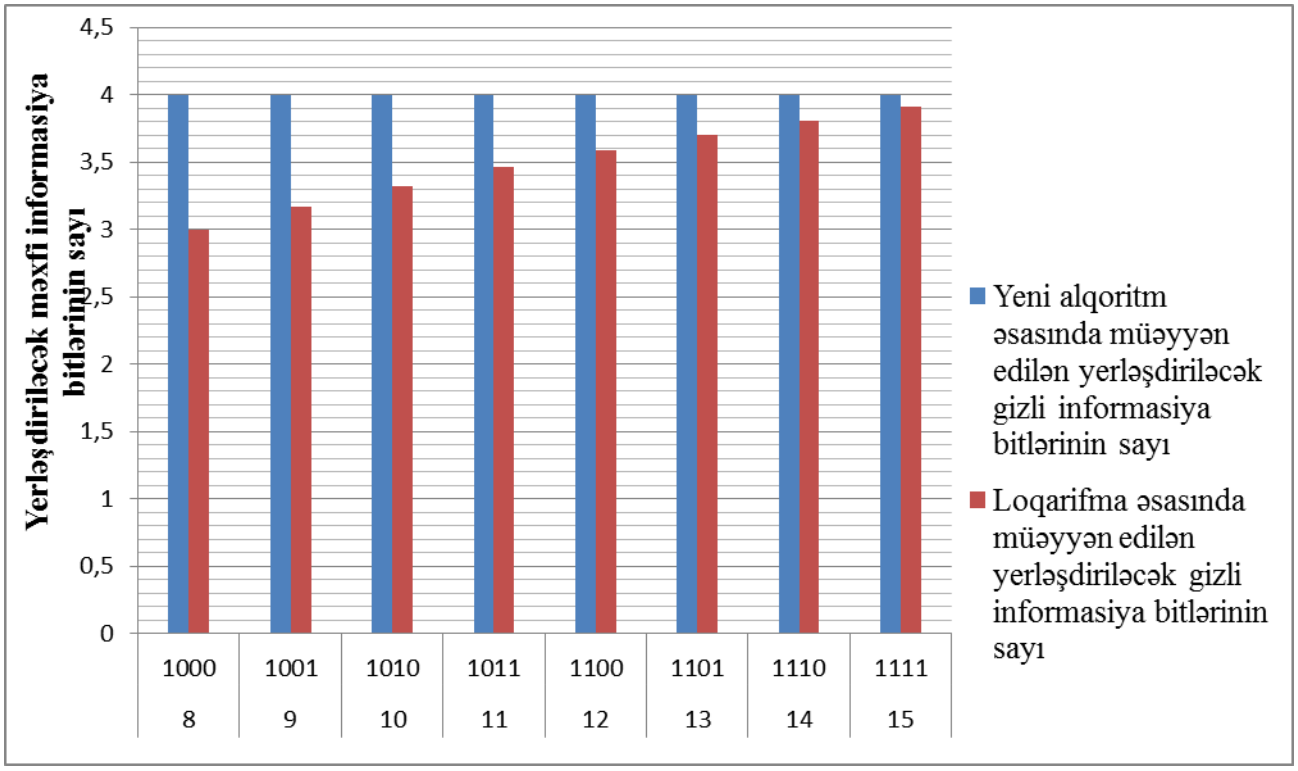
64. Lien, B., Lin, Y., High-capacity reversible data hiding by inaximum-span pairing// Multimedia Tools and Applications, – 2011. № 52, –p. 499-511.
65. Liao, X., Wen, Q., Zhang, J. A steganographic method for digital images with four-pixel differencing and modified LSB substitution// Journal of Visual Communication Image Representation,– 2011. № 22,– p.1–8.
66. Liang, T., Shuhua, M., Xianchun, M., Hairong, Y. Research on Image Matching of Improved SIFT Algorithm Based on Stability Factor and Feature Descriptor Simplification // Applied science, - Shenyang:– 2022. № 17, – p. 1-19.
67. Masud, K. A new approach for LSB based image steganography using secret key // 14th international conference on computer and information technology,- Dhaka: Computer science,– 9 March, – 2011, –p. 286–291.
68. Mehdi, H. Image Steganography in Spatial Domain: A Survey / W. Ainuddin, I. Yamani, K.H. Jung // Signal Processing: Image Communication,–2018. № 65, – p. 46-66.
69. Mawita, E., Abdelmegid, A. A modified image steganography method based on LSB technique // International Journal of Computer Applications,– 2015. № 125, –p.12-17.
70. Manikopoulos, C., Detection of block DCT-based steganography in gray- scale images / S, Yun-Qing, S, Sui, Z. Zeng, N. Zhicheng, Z. Dekun// Proceedings of the IEEE workshop on Multimedia Singal Processing, – 2002,– p. 355-358.
71. Malik, A. Sikka, G., Verm, H.K. Image interpolation based high capacity reversible data hiding scheme // Multimedia Tools Application,– 2018. № 76,– p. 2454-7190.
72. Muhammad, K., A novel image steganographic approach for hiding text in color images using HSI color model / J. Ahmad, H. Farman, M. Zubair // Journal of Scientific Research, – 2015, – p. 647-654.
73. Muhammad, K. A novel magic LSB substitution method using multi-level encryption and achromatic component of an image/ M. Sajjad, I. Mehmood, S. Rho // Multimedia Tools Application, – 2016. № 75, – p.14867–14893.
74. Nissar, A., Mir, A. Classification of steganalysis techniques: A study // Digital Signal Processing,– 2010. № 20, – p.1758-1770.
75. Naghiyeva, A.F., Akbarzadeh, K. A., Verdiyev, S.G. New steganography method of reversible data hiding with priority to visual quality of image // IEEE International Conference Advances in Computing Communication, Embedding and Secure System– India: Scopus, – 2-4 september,– 2021,– p.329-333.
76. Naghiyeva, A.F. Verdiyev, S.G. A brief overview of data hiding methods in digital images // Инфокоммуникационные технологии,–2020. №18, – p.427-437.

77. Verdiyev, S.G., Naghiyeva, A.F., Ajay, K. Experimental study of a novel technique of data hiding with high PSNR // IEEE International Conference Advances in Computing Communication, Embedding and Secure System- India: IEEE, – 18-20 may,–2023. – p. 77-80.
78. Parah, S.A. Hiding clinical information in medical images: a new high capacity and reversible data hiding technique / F. Ahad, J. Sheikh, G. Bhat // Journal of Biomedical Informatic,– 2017. № 66,– p. 214–230.
79. Paul, G., Keyless steganography in spatial domain using energetic pixels / I. Davidson, I. Mukherjee, S. Ravi // ICISS, Springer,–2012.– p.134–148.
80. Rudder, A., Goodridge, W., Mohammed, S. Using Bias optimization for reversible data hiding using image interpolation// International Journal of Network Security & Its Applications,–2013. № 5, – p. 65-76.
81. Ritchey, P. C. Synthetic steganography: Methods for generating and detecting covert channels in generated media: / Degree of Doctor of Philosophy. Dissertations. /–West Lafayette, –2015. - p. 549.
82. Seyyedi, A, Ivanov, N. A novel Secure Steganography Alqoritm Based on Zero Tree Method // International Journal of Advanced Studies in Computer Science and Engineering,– 2014. №3,– p. 1-9.
83. Subhedar, M. S., Mankar, V.H. Current status and key issues in image steganography: A survey // Science Direct,–2014. №13, – p. 95-113.
84. Seyyedi, A., Ivanov, N. Statistical Image Classification for Image Steganographic Techniques// International Journal of Image, Graphics and Signal Processing,– 2014. № 6,– p.19–24.
85. Sadkhan, S. B. Al-Barky, A.M., Muhammad, N.N. An agent based image steganography using information theoretic parameters // MASAUM Journal of Computing, – 2009. 1(2), – p. 258-264.
86. Sabeen, G. P. V. Sajila, M. K. Bindiya, M. V. A two stage data hiding scheme with high capacity based on interpolation and difference expansion // Procedia Technology, Elsevier,– 2016. 24(1), – p. 1311-1316.
87. Sabeen, G. P.V. Judy, M.V. A secure framework for remote diagnosis in health care: A high capacity reversible data hiding technique for medical images // Computers and Electrical Engineering,– 2020. 89 (25),– p. 300-314.
88. Sabeen, G., P.V., Bindiya, M. V., Judy, M. V. A high imperceptible data hiding technique using quorum function // Multimedia tools and applications, Springer,– 2021. 80(5),– p. 20527 –20545.
89. Shaik, A, V, T. High capacity reversible data hiding using 2D parabolic interpolation // Multimed Tools Application,–2018. 78(8),– p. 9717–9735.

90. Solak, S. Altınışık, U. Image steganography based on LSB substitution and encryption method: adaptive LSB+3J // Electronic Imaging,– 2019. 28(04),– p.1-25.
91. Swain, G. Very high capacity image steganography technique using quotient value differencing and LSB substitution //Arabian Journal for Scienceand Engineering,– 2018. 44(4),– p. 2995–3004.
92. Sanglikar, H. Reversible data-hiding in encrypted images by reserving room before encryption technique and LSB matching algorithm // Intemational Joumal of Technical Research and Applications, –2015. 3(2),–p. 52-54.
93. Singh, A. Medical image watermarking / B. Kumar, G. Singh, A. Mohan // Multimedia systems and applications. Spring,- USA: –2019. 1 (3), -p. 43-60.
94. Skrypnyk, I., Lowe, D.G., Scene Modelling, Recognition and Tracking with Invariant Image Features // Third IEEE and ACM International Symposium on Mixed and Augmented Reality, - Arlington, VA, USA, IEEE,- 05 November,-2004,– p. 110-119.
95. Thanikaiselvan,V., Subashanthini, S., Amirtharajan, R. Pvd based steganography on scrambled rgb cover images with pixel indicator// Journal of Artificial Intelligence,– 2014. 36(5),-p.54-68.
96. Tang, M., Hu, J., Song, W. A high capacity image steganography using multilayer embedding //International Journal for Light and Electron Optics,–2014.125(15),- p. 3972-3976.
97. Tsai, P., Hu, Y.C., Yeh, H.L. Reversible image hiding scheme using predictive coding and histogram shifting // Signal Processing,– 2009. 89(6),-p.1129-1143.
98. Taleby, A. M, A comparative analysis of information hiding techniques for copyright protection of text documents/ Q. Li, H. Shim, Y. Huang // Security Communication Networks,–2018. 31(4),- p.1–22.
99. USC-SİPİ image database, university of southern california. Available online at http://sipi.usc.edu/database
100. Wu, H.-C., Image steganographic scheme based on pixel-value differencing and LSB replacement methods / N.-I. Wu, C.-S. Tsai, M.-S. Hwang, // IEEE Proceedings-Vision, Image and Signal Processing, –2005. 15(2),– p.611-615.
101. Wahed, M.A. Nyeem, H. Reversible data hiding with interpolation and adaptive embedding // Multimedia Tools and Applications,– 2019. 78(3),–p.10795-10819.
102. Wu D.C., Tsai, W.H. A steganographic method for images by pixelvalue differencing//Pattern Recognition Letters –2003. 24 (9–10),–p. 1613–1626.
103. Weimann, G. New Terrorism and New Media // Commons Lab, Research series, – 2014. 2, –p.1-20.

