AZƏRBAYCAN RESPUBLİKASI

Əlyazması hüququnda

MƏXFİ İNFORMASİYANIN GİZLƏDİLMƏSİ ÜÇÜN EFFEKTİV ALQORİTMLƏRİN TƏDQİQİ VƏ İŞLƏNİLMƏSİ

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

Elm sahəsi: Texnika elmləri

İddiaçı: **Ababil Faxrəddin qızı Nağıyeva**

Fəlsəfə doktoru elmi dərəcəsi almaq üçün
təqdim edilmiş dissertasiyanın

AVTOREFERATI

Gəncə – 2025

Dissertasiya işi Azərbaycan Texnologiya Universitetində yerinə yetirilmişdir.

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

Rəsmi opponentlər: ----------

Azərbaycan Elm və Təhsil Nazirliyinin İnformasiya Texnologiyaları İnstitutunun nəzdində fəaliyyət göstərən ED 1.35 Dissertasiya Şurası

Dissertasiya şurasının sədri:
AMEA-nın həqiqi üzvü,
texnika elmləri doktoru, professor.
_____ **Rasim Məhəmməd oğlu Əliquliyev**

Dissertasiya şurasının elmi katibi:
texnika üzrə fəlsəfə doktoru, dosent
_____ **Fərqanə Cabbar qızı Abdullayeva**

Elmi seminarın sədri:
AMEA-nın müxbir üzvü,
texnika elmləri doktoru,
_____ **Ramiz Məhəmməd oğlu Alıquliyev**

İŞİN ÜMUMİ XARAKTERİSTİKASI

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 istifadə edilən 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. Aparılan tədqiqatlarda mövcud olan 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 alqoritimlərinin 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 miqyasca dəyişməyən xüsusiyyət çevrilməsi (scale invariant feature transform SIFT) 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.

İŞİN MƏZMUNU

Girişdə dissertasiya mövzusunun aktuallığının əsaslandırılması, problemin qoyuluşu və görüləsi işlərin səciyyəsi verilmişdir.

Birinci fəsildə (İnformasiya təhlükəsizliyinin əhəmiyyəti və istiqamətləri) [1,2,5,13] informasiya təhlükəsizliyi anlayışı, steqanoqrafiyanın informasiya təhlükəsizliyində yeri və rolu, steqanoqrafiya elmi ilə kriptoqrafiya elminin fərqli xüsusiyyətləri, steqanoqrafiya üsullarının qiymətləndirilməsi, steqanoqrafik üsulların kateqoriyaları, təsvir steqanoqrafiyası, hazırda steqanoqrafiya elmində həll olunmamış mövcud problemlər, steqoanaliz metodları ilə alqoritmlərin təhlükəsizlik səviyyəsinin qiymətləndirilməsi araşdırılaraq şərh edilmişdir. Təsvir steqanoqrafiyasında məxfi informasiyaları gizlətmək üçün müxtəlif metodlara əsaslanan alqoritmlərdən istifadə olunur. Bu fəsildə son illərdə təklif edilən metodlara nəzər yetirilir.

İnterpolyasiya əsaslı informasiya gizlədilmə metodu ilk dəfə "Qonşu piksellərin orta qiymətinə əsaslanan interpolyasiya" [1](Neighbor mean interpolation NMİ) metodu 2009–cu ildə Ki-Hyun Jung və Kee-Young Yoo tərəfindən təqdim edilmişdir. Bu metodla daha yüksək aydınlıq göstəricisi olan piksellər əldə etmək mümkün olur. Bu və digər seçilmiş metodların alqoritmləri və iş prinsipləri təfsilatları ilə dissertasiyada verilərək hərtərəfli analiz edilib.

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.

Analiz edilən 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 tədqiqatlar da təklif edilən alqoritmləri yoxlamaq məqsədi ilə eyni təsviri ilkin təsvir kimi

[1] Jung K.H, Yoo K.Y. Data hiding method using image interpolation //Comput Stand Interfaces,- 2009.№ 31,- p.465-470.

və eyni həcmdə məxfi informasiyanı həmin alqoritmlər vasitəsi ilə təklif edilən alqoritmlərdə gizlədilib. Bundan sonra əldə edilmiş steqo−təsvirin PSNR, MSE, SSIM, HC və ümumi həcmini aşağıda təqdim edilən düsturlar ilə hesablanıb.

Orta kvadratik xəta − MSE (Mean Square Error)

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

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)

$$RMSE = \sqrt{MSE} \quad (2)$$

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)

$$SNR = 10 \times \log_{10} \left(\frac{\sum_{i=1}^{M \times N} (C_i)^2}{\sum_{i=1}^{M \times N} (C_i - S_i)^2} \right) \quad (3)$$

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)

$$PSNR = 10 \times \log_{10} \left(\frac{Max}{MSE} \right) \quad (4)$$

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)

$$SSIM(x,y)=\left(\frac{\left(\left(2\cdot\mu_x\mu_y+C_1\right)\cdot\left(2\cdot\sigma_{xy}+C_2\right)\right)}{\left(\left(\mu_x^2+\mu_y^2+C_1\right)\cdot\left(\sigma_x^2+\sigma_y^2+C_2\right)\right)}\right) \quad (5)$$

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 EC (embedding capacity) isə hər pikselə gizlədilən məxfi informasiya bitlərinin miqdarını göstərir.

$$EC=\frac{tutum}{W\times H} \quad (6)$$

burada W və H təsvirin eni və hündürlüyüdür.

Aparılan analizin nəticələri dissrtasiya işində cədvəl 1.3.1-də verilib.

Cədvəldə ən yüksək ümumi həcm göstəricisi "Yeni interpolyasiya genişlənməsi" (new interpolation expasion NIE[2]) adlanan 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 qonşu piksellərin orta qiymətinə əsaslanan (Enhanced Neighbor Mean

[2] 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, 6,- p.7181-7205.

Interpolation, ENMİ[3]) interpolyasiya əsasında təqdim etdikləri məxfi informasiya gizlədilmə alqoritmindədir. 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 NIE metodunda PSNR 24,05 olduğu halda orta kvadratik xəta (MSE) 0,009 qiymətini alıb. Buna görə də yeni alqoritmlər işlənilərkən burada əldə edilən nəticələr nəzərə alınmalıdır.

Son illərin ən uğurlu hesab edilən steqanoqrafiya metodlarının analizi nəticəsində belə qənaətə gəlinir ki, informasiyanın gizlədilməsi üçün təklif edilən alqorimtlər keyfiyyət etibarilə yeni, daha çox həcmdə informasiyanın yerləşdirlməsini təmin edə bilən steqanoqrafik alqoritmlərin yaradılması zəruridir.

İkinci fəsildə (Yeni steqanoqrafik alqoritmlərin işlənilməsi) təklif edilən 3 yeni steqanoqrafik alqoritmlərin mahiyyəti açıqlanır. İkinci fəsildə təklif edilən alqoritmlər bunlardır:

- Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritmi;
- Təsvir interpolyasiyasına əsaslanan məxfi informasiya gizlədilmə alqoritmi;
- Kvorum funksiyasına əsaslanan informasiya gizlədilmə alqoritmi.

Təklif edilən steqanoqrafik alqoritmlərin işləməsinin hər bir addımı dissertasiyada ətraflı izah edilir.

Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritmində [9, 13] təsvirin vizual keyfiyyətinə üstünlük verilib və məlumatların gizlədilməsinin yeni steqanoqrafik alqoritminə əsaslanmışdır.

Bu bölmənin məqsədi böyük həcmdə məxfi informasiya gizlətmə qabiliyyəti, yüksək dayanıqlılıq və steqo−təsvirin vizual keyfiyyətinin qorunması prioriteti ilə məxfi informasiyaların gizlədilmə alqoritminin yaradılmasıdır. Problem iki mərhələdə həll olunur [9]. İlk

[3] 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.

addımda məxfi informasiyanın gizlədilməsi üçün məxfi açara əsaslanan ən az əhəmiyyətli bitlərin dəyişdirilməsindən (Least significant bit- LSB) istifadə olunur.

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

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. Beləliklə, bütün məxfi informasiya bitləri konteyner təsvirinin 2x2 bloklarındakı minimum pikselləri istisna olmaqla ixtiyari seçilmiş pikselərinə yerləşdirilərək steqo−təsviri əmələ gətirir. Məxfi informasiya bitlərinin gizlədilməsi və yenidən bərpa edilməsi steqo-açar vasitəsilə həyata keçirilir.

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. Fərz edək ki, N - mövcud konteyner bitlərinin sayı P_0^N və 0-dan $N-1$-ə qədər olan ədədlərin permutasiyası olsun.

Burada məxfi informasiya bitlərini yerləşdirəcəyimiz piksellər isə $P_0^N(0), P_0^N(1),.....P_0^N(n-1)$ bərabər 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 $\{0,...N-1\}$ arasında fərqli nəticələr alır. Bu prosesdə K gizli açarını bilmədən heç kim məxfi informasiya bitinin harada yerləşdirildiyini təxmin edə bilməməlidir.