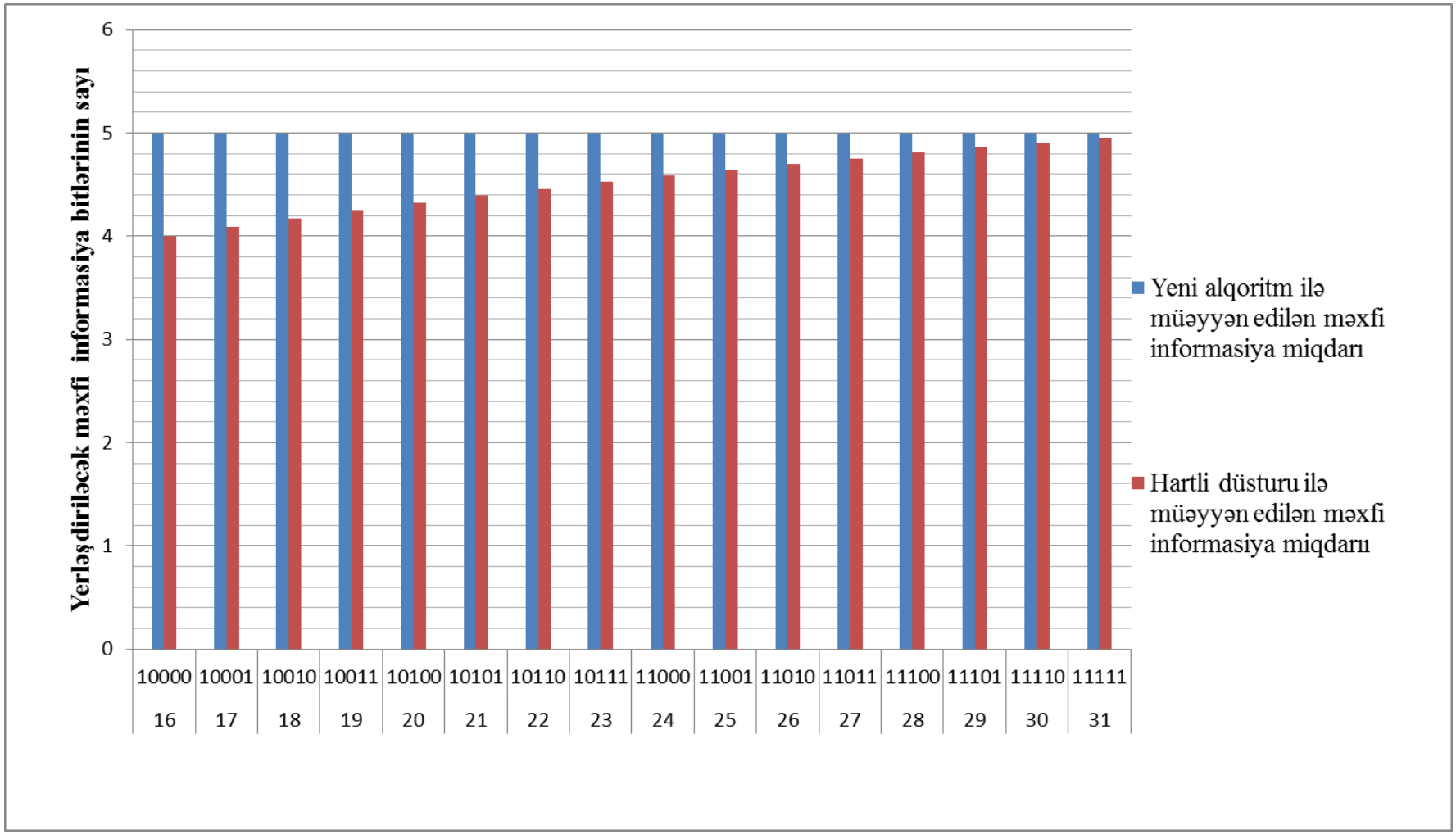
104. Ya-Ting C., Cheng-Ta H., Chin-Feng, L. Image interpolating based data hiding in conjuction with pixel-shifting of histogram // Journal of Supercomputing, Springer,– 2013. 66 (2),– p.1093-1110.
105. Yang C. H, Hsu, C. H. A high quality reversible data-hiding method using interpolation technique // International Conference on Information Assurance and Security,– 2009. 9(3),– p. 603-606.
106. Zaker, N., Hamzeh, A. A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram//Multimedia Tools and Applications, – 2012. 58(3),– p.147-166.
107. Zhang, X., High capacity data hiding based on interpolated image / Z. Sun, Z. Tang, C. Yu, X. Wang // Multimedia Tools Application,– 2017. № 76,– p.9195–9218.
108. Zhang, Z. Separable reversible data hiding in encrypted image // IEEE Transactions on Information Forensics and Security,– 2012. 7(8),–p.553-562.
109. Zeki, A.M., Manaf, A. A. A novel digital watermarking technique based on ISB (Intermediate Significant Bit) // World Academy of Science, Engineering and Technology,– 2009. 38(3),–p.996-989.

Konteyner pikselinin 8÷255 intervalına qədər olan qiymətlərində məxfi informasiya bitlərinin Hartli düsturu əsasında və yeni alqoritm əsasında yerləşdirilməsinin müqayisəsi

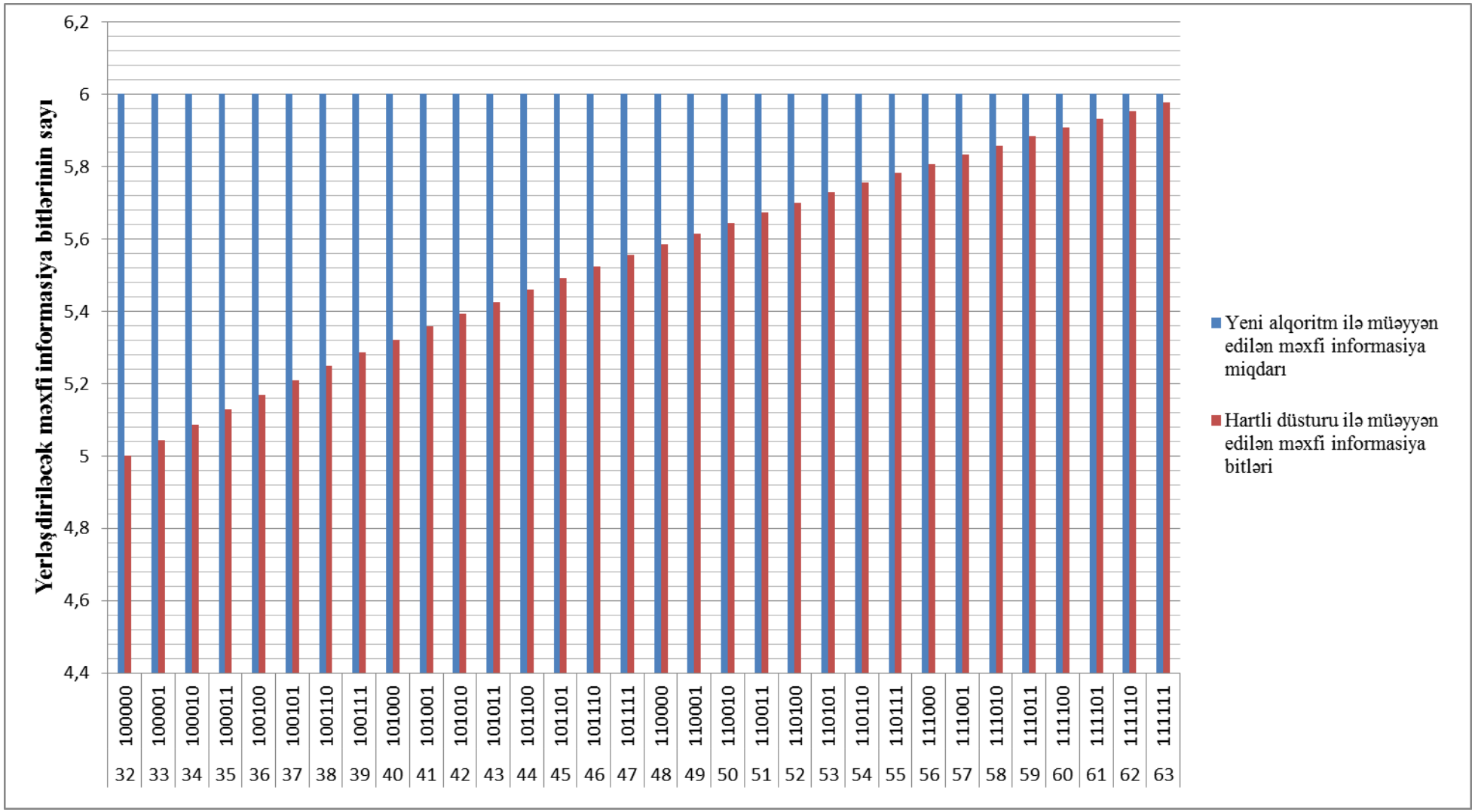


Şəkil 1. Konteyner pikselinin 8÷15 intervalındakı qiymətlərində məxfi informasiya bitlərinin Hartli düsturu əsasında və yeni alqoritm əsasında yerləşdirilməsinin müqayisəsi

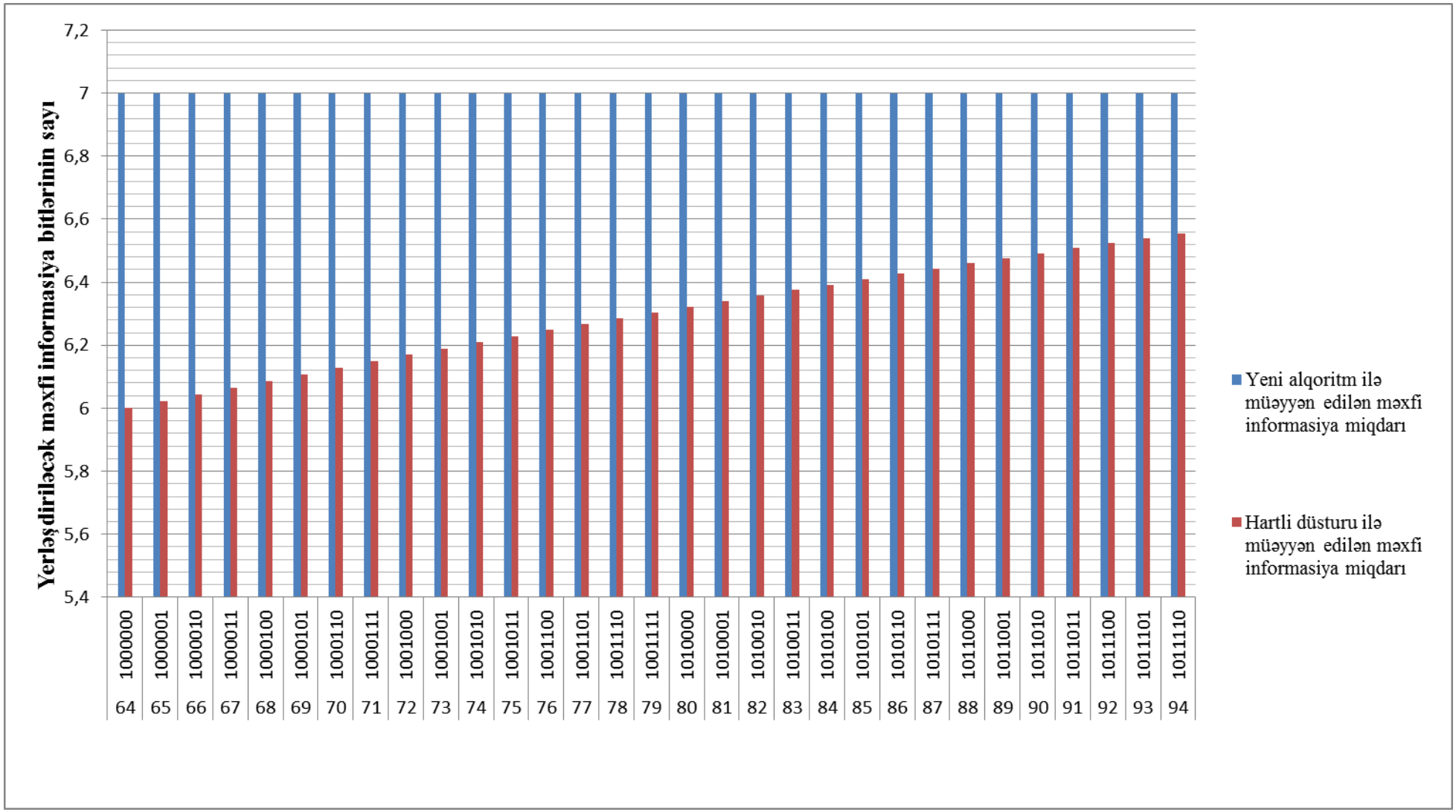
.