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

$$f_K(i)=H(K\circ i) \tag{7}$$

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 açarıda 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.

$$\begin{aligned} &Y = Y \oplus f_{K1}(X)\\ &X = X \oplus f_{K2}(Y)\\ &Y = Y \oplus f_{K3}(X)\\ &Y = X \oplus f_{K4}(Y)\\ &\textit{geridönüş } X\circ Y \end{aligned} \tag{8}$$

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

$$\begin{aligned} Y &= i \; div \; x \\ X &= i \bmod x \\ Y &= \left(Y + f_{K1}(X)\right) \bmod y \\ X &= \left(X + f_{K2}(Y)\right) \bmod x \\ Y &= \left(Y + f_{K3}(X)\right) \bmod y \\ sonda &\mapsto Y * x + X \end{aligned} \tag{9}$$

Addım 6. İlkin təsvir 2x2 bloklara bölünür, onların daxilində ən aşağı qiyməti olan piksel minimal piksel olaraq təyin olunur (şəkil 1).

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

Şəkil 1. Konteyner təsvir bloku

Addım 7. Digər 3 pikselin hər birindən ən kiçik pikselin qiyməti çıxılır. (10) düsturundan istifadə edərək $D(j,j)$ fərq qiyməti hesablanır.

$$D(j,j) = I(i,j) - \min \tag{10}$$

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

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

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

Məsələnin həllinin ədədi nümunəsi və steqo-təsvirdən məxfi informasiyanın çıxardılması dissertasiya işində geniş verilmişdir.

Təsvir interpolyasiyasına əsaslanan məxfi informasiya gizlədilmə alqoritmi [10]. 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 interpolyasiya metodu ilə yerləşdirməkdir.

Təklif olunan üsul aşağıdakı mərhələlərdən ibarətdir:

- təsvirin kiçildilməsi
- təsvirin genişləndirilməsi
- məxfi informasiyanın yeni alqoritm ilə 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 (11) istifadə olunur.

$$\begin{aligned} C(0,0) &= O(0,0) \\ C(0,1) &= \left(O(0,0)+O(0,2)\right)/3+\left(O(2,0)+O(2,2)\right)/6 \\ C(1,0) &= \left(O(0,0)+O(2,0)\right)/3+\left(O(0,2)+O(2,2)\right)/6 \\ C(1,1) &= \left(O(0,0)+O(0,2)+O(2,0)+O(2,2)\right)/4 \end{aligned} \tag{11}$$

burada $O(i,j)$ ilkin təsvirin pikselləri, $C(i,j)$ isə interpolyasiya üsulu 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 (12) düsturu istifadə edərək piksellər arasında fərq qiymətləri hesablanır.

$$\begin{aligned} d_1 &= \max\left(\left|C_1(0,1)-C_1(0,0)\right|,\left|C_1(0,1)-C_2(0,0)\right|\right), \\ d_{2=}& \max\left(\left|C_1(1,0)-C_1(0,0)\right|,\left|C_1(1,0)-C_3(0,0)\right|\right) \\ d_3 &= \max\left(\left|C_1(1,1)-C_1(0,0)\right|,\left|C_1(1,1)-C_2(0,0)\right|,\left|C_1(1,1)-C_3(0,0)\right|,\left|C_1(1,1)-C_4(0,0)\right|\right) \end{aligned} \tag{12}$$

Addım 3. Hər bir pikselə daxil ediləcək məxfi bitlərin sayını müəyyən etmək üçün fərq qiymətlərini hesabladıqdan sonra hesab-

lamalardan 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 (13) düsturundan istifadə etməklə konteyner pikselinə məxfi bitlər yerləşdirilir

$$S_1(0,1)=\begin{cases}C_1(0,1)+b_1, C_1(0,1)\le O_1(0,1)\\ C_1(0,1)-b_1\end{cases}$$
$$S_2(1,0)=\begin{cases}C_1(1,0)+b_2, C_1(1,0)\le O_1(1,0)\\ C_1(1,0)-b_2\end{cases} \quad (13)$$
$$S_3(1,1)=\begin{cases}C_1(1,1)+b_3, C_1(1,1)\le O_1(1,1)\\ C_1(1,1)-b_3\end{cases}$$

burada Ckonteynerin pikselləri, S steqo-təsvirin pikselləri, b_1, b_2, b_3 isə məxfi informasiya bitləridir (Şəkil 2.).

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

C(0,0)	C(0,1)
C(1,0)	C(1,1)

Şəkil 2. (a) Steqo-təsvir (b) Konteyner təsvir

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

Kvorum funksiyasına əsaslanan informasiya gizlədilmə alqoritmi [3, 12]. 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. Dəyişilmənin nəticəsində 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 informasiyanın steqo−təsvirdən çıxarılması prosesi isə yerləşdirmə alqoritminin əksi olan alqoritmdən istifadə olunaraq həyata keçirilir.