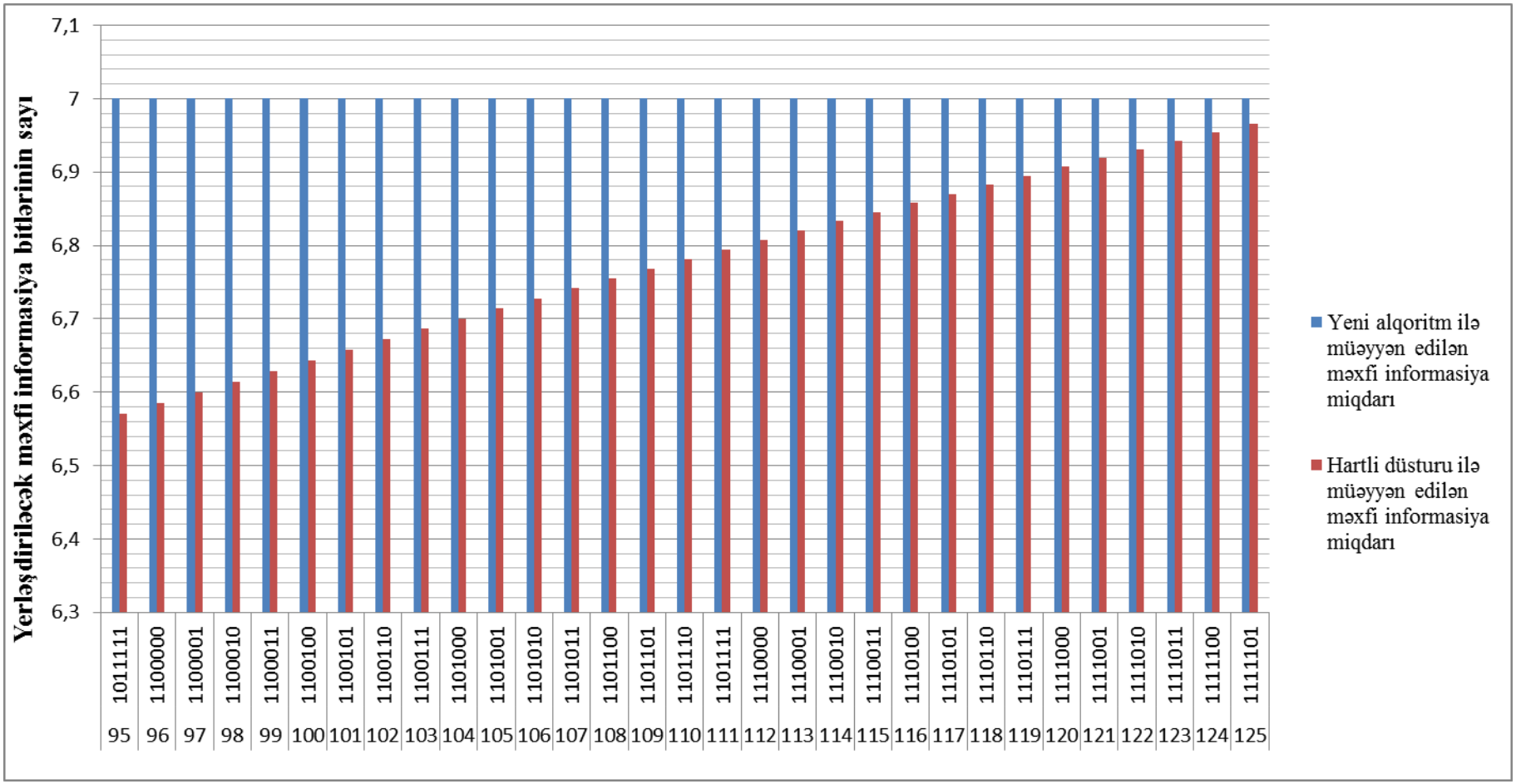
Şəkil 2. Konteyner pikselinin 16÷31 intervalındakı qiymətlərində məxfi informasiya bitlərinin Hartli düsturu əsasında və yeni alqoritm əsasında yerləşdirilməsinin müqayisəsi



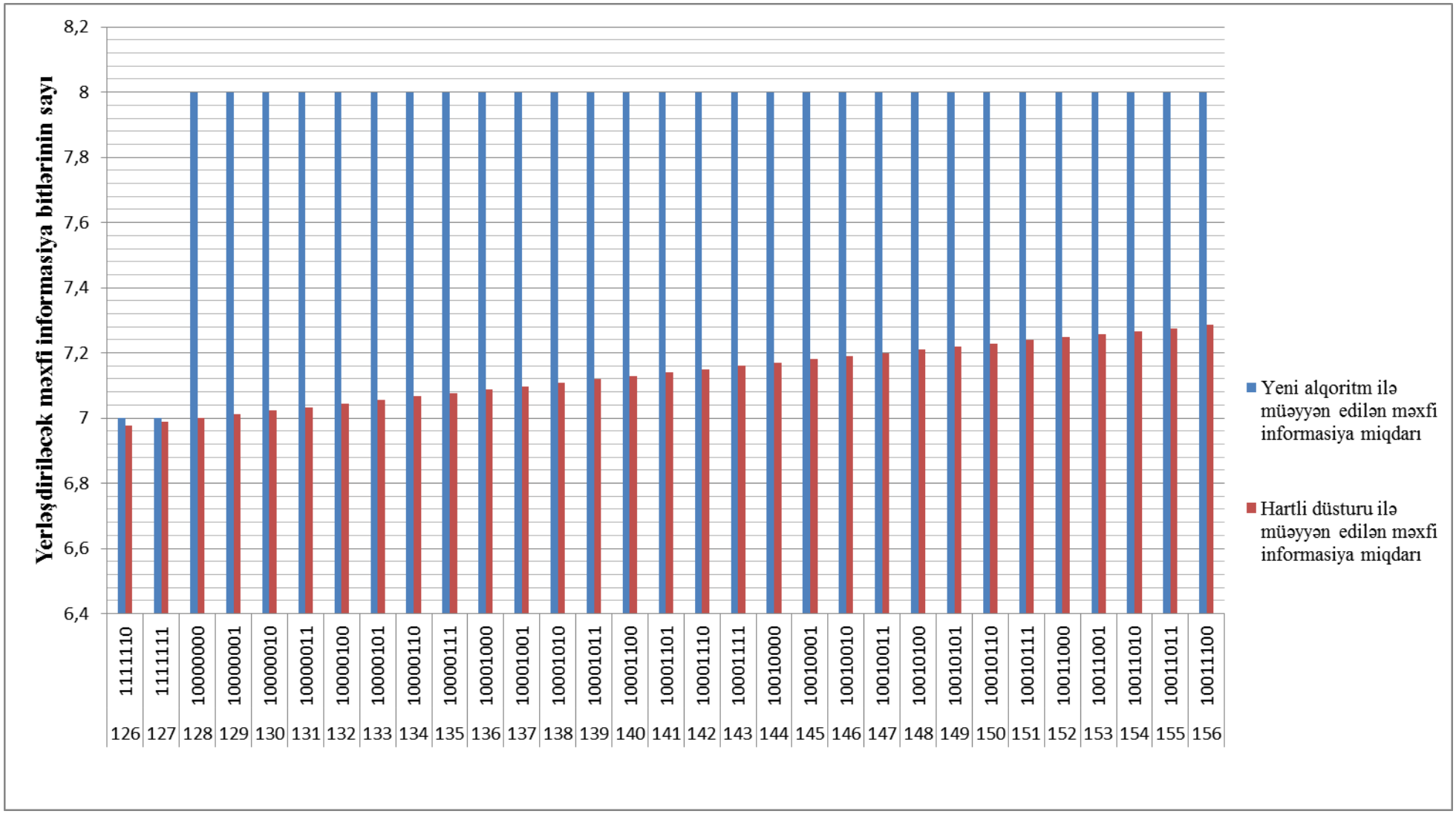
Şəkil 3. Konteyner pikselinin 32÷63 intervalındakı qiymətlərində məxfi informasiya bitlərinin Hartli düsturu əsasında və yeni alqoritm əsasında yerləşdirilməsinin müqayisəsi



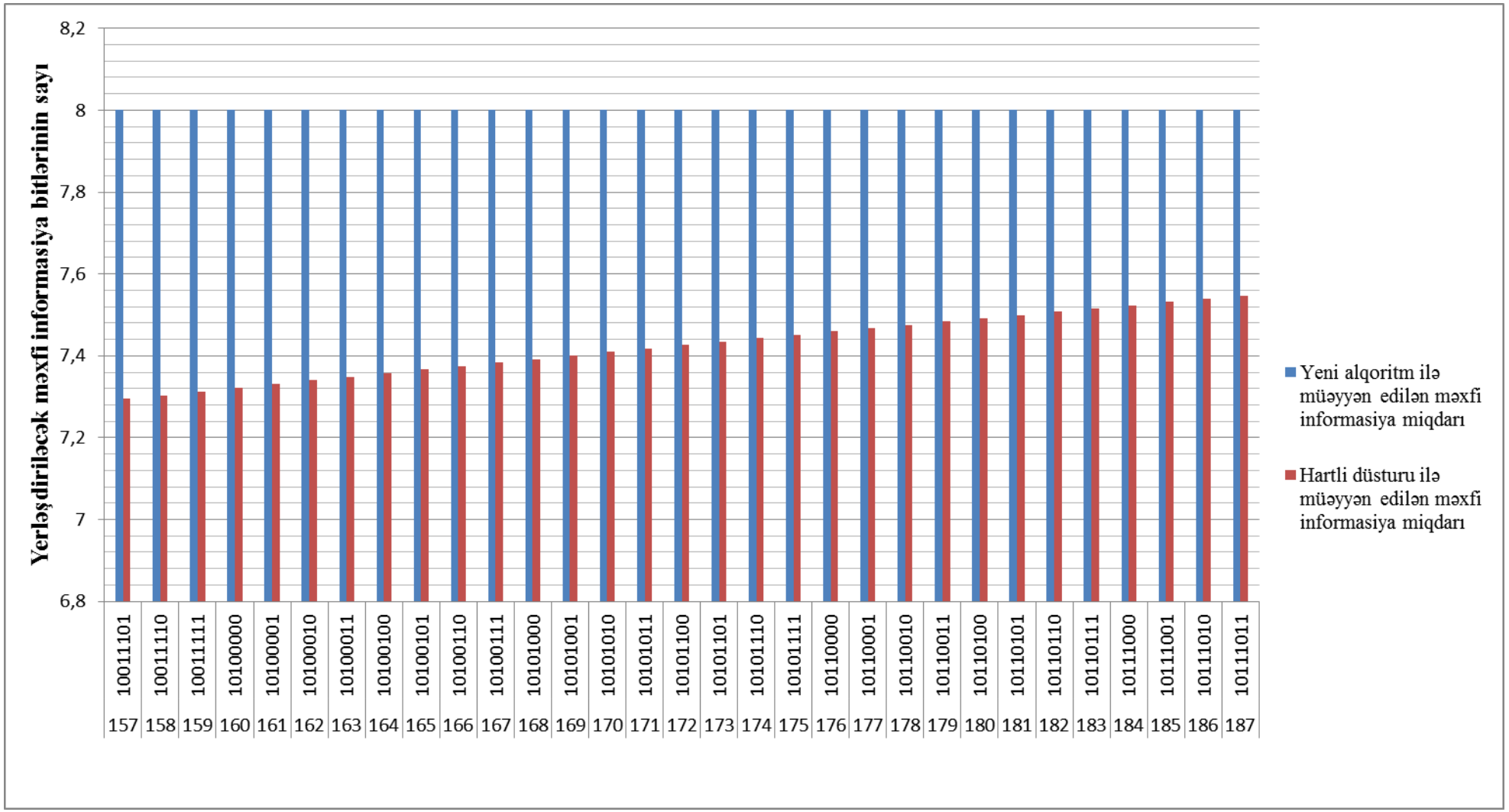
Şəkil 4. Konteyner pikselinin 64÷94 intervalındakı qiymətlərində məxfi informasiya bitlərinin Hartli düsturu əsasında və yeni alqoritm əsasında yerləşdirilməsinin müqayisəsi



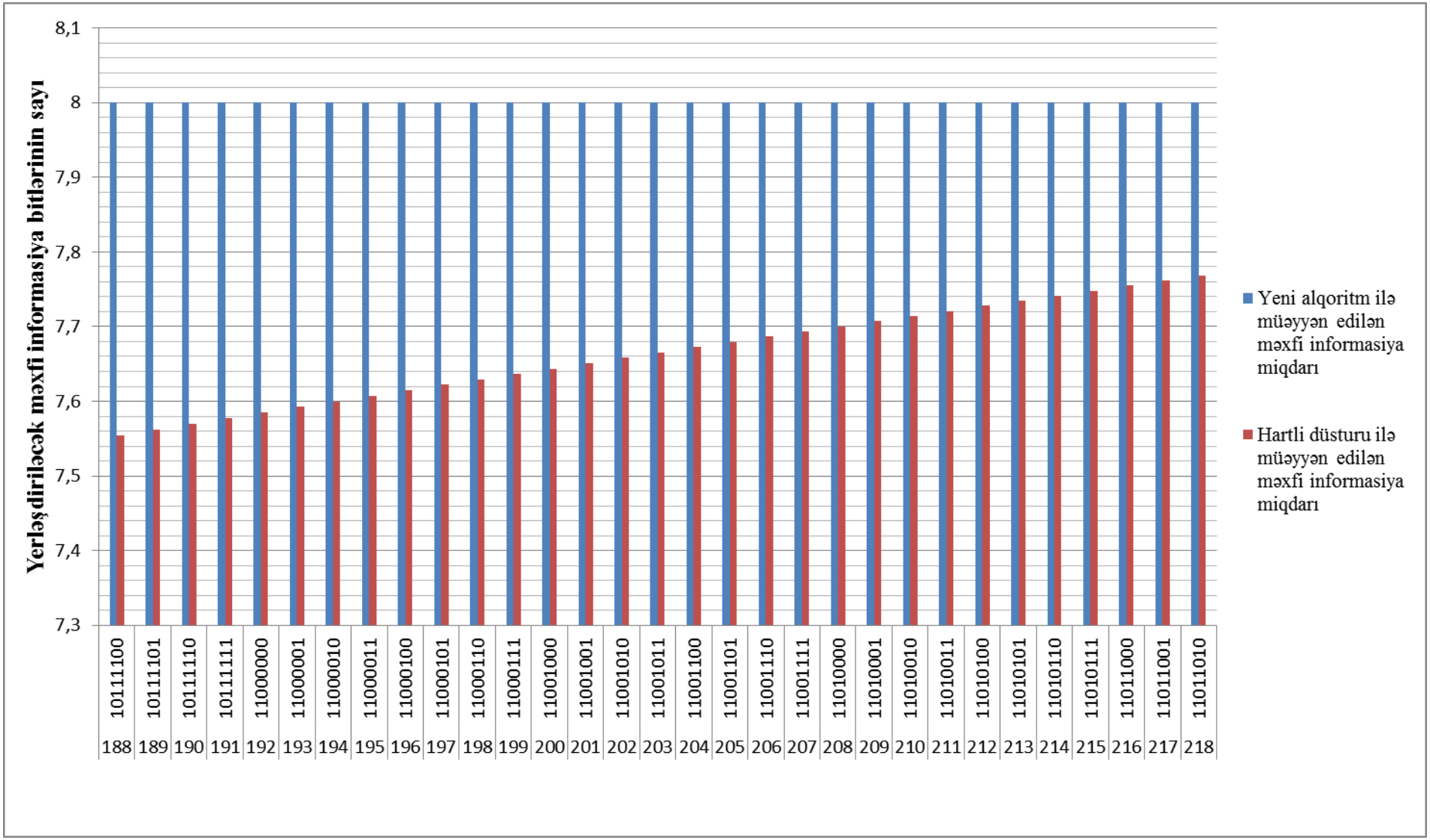
Şəkil 5. Konteyner pikselinin 95÷125 intervalındakı qiymətlərində məxfi informasiya bitlərinin Hartli düsturu əsasında və yeni alqoritm əsasında yerləşdirilməsinin müqayisəsi



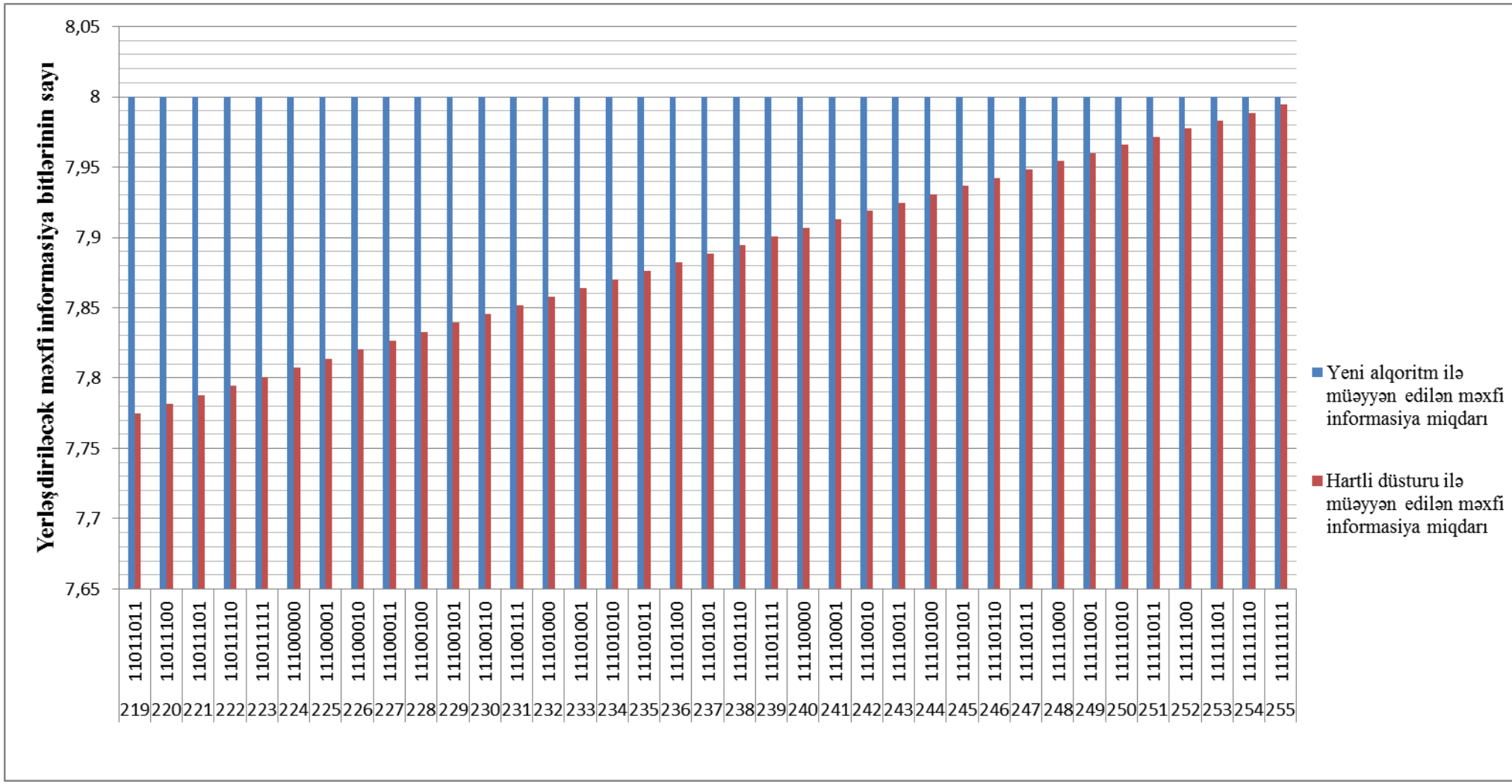
Şəkil 6. Konteyner pikselinin 126÷156 intervalındakı qiymətlərində məxfi informasiya bitlərinin Hartli düsturu əsasında və yeni alqoritm əsasında yerləşdirilməsinin müqayisəsi



Şəkil 7. Konteyner pikselinin 157÷187 intervalındakı qiymətlərində məxfi informasiya bitlərinin Hartli düsturu əsasında və yeni alqoritm əsasında yerləşdirilməsinin müqayisəsi



Şəkil 8. Konteyner pikselinin 188÷218 intervalındakı qiymətlərində məxfi informasiya bitlərinin Hartli düsturu əsasında və yeni alqoritm əsasında yerləşdirilməsinin müqayisəsi

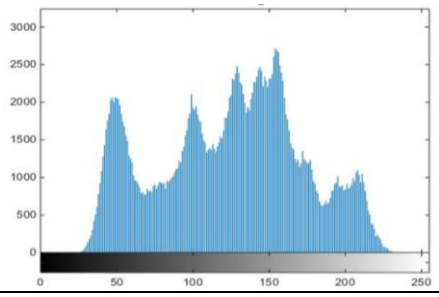
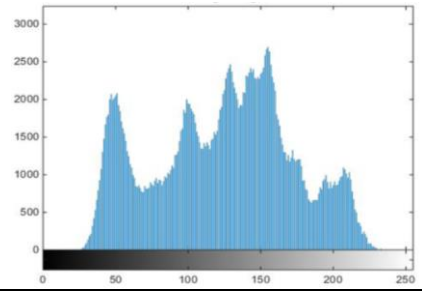
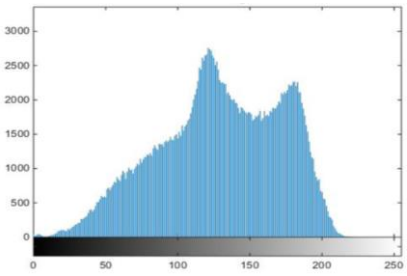
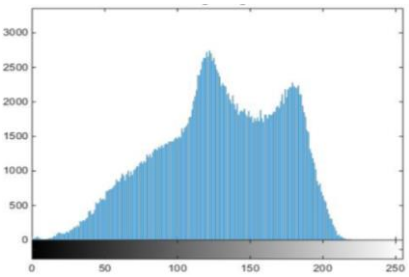
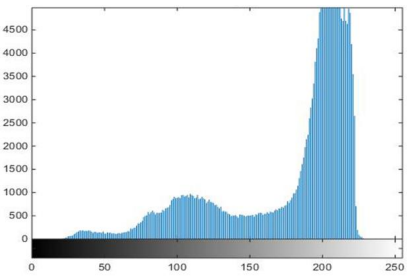
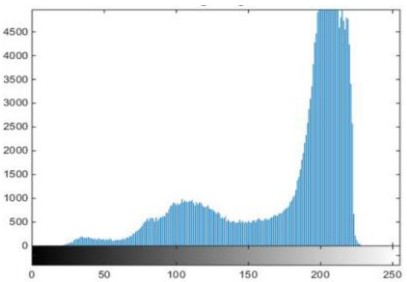
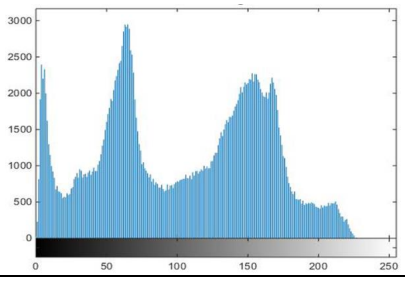
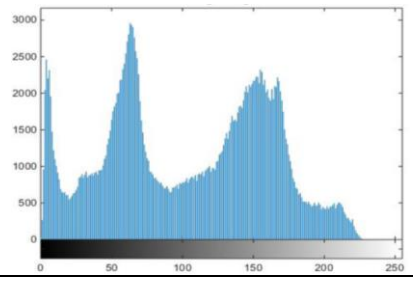


Şəkil 9. Konteyner pikselinin 219÷255 intervalındakı qiymətlərində məxfi informasiya bitlərinin Hartli düsturu əsasında və yeni alqoritm əsasında yerləşdirilməsinin müqayisəsi

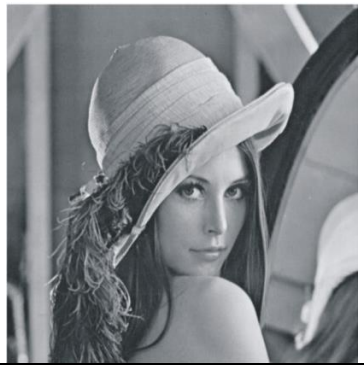
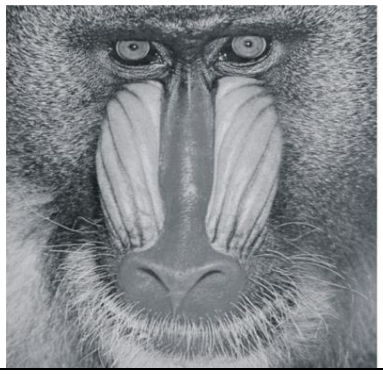
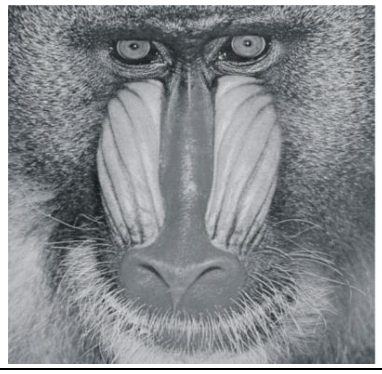
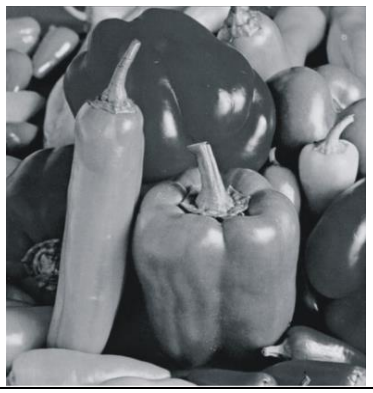
Təkli edilən alqoritmlərin eksperimental nəticələrini əks etdirən histoqramlar, konteyner və steqo−təsvirlərin müqayisəsi

Cədvəl 1.