İşlənilib təklif edilən kvorum funksiyası əsaslı informasiya gizlətmə alqoritminin steqo-hücumlara dayanıqlılığını, yəni təhlükəsizliyini təmin etmək məqsədi ilə məxfi informasiyanın şifrlənməsindən istifadə edilib.

Rijindel alqoritmi vasitəsilə məxfi informasiya bitləri tam şifrlənir və təklif edilən alqoritm vasitəsilə konteyner təsviri içərisinə yerləşdirilir. Təklif olunan steqanoqrafik alqoritmin yerinə yetirilmə ardıcıllığı aşağıdakı kimidir.

Məxfi informasiyanın konteyner təsvirinə gizlədilməsi:

Addım 1. Rijindel alqoritmindən istifadə edərək məxfi informasiya bitləri şifrlənir

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

Addım 2. Konteyner təsvir 2x2 bloklara bölünür (Şəkil 3)

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

Şəkil 3. Konteyner təsvir

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

$$c_{12} = a_{12} - \min$$
$$c_{21} = a_{21} - \min \quad (14)$$
$$c_{22} = a_{22} - \min$$

Alqoritmdə məxfi informasiyaların daxil edilməsi və çıxarılması üçün 3 girişli kvorum funksiyasından istifadə edilir. Kvorum funksiyası (QF), Bul cəbrində, heş funksiyasında və s. geniş istifadə olunur. Kvorum funksiyası aşağıdakı kimi verilir [4].

$$QF(x_1, x_2, ...x_n) = \left\{ 1, \sum_{i=1}^{n} x_i \geq \frac{n}{2} \right. \quad (15)$$

Konteyner təsvirin c_{12}, c_{21}, c_{22} piksellərinin son 3 ən az əhəmiyyətli bitində məxfi informasiyaların gizlədilməsi üçün kvorum funksiyasından istifadə edilmişdir. Bunun üçün (16) düsturu ilə üç girişli kvorum funksiyasını (3QF) istifadə etmək mümkündür.

$$3QF(x_1, x_2, x_3) = (x_1 \wedge x_2) \oplus (x_1 \wedge x_3) \oplus (x_2 \wedge x_3) \quad (16)$$

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 olarsa, kvorum funksiyasının çıxış qiyməti 0-a bərabər olacaqdır. Kvorum funksiyası ilə məxfi informasiya bitləri gizlədildikdən sonra bloklardakı minimum qiymətlər yenidən həmin piksellər ilə cəmlənir.

Üç girişli kvorum funksiyasından (3QF) istifadə edərək informasiyaların gizlədilməsi proseduru dissertasiya işində ətraflı təsvir edilmişdir.

<u>Üçüncü fəsildə</u> (Rəngli təsvirlərdə SIFT alqoritmi istifadə etməklə məxfi informasiyanın gizlədilmə alqoritmlərinin işlənilməsi) iki yeni alqoritm təklif edilib:

[4] 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),- pp. 20527 –20545.

- Böyük həcmli məxfi informasiya gizlədilmə alqoritmi;
- Yüksək vizual keyfiyyət prioritetli məxfi informasiya gizlədilmə alqoritmi.

Böyük həcmli məxfi informasiya gizlədilmə alqoritmi. Bu fəsildə də steqanoqrafik alqoritmlərin keyfiyyət göstəricilərinə uyğun olması 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)) alqorimindən istifadə edilib.

Təklif edilən məxfi informasiya gizlədilmə alqoritmində məxfi informasiya bitləri konteyner təsvirin mavi kanalının SIFT alqoritmi ilə seçilmiş piksellərinə yerləşdirilir. SIFT alqoritmi təsvirdə əsas nöqtə xüsusiyyətlərini müəyyən etmək üçün istifadə edilən alqoritmidir[5]. SIFT alqoritmi həm də obyekt və ya səhnənin tanınması, 3D strukturun modelləşdirilməsi, hərəkətin izlənməsi və s. kimi və təsvirlər arasında müqayisə üçün istifadə edilə bilən xüsusiyyətlərə malikdir.

İnformasiya gizlədilmə prossesinə keçməzdən əvvəl SIFT alqoritmindən istifadə etməklə rəngli təsvirdə açar nöqtə pikselləri müəyyən edilir.

Məxfi informasiya bitlərinin gizlədilməsinin xaotik olması alqoritmin vizuallıq və təhlükəsizlik keyfiyyətini yüksəldir. SIFT alqoritmi ilə müəyyən edilən açar nöqtə piksellərinə məxfi informasiya bitlərinin gizlədilmə ardıcıllığı aşağıdakı kimidir [6].

Addım 1. SIFT alqoritmi ilə açar nöqtə pikselləri tapılır (Şəkil 4).

[5] 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. doi: 10.1109/ICCRE.2018.8376448.


Şəkil 4. İlkin təsvir Əsas nöqtələri müəyyən edilmiş təsvir

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 (17) düsturu ilə müəyyən edilmiş piksellərin səkkizə bölünməsindən alınan qalıq hesablanır:

$$n = p_{i,j} \bmod 8 \qquad (17)$$

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. (18) düsturunda göstərildiyi kimi konteyner təsvirinin pikseli ilə cəmlənir.

$$S_{i,j} = p_{i,j} + d_8 \qquad (18)$$

burada $S_{i,j}$ steqo−təsvir pikseli, d_8 isə səkkizlik say sisteminə çevrilmiş məxfi informasiya bitidir.

Beləliklə məxfi informasiya bitləri konteyner təsvirinə yerləşdirilir.

Məxfi informasiyanın çıxardılması (gizlədilmənin əksi) dissertasiya mətnində verilib.

- **Yüksək vizual keyfiyyət prioritetli məxfi informasiya**

gizlədilmə alqoritmi. Yuxarıda təqdim edilən alqoritmin digər bir variantında isə vizual keyfiyyəti qoruyub saxlamaq məqsədi ilə mavi kanalın müvafiq piksellərinin 4-ə bölünməsindən alınan qalığı tapılır, daha sonra alınan qalığı ikilik say sisteminə çevirərək oradakı bitlərin sayına uyğun məxfi informasiya bitləri seçilir. Daha sonra seçilən bitlər 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 gizlədiləcəkdir. Bu alqoritmin əsas məqsədi konteynerin vizual keyfiyyətinin qorunub saxlanılmasıdır. Belə ki, bu alqoritimdə 3.2 bölməsində təklif edilən alqoritmə nisbətən vizuallıq keyfiyyət daha yüksəkdir. Alqoritm-aşağıdakı addımlarla realizə edilir.

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 (19) düsturu ilə müəyyən edilmiş piksellərin dördə bölünməsindən alınan qalıq hesablanır:

$$n = p_{i,j} \bmod 4 \tag{19}$$

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

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

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

Addım 7. (20) düsturunda göstərildiyi kimi konteyner təsvirinin pikseli ilə cəmlənir.

$$S_{i,j} = p_{i,j} + d_4 \tag{20}$$

burada $S_{i,j}$ steqo−təsvir pikseli, d_4 isə dördlük say sisteminə çevrilmiş məxfi informasiya bitidir.

Beləliklə məxfi informasiya bitləri konteyner təsvirinə

yerləşdirilir.

Dördüncü fəsildə təklif edilən alqoritmlərin eksperimental tədqiqi verilmişdir.

EKSPERİMENTAL TƏDQİQATLAR

Ən az əhəmiyyətli bitlərin əvəz edilməsi metoduna əsaslanan məxfi informasiyanın gizlədilmə alqoritminin [7 ,9, 11] eksperimental tədqiqatlarının nəticələri, nəzəri aparılan tədqiqatların doğruluğunu yoxlamaq məqsədi ilə təsvirlər bazasından USC-SIPI götürülmüş standart təsvirlər üzərində aparılaraq əldə olunub. Eksperimentlər MATLAB/R2023b proqram mühitində aparılıb. Steqo-təsvirin keyfiyyətini yoxlamaq üçün PSNR-ın qiyməti ümumi qaydada hesablanır. Alınan nəticə konteyner təsviri ilə steqo-təsvirin oxşarlıq dərəcəsini müəyyən edir. PSNR-ın qiyməti bilavasitə steqo-təsvirin vizual keyfiyyəti ilə bağlıdır. Bu qiymət nə qədər çox olarsa, müqayisə olunan təsvirlərin oxşarlığı bir o qədər yüksəkdir. Müqayisə edilən təsvirlərin nümunələri cədvəl 1-də göstərilib.