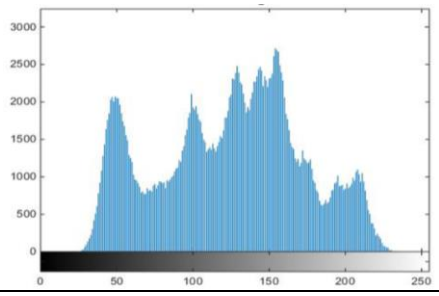
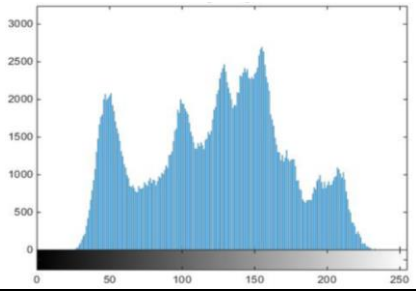
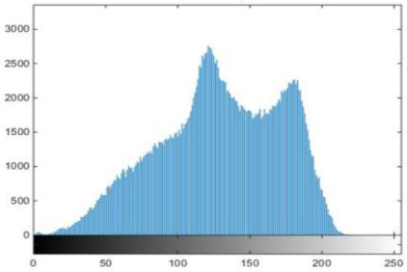
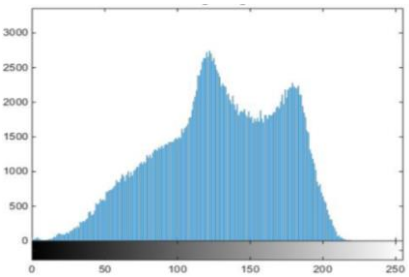
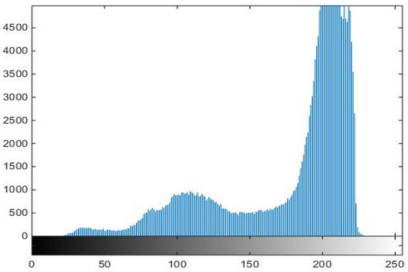
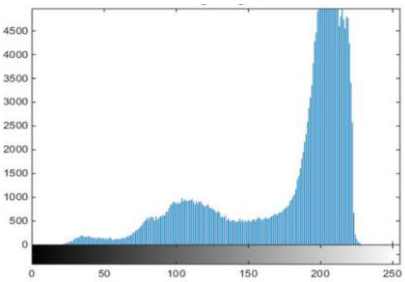
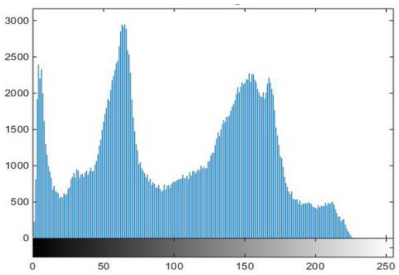
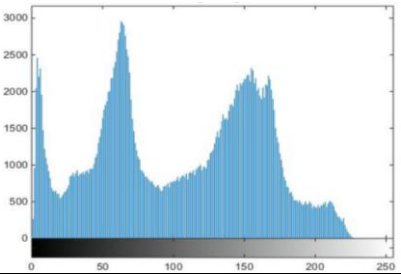
Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritminin histoqram göstəriciləri

Təsvirlər	İlkin təsvir	Steqo−təsvir
Lena		
Baboon		
Airplane		
Pepper		

Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritminin konteyner və steqo−təsvirlərinin vizual müqayisəsi

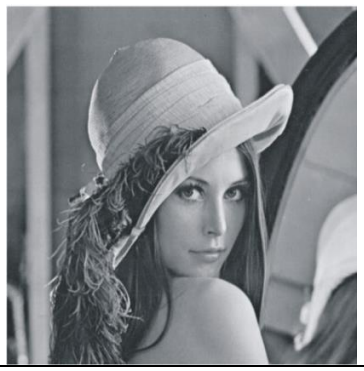
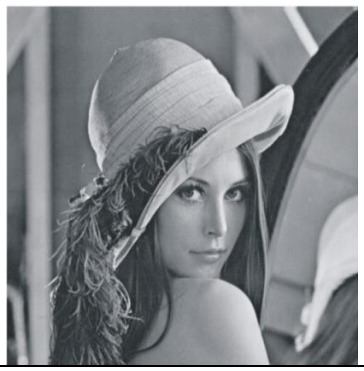
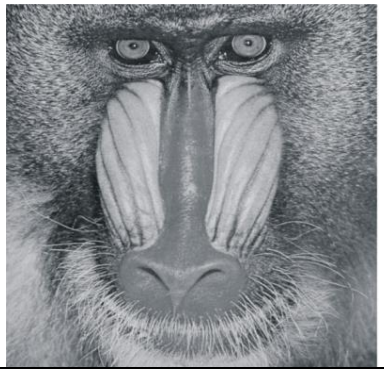
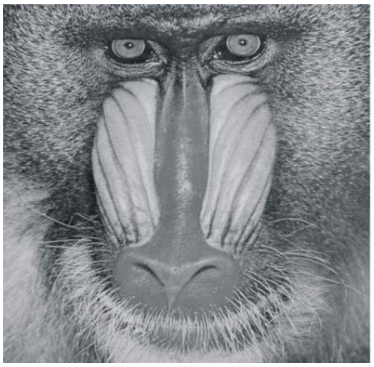
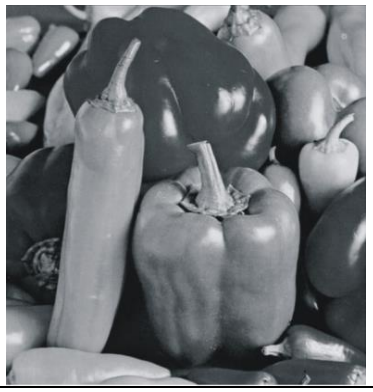
Təsvirlər	İlkin təsvir	Steqo –təsvir
Lena		
Baboon		
Pepper		
Airplane		

Cədvəl 3.
Təsvir interpolyasiyasına əsaslanan məxfi informasiya gizlədilmə alqoritminin histoqram göstəriciləri

Təsvirlər	İlkin təsvir	Steqo−təsvir
Lena		
Baboon		
Airplane		
Pepper		

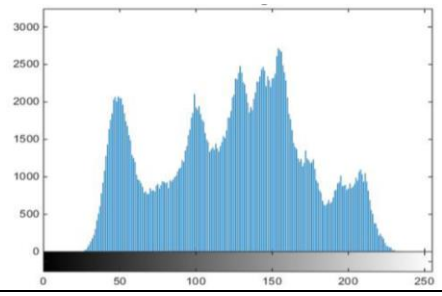
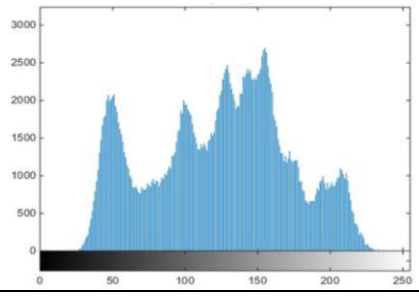
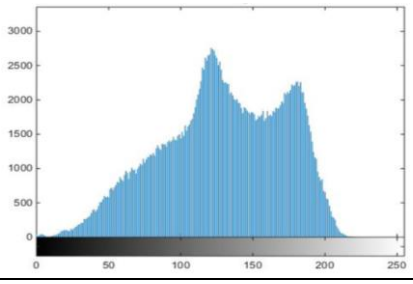
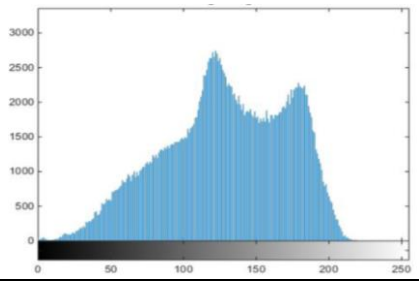
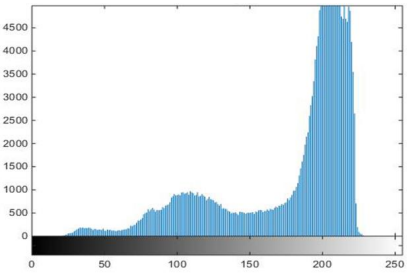
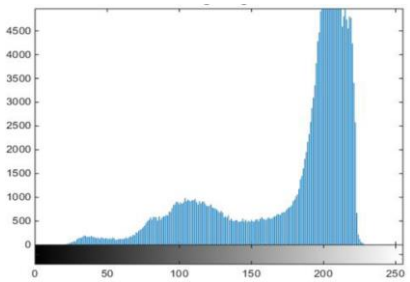
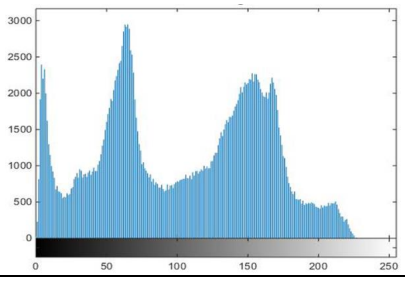
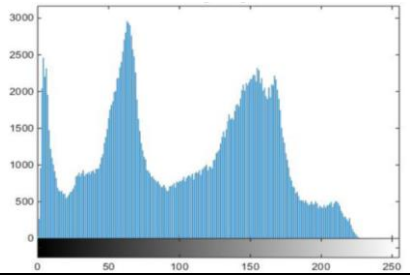
Cədvəl 4.

Təsvir interpolyasiyasına əsaslanan məxfi informasiya gizlədilmə alqoritminin konteyner və steqo−təsvirlərinin vizual müqayisəsi

Təsvirlər	İlkin təsvir	Steqo –təsvir
Lena		
Baboon		
Pepper		
Airplane		

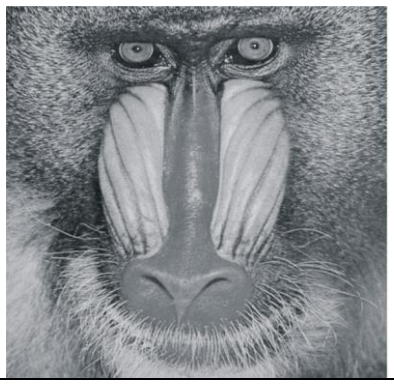
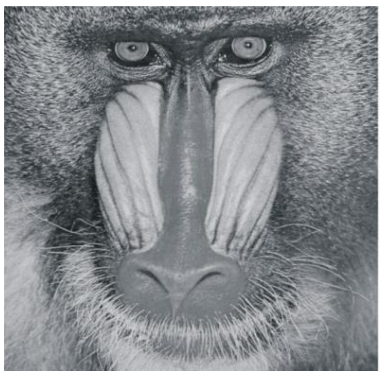
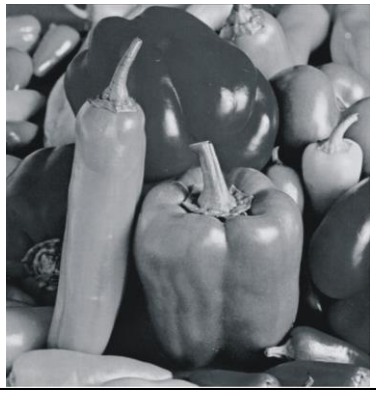
Cədvəl 5

Kvorum funksiyasına əsaslanan informasiya gizlədilmə alqoritminin histoqram göstəriciləri