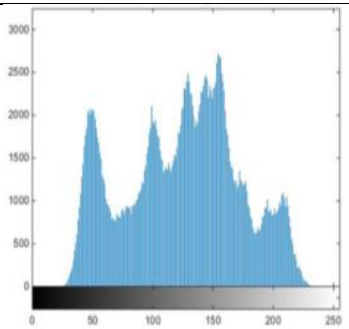
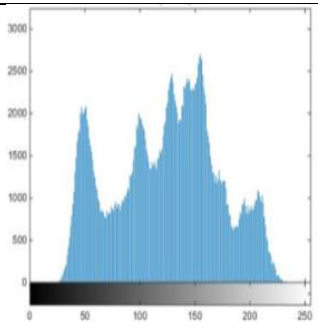
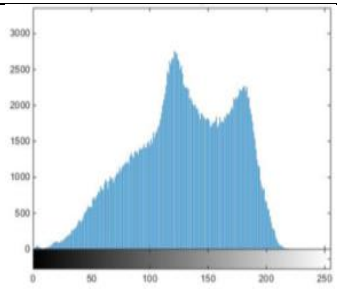
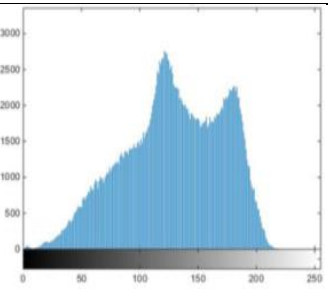
Cədvəl 2-də ilkin və onlara müvafiq olan steqo-təsvirlərin histoqramları verilib. Cədvəldən görünür ki, müqayisə edilən təsvirlərin histoqramları bir birindən demək olar ki, fərqlənmir. Bu da o deməkdir ki, müqayisə edilən təsvirlər yüksək dərəcədə identikdir və ona görə də açıq kommunikasiya kanalında ötürülən informasiyanın mövcudluğunu aşkarlamaq çətindir.

Cədvəl 1. Müqayisə edilən təsvirlər

Təsvirlər	İlkin-təsvirlər	Steqo – təsvirlər
Lena		

Baboon		

Cədvəl 2. Müqayisə edilən təsvirlərin histoqramları

Təsvirlər	Ilkin təsvir	Steqo-təsvir
Lena		
Baboon		

Konteyner və steqo–təsvir arasındakı PSNR qiymətləri müxtəlif müəlliflərin son illər elmi ədəbiyyatda təqdim etdikləri göstəricilər ilə müqayisə edilib. Müqayisə üçün eyni sınaq təsvirlərindən istifadə

olunub. Sınaqların nəticələri cədvəl 3-də verilib. Cədvəldə verilən rəqəmlərdən məlum olur ki, təklif olunan alqoritm müqayisə edilən alqoritmlərə görə nisbətən daha yüksək PSNR və daha böyük həcmdə məxfi informasiya gizlədilməsinə malikdir.

Təsvirlərin hər birinin PSNR-ı 36 dB-dən yüksəkdir, bu da o deməkdir ki, konteynerə informasiyanın gizlədilməsi ilə əlaqədar olan qaçılmaz pozuntular insan gözü tərəfindən qavranılmaz olur. PSNR ilə yanaşı daha dəqiq nəticələr əldə etmək məqsədi ilə qrafiki histoqram metodu da istifadə edilib.

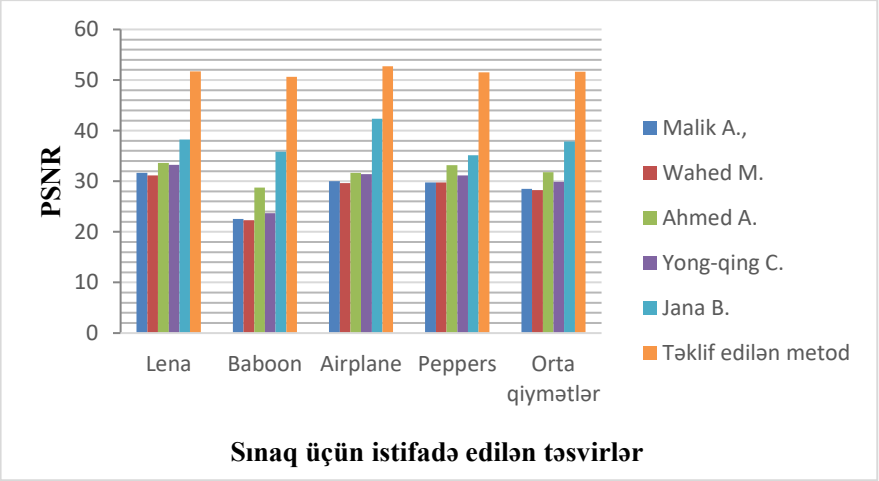
Cədvəl 3. Steqo-təsvirin keyfiyyət göstəricilərinin müqayisəli cədvəli

Giriş təsvirləri	**Keyfiy-yət göstəri ciləri**	**Malik A., Sikka G.[6] .**	**Wahed M.A., Nyeem , H[7]**	**Ahmad A.M[2].,**	**Yong-qing C.[8]**	**Jana B., Giri D.,[9]**	**Təklif edilən alqo-ritm**
Lena	HC (bit) PSNR (dB)	177777 31,67	198902 31,14	224528 33,60	226085 33,27	223031 38,25	240962 51,73
Baboon	HC (bit) PSNR (dB)	262272 22,57	125562 22,29	259737 28,77	231401 23,70	273235 35,85	277492 50,62
Airplane	HC (bit)	185676 30,01	179961 29,66	228863 31,67	213460 31,43	211321 42,34	208392 52,74

[6] Malik, A. Sikka, G., Verm, H.K. Image interpolation based high capacity reversible data hiding scheme//Multimedia Tools Application,- 2018. №76,- p. 2454-7190.
[7] Wahed, M.A. Nyeem, H. Reversible data hiding with interpolation and adaptive embedding // Multimedia Tools and Applications,- 2019. 78(3),-p.10795-10819.
[8] 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**.**
[9] 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.

	PSNR (dB)						
Peppers	HC (bit) PSNR (dB)	175669 29,78	195490 29,78	223295 33,18	227493 31,13	232563 35,12	247864 51,53
Orta qiymət-lər	HC (bit) PSNR (dB)	**200348** **28,50**	**189978** **28,22**	**234106** **31,8**	**224609** **29,88**	**235037** **37,89**	**243677** **51,65**

Şəkil 5-də cədvəl 3-ün diaqramı təqdim olunub. Diaqramda təklif edilən alqoritmin PSNR qiymətlərinin digər tədqiqatlarda təqdim olunan PSNR qiymətlərindən fərqi və müxtəlif təsvirlərdən asılılığı göstərilir.



Şəkil 5. PSNR göstəricilərinin müxtəlif təsvirlərdən asılılığı

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

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

Cədvəl 4. 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

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 5-də verilib.

Cədvəl 5. Steqo-təsvirlərin RS steqoanaliz nəticələri

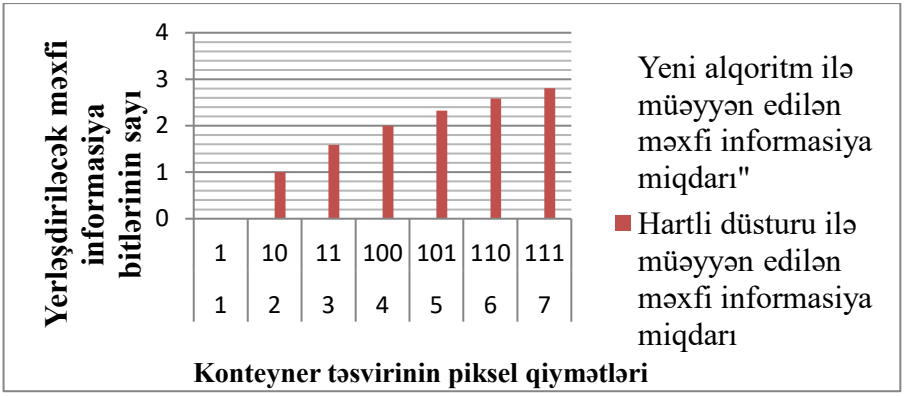
Steqo−təsvir	**RS steqo-analizi**	**Gizlədilmiş məxfi informasiya həcmi (bayt)**			
		1000	5000	10000	15000
Lena	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0080	0,0087	0,0093	0,0099
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0091	0,0095	0,0097	0,0099
Baboon	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0064	0,0079	0,0093	0,0752
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0073	0,0163	0,0231	0,0243
Airplane	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0093	0,0095	0,0099	0,0103
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0082	0,0086	0,0205	0,0216
Peppers	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0097	0,0098	0,0100	0,0109
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0085	0,0085	0,0092	0,0098

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

Təsvir interpolyasiyasına əsaslanan steqanoqrafik məlumat gizlətmə alqoritminin [7,10,11] eksperimentləri 512x512 ölçülü standart təsvirlərdə aparılıb. Həmin təsvirlər giriş təsviri kimi təklif edilən informasiyanın gizlədilmə alqoritmin effektivliyini yoxlamaq üçün istifadə edilib. Eksperimentlər ədəbiyyatda təklif edilən dörd uğurlu alqoritmlərin istifadə etdikləri eyni təsvirlər üzərində aparılıb. Hər bir təsvir dissertasiyada təklif olunan alqoritmə uyğun tərzdə emal edilib.

İlk olaraq yeni alqoritm əsasında məxfi informasiyanın miqdarının müəyyən olunmasına nəzər yetirək. İşlənilən alqoritmin digər alqoritmlər ilə müqayisəsinin eksperimental nəticələrinin qrafiki Şəkil 6 - da 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 6. Konteyner pikselinin 1÷7 intervalındakı qiymətlərində məxfi informasiya bitlərinin yerləşdirilməsinin müqayisəsi.

Şəkil 6-dan göründüyü kimi konteyner təsvirin piksellərinin 1÷7 intervalındakı qiymətlərində pikselin qiymətindən asılı olmayaraq gizlədilən məxfi bitlərin sayı daha çoxdur.