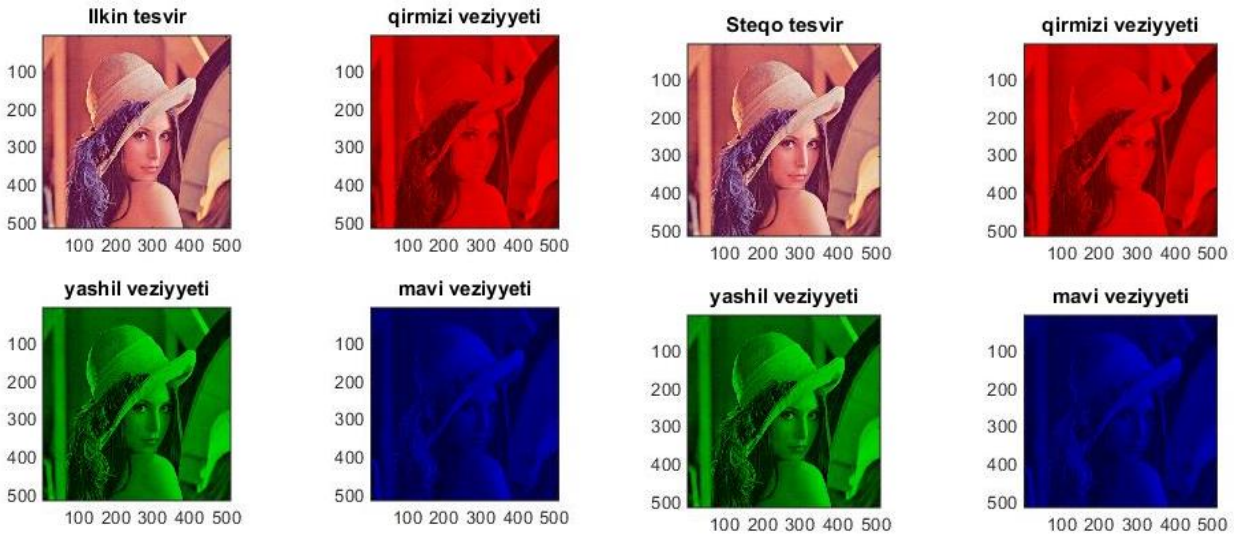
Təsvirlər	İlkin təsvir	Steqo−təsvir
Lena		
Baboon		
Airplane		
Pepper		

Cədvəl 6

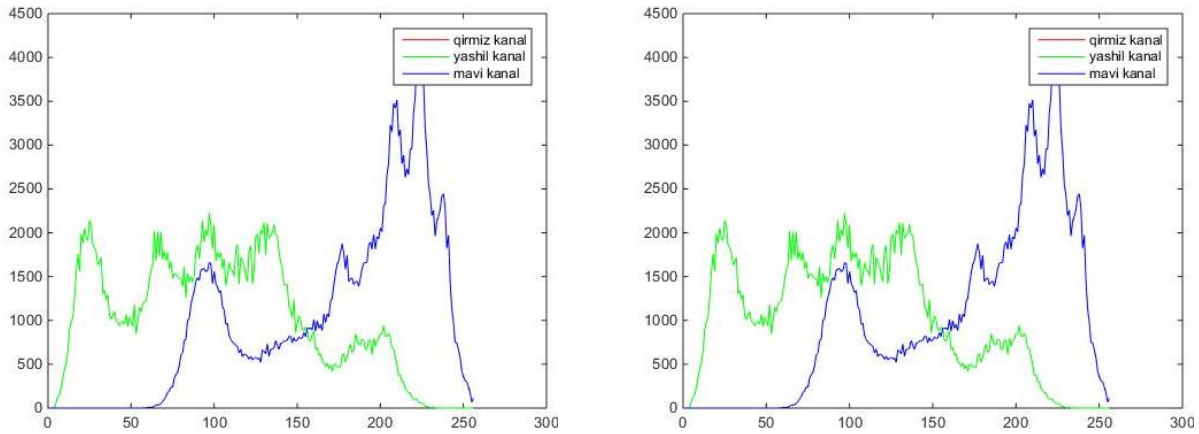
Kvorum funksiyasına əsaslanan informasiya gizlədilmə alqoritminin konteyner və steqo−təsvirlərinin vizual müqayisəsi

Təsvirlər	İlkin təsvir	Steqo –təsvir
Lena		
Baboon		
Pepper		
Airplane		

Böyük həcmli məxfi informasiya gizlədilmə alqoritminin təsvirləri və onların histoqram göstəriciləri

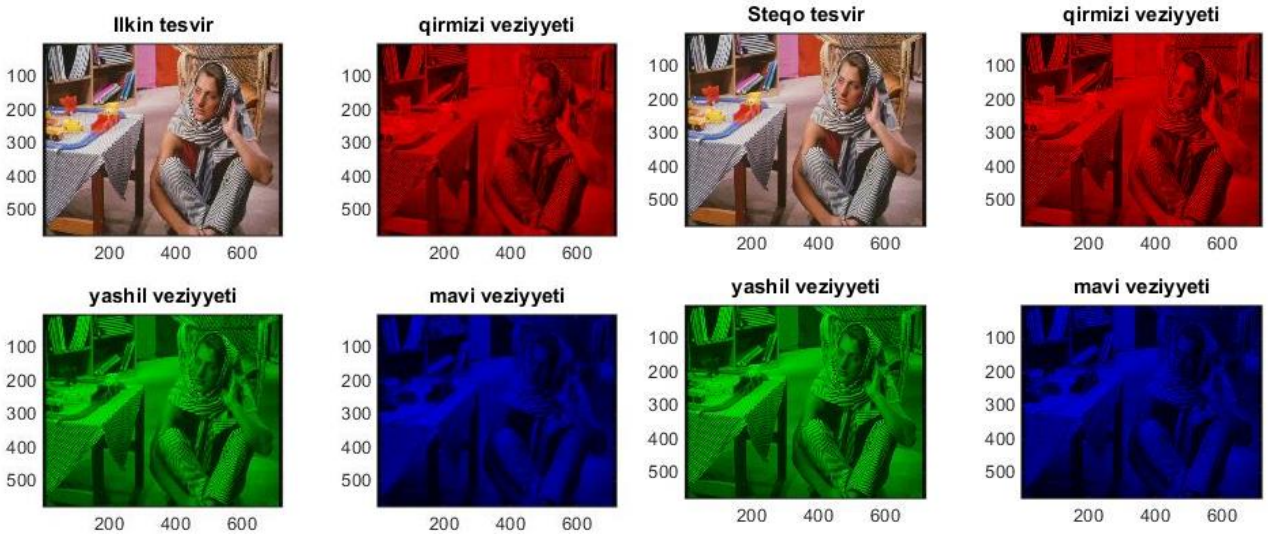


Şəkil 1. Konteyner təsvir və steqo- təsvir Lena

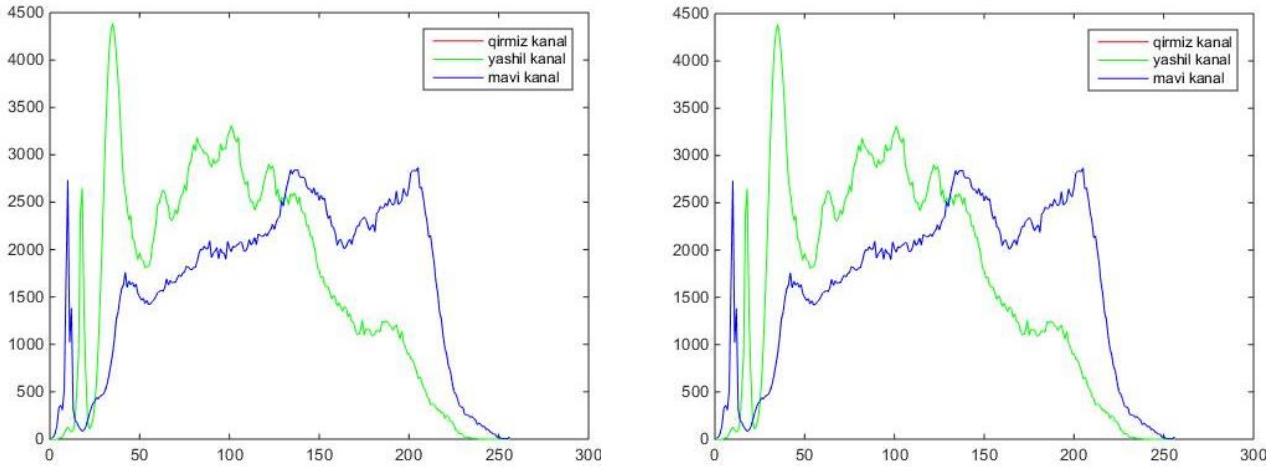


(a) **(b)**

Şəkil 2. Konteyner təsvirin histoqramı (a), steqo−təsvirin histoqramı (b)

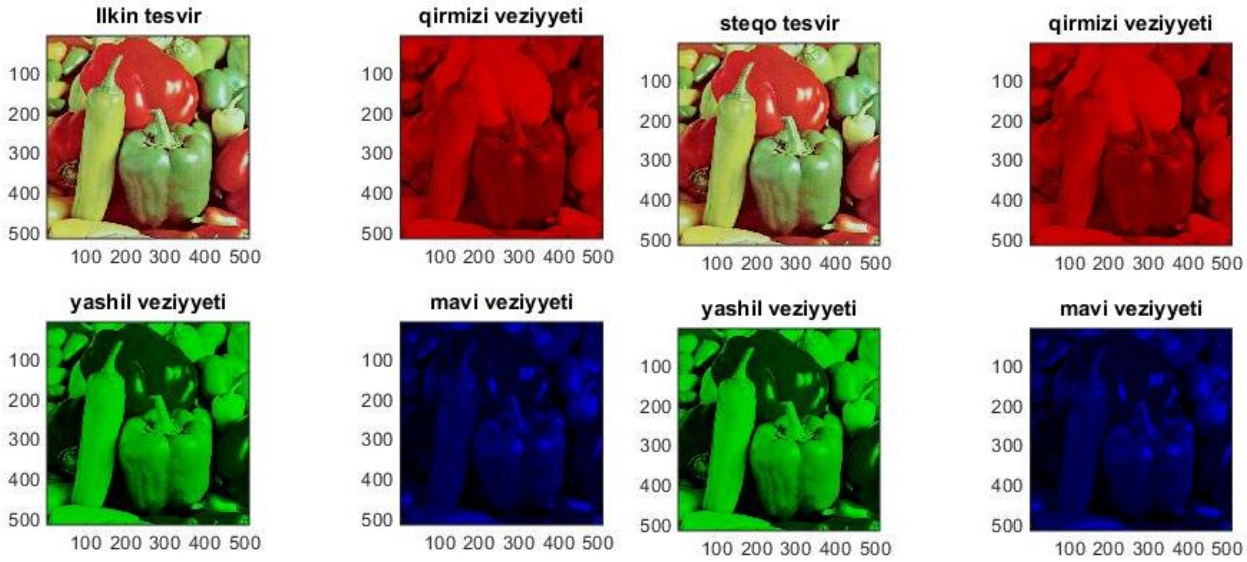


Şəkil 3. Konteyner təsvir və steqo- təsvir Barbara

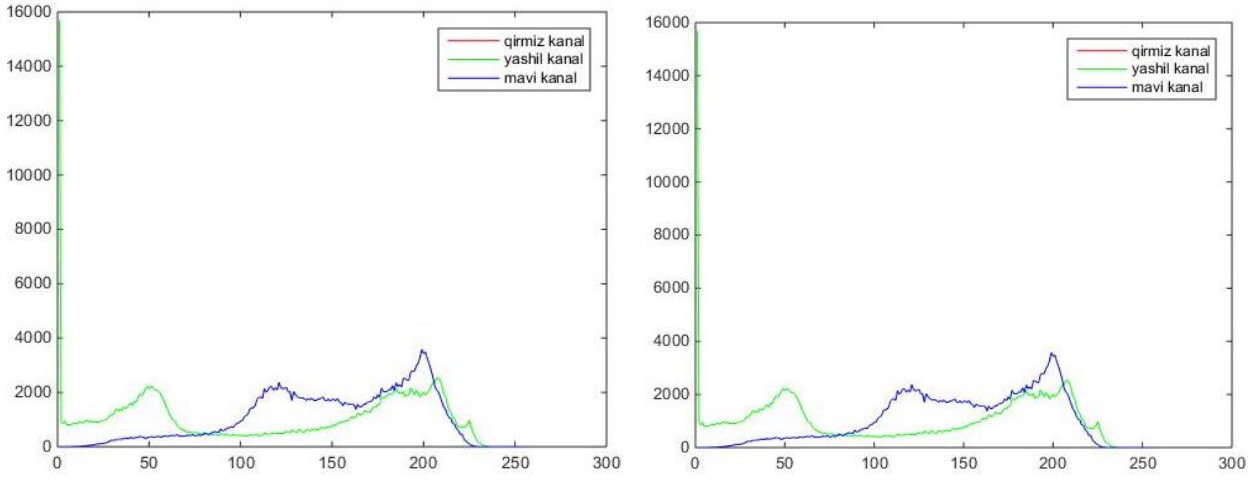


(a) **(b)**

Şəkil 4. Konteyner təsvirin histoqramı (a), steqo−təsvirin histoqramı (b)

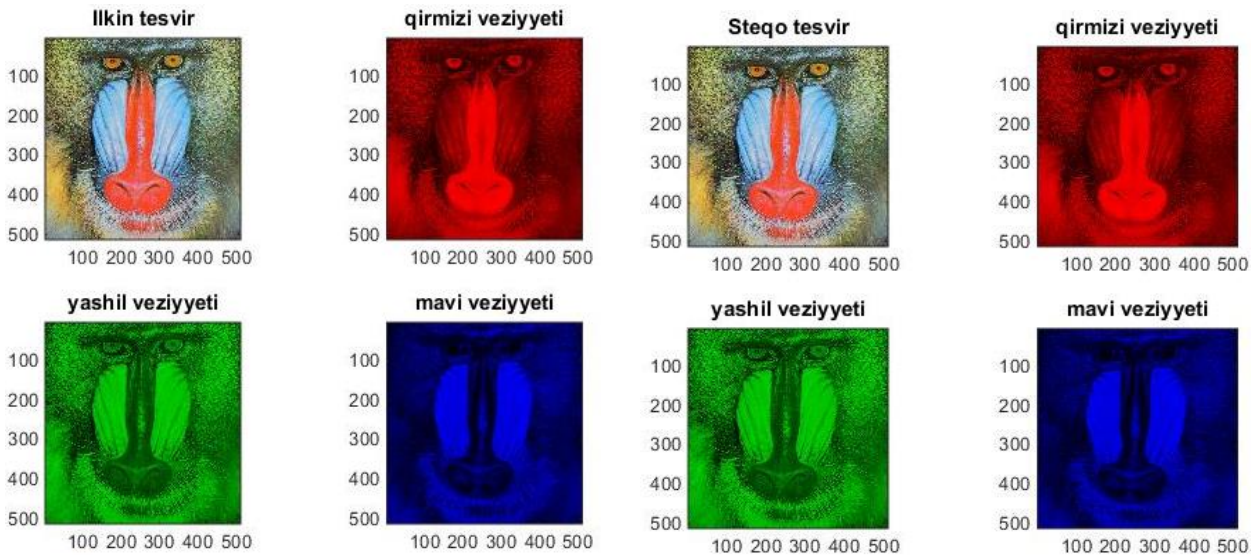


Şəkil 5. Konteyner təsvir və steqo–təsvir peppers

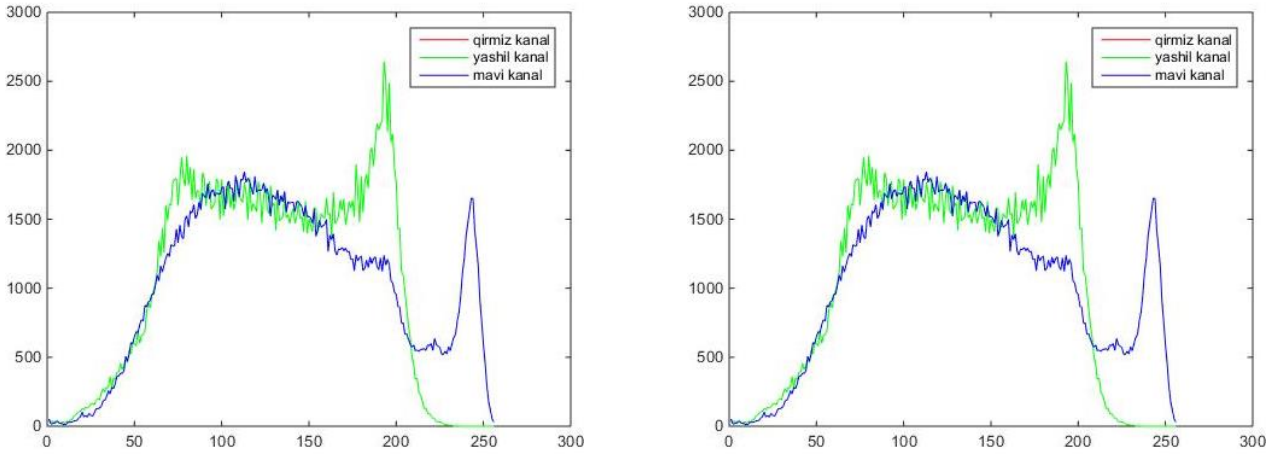


(a) **(b)**

Şəkil 6. Konteyner təsvirin histoqramı (a), steqo−təsvirin histoqramı (b)



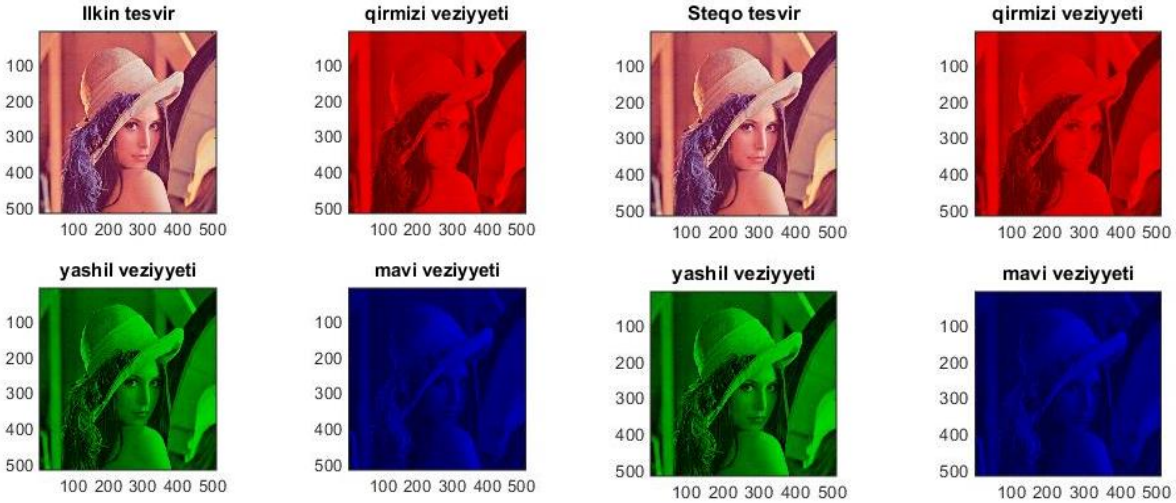
Şəkil 7. Konteyner təsvir və steqo- təsvir baboon



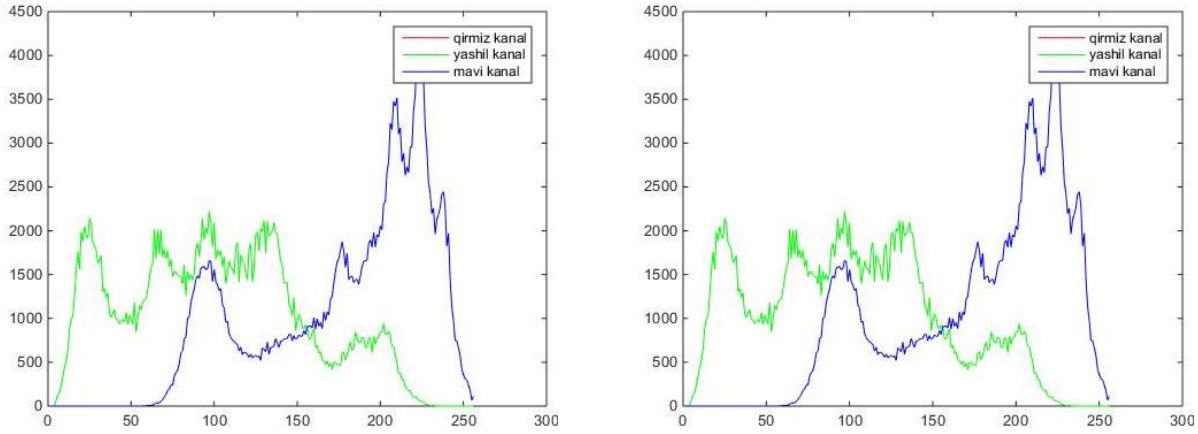
(a) **(b)**

Şəkil 8. Konteyner təsvirin histoqramı (a), steqo−təsvirin histoqramı (b)

Yüksək vizual keyfiyyət prioritetli məxfi informasiya gizlədilmə alqoritminin təsvirləri və onların histoqram göstəriciləri

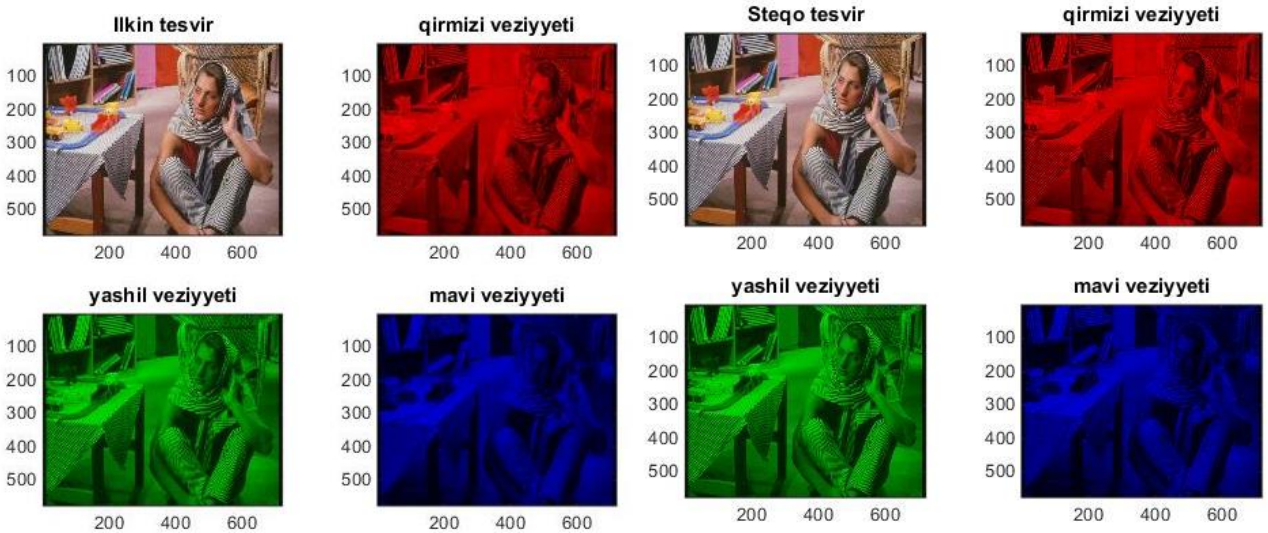


Şəkil 1. Konteyner təsvir və steqo- təsvir Lena

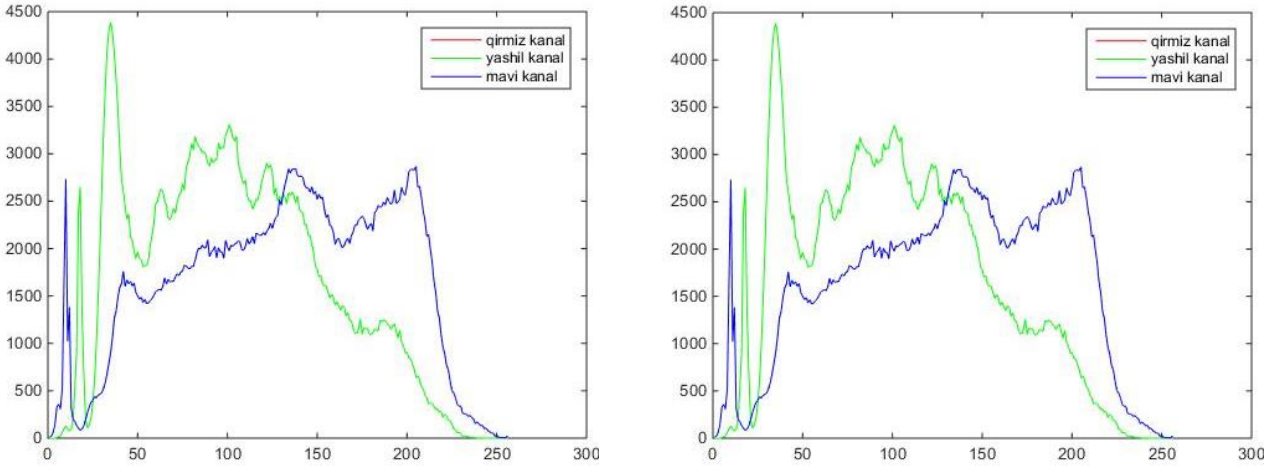


(a) (b)

Şəkil 2. Konteyner təsvirin histoqramı (a), steqo−təsvirin histoqramı (b)

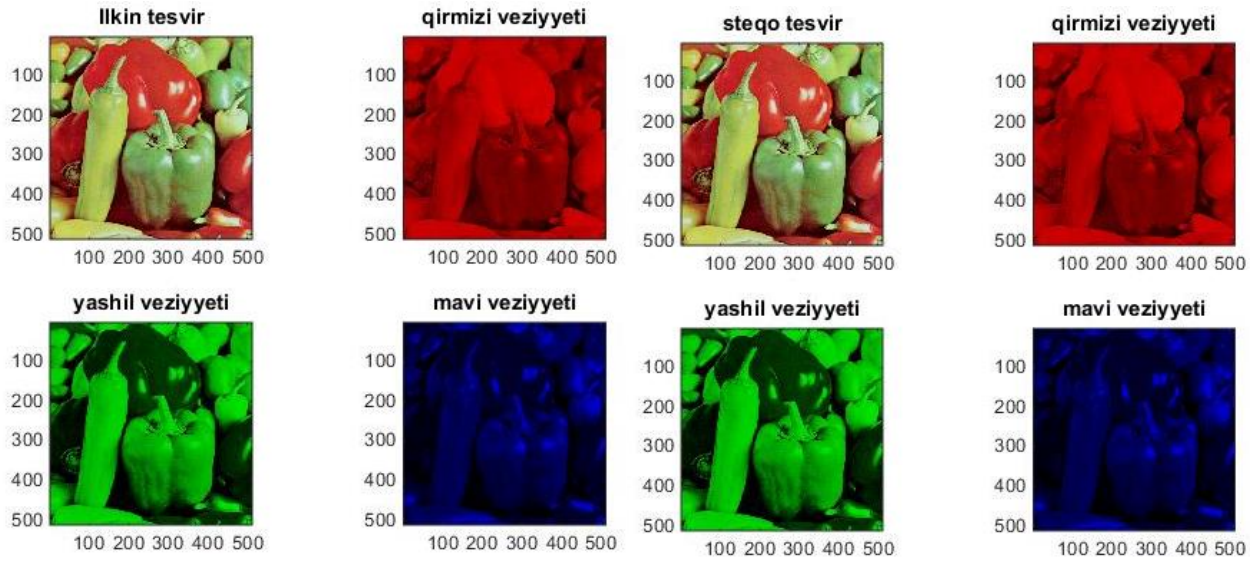


Şəkil 3. Konteyner təsvir və steqo- təsvir Barbara

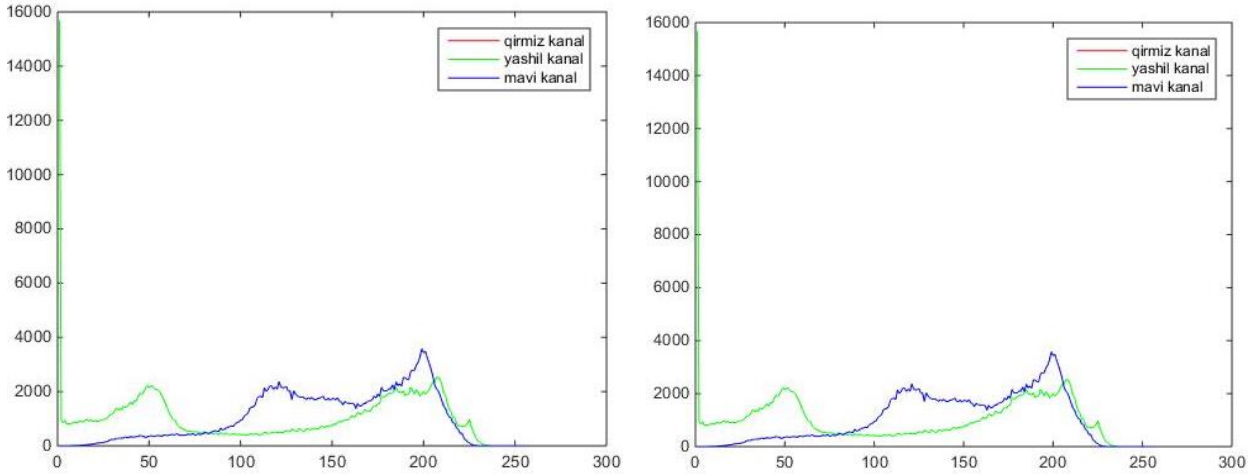


(a) (b)

Şəkil 4. Konteyner təsvirin histoqramı (a), steqo−təsvirin histoqramı (b)

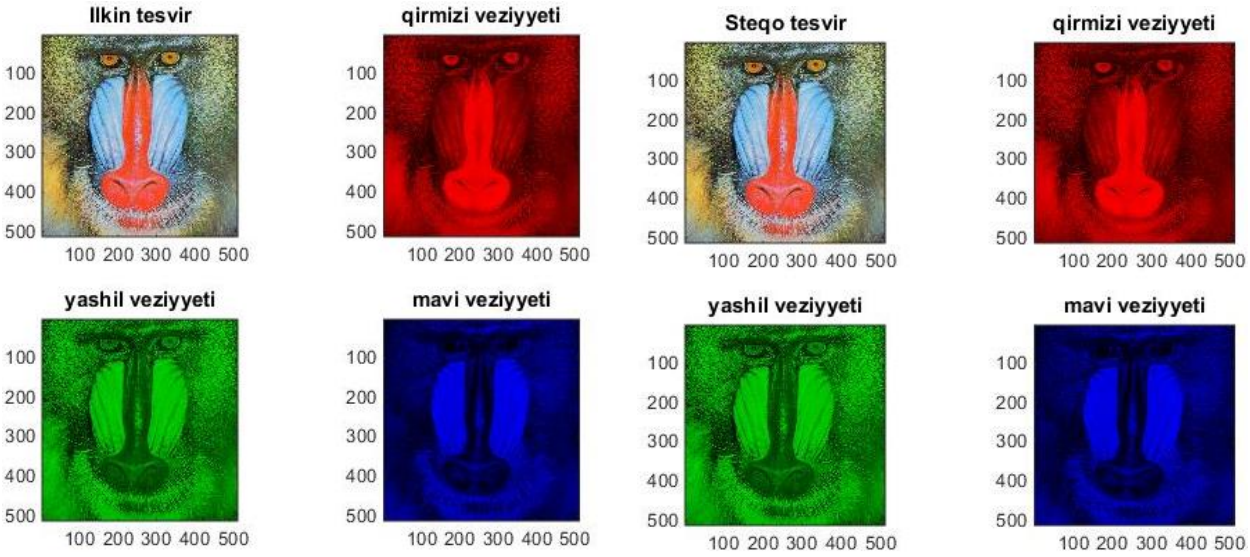


Şəkil 5. Konteyner təsvir və steqo- təsvir peppers

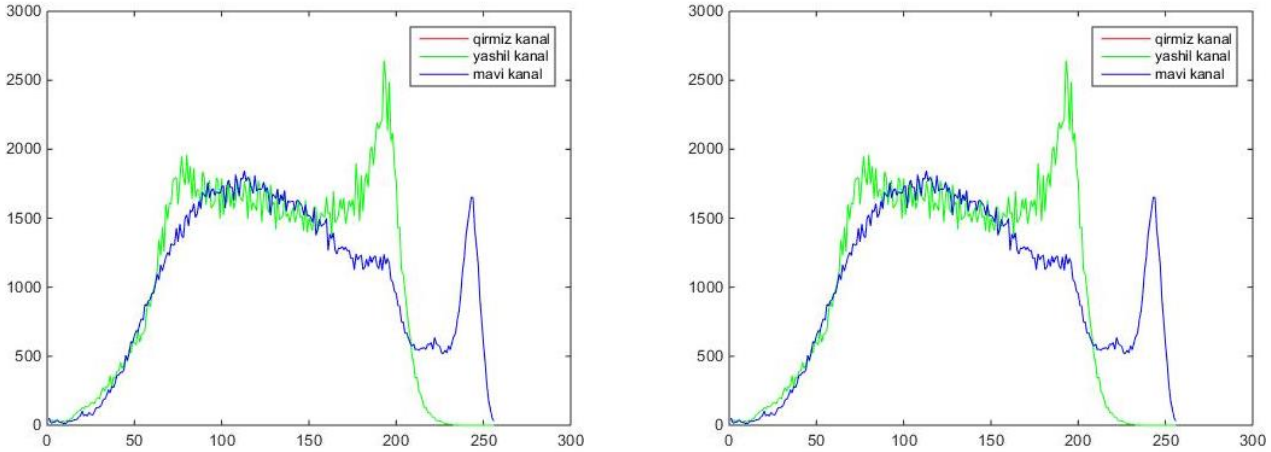


(a) **(b)**

Şəkil 6. Konteyner təsvirin histoqramı (a), steqo−təsvirin histoqramı (b)



Şəkil 7. Konteyner təsvir və steqo- təsvir baboon



(a) **(b)**

Şəkil 8. Konteyner təsvirin histoqramı (a), steqo−təsvirin histoqramı (b)

İXTİSARLARIN SİYAHISI VƏ ŞƏRTİ İŞARƏLƏR

BMP - Bit map point

BSM - Binary similarity measures - Binar oxşarlığın ölçülməsi

DFT - Discrete fourier transform technique - Diskret furye çevrilmə texnikası

DKT - Discrete cosine transform techniques -Diskret kosinus çevrilmə texnikaları

DVT - Discrete wavelet transform method - Diskret vayvelet çevrilmə alqoritmi

EC - Embedding capacity - Yerləşdirmə tutumu

EMD - Exploiting modification direction – Modifikasiya istiqamətindən istifadə

ENMI - Enhanced neighbor mean interpolation – Gücləndirilmiş qonşu interpolyasiya

ERİ - Elektron rəqəm imzası

ƏAB - Ən az əhəmiyyətli bit

GİF - Graphical data interchange format

GLM - Gray level modification - Boz səviyyə modifikasiyası

HCF - Histogram characteristic function- Histoqram xarakterik funksiyası

İGS - İnsan görmə sistemi

INP - İnterpolation by neighboring pixels – Qonşu piksellər üzrə interpolyasiya

JPEG - Joint photographic experts group

QF - Quarum function – Kvorum funksiyası

LSB - List significant bit

MBNS - Multi base notation system

MSE - Mean squared error – Orta kvadratik xəta

NMİ - Neighbor mean interpolation

NNC - Normalized cross correlation – Normallaşdırılmış çarpaz korrelyasiya

PFQ - Piksellərin fərq qiyməti

PNG - Portable network graphics

PoVs - Pair of Values – Qiymətlər cütü

PPM - Pixel pair matching- piksel cüt uyğunluğu

PSNR - Peak signal to noise ratio – Pik siqnal küy nisbəti

PVD - Pixel value diffrent

RDH - Reversible data hiding – Geri döndərilə bilən informasiya gizlədilməsi

RMSE - Root mean squared error – Kökaltı orta kvadratik xəta

RS - Regular and singular – Nizamlı və tək

SIFT - Scale invariant feature transform – Miqyasca dəyişməyən xüsusiyyət çevrilməsi

ŞAE - Şəbəkələr arası ekran

TCP - Transmission control protocol/ Internet protokol - Transmissiya nəzarət protokolu

TIFF - Targed image file format

TPVD - Tri-way pixel value differencing- Üç tərəfli piksel qiymətləri fərqi

TS - Təhlükəsizlik siyasəti

UDP - User datagram protocol -

VXŞ - Virtual xüsusi şəbəkə.