Təklif edilən alqoritmin effektivliyini dəyərləndirmək məqsədilə, onun eksperimental göstəricilərini son illərdə dərc olunmuş alqoritmlərlə müqayisə edilib. Təklif edilən yeni alqoritmin hədəfi etalon təsvirlərin minimal pozuntuları ilə daha böyük həcmdə məxfi informasiya gizlədilməsinə nail olmaqdır.

Eksperimentlərin müqayisəli nəticələri cədvəl 6-da verilib. Cədvəldən göründüyü kimi təqdim edilən alqoritmlərə təxminən bənzər gizlətmə həcminə, malik olduğu halda daha yüksək vizual keyfiyyəti təmin edir. Böyük həcmdə məxfi informasiyanın gizlədilməsindən sonra təsvirin vizual keyfiyyətinin yüksək səviyyədə qorunub saxlanılması təklif olunan alqoritmin üstün cəhti kimi dəyərləndirilə bilər.

Eksperimental təsvirlər tam olaraq dissertasiyada verilib. Eyni zamanda məxfi informasiyaları gizlətmə proseduru sadə yolla həyata keçirilir, hesablama mürəkkəbliyi müşahidə edilmir. Təsvirin növündən asılı olmayaraq PSNR 50 dB artıq olub. Cədvəl 6-dan aydın görünür ki, təklif edilən alqoritm müqayisə edilənlərdən öz göstəricilərinə görə daha üstündür və gələcək tədqiqatlarda daha böyük həcmdə məxfi informasiya biti gizlədilməsinə təkan verir.

PSNR-ın qiymətləri histoqram steqoanaliz üsulu ilə də təsdiqlənib. Histoqramlar və steqo-təsvirlərin keyfiyyət göstəricilərinin müqayisəli cədvəli dissertasiya işində verilib.

Cədvəl 6. Steqo-təsvirlərin keyfiyyət göstəricilərinin müqayisəli cədvəli

Giriş təsvirləri	**Keyfiyyət göstəriciləri**	**Yong-qing C.[8]**	**Malik A., Sikka G[6].**	**Jana B., Giri D[9]., **	**Təklif olunan alqo-ritm**
Lena	HC (bit) PSNR (dB)	226085 33,27	177777 31,67	223031 38,25	564744 39,56

Baboon	HC (bit) PSNR (dB)	231401 23,70	262272 22,57	273235 35,85	676791 36,47
Airplane	HC (bit) PSNR (dB)	213460 31,43	185676 30,01	211321 42,34	524719 35,88
Peppers	HC (bit) PSNR (dB)	227493 31,13	175669 29,78	232563 35,12	656611 39,32
Sailboat	HC (bit) PSNR (dB)	364589 31,80	175183 29,04	236132 29,03	378123 33,36
Boat	HC (bit) PSNR (dB)	343589 29,82	124236 32,22	295325 31,26	369563 35,93
Couple	HC (bit) PSNR (dB)	381589 26,82	354137 24,36	378256 23,48	400021 29,68
House	HC (bit) PSNR (dB)	236589 32,02	235325 31,32	217482 33,27	282753 36,21
Orta qiymətlər	**HC (bit) PSNR (dB)**	**278099 29,99**	**211284 28,87**	**258418 33,575**	**481666 35,80**

Təklif edilən alqoritmin dayanıqlılığının daha dəqiq yoxlanılması üçün histoqram steqoanalizindən başqa RS steqoanalizindən istifadə edilmişdir. RS steqoanalizinin nəticələri 7-ci və 8-ci cədvəllərdə təqdim edilib. Yenə əvvəlcə boş konteyner təsvirlərinə RS steqoanalizi tətbiq edilib. Bu analizin nəticələri cədvəl 7- də göstərilib.

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

Daha sonra konteyner təsvirinə müxtəlif həcmdə məxfi informasiya bitləri müvafiq alqoritm vasitəsilə yerləşdirildikdən sonra RS steqoanalizi tətbiq edilərək dayanıqlılığı test edilib. Steqoanalizin nəticələri cədvəl 8- də göstərilib.

Cədvəl 7. 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

Cədvəl 8. Steqo−təsvirlərin RS steqoanaliz nəticələri

Steqo−təsvir	**RS steqoanalizi**	**Gizlədilmiş məxfi informasiya həcmi (bayt)**			
		1000	5000	10000	15000
Lena	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0080	0,0087	0,0093	0,0099
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0091	0,0095	0,0097	0,0099
Baboon	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0064	0,0079	0,0093	0,0752
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0073	0,0163	0,0231	0,0243
Airplane	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0093	0,0095	0,0099	0,0103
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0082	0,0086	0,0205	0,0216
Peppers	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0097	0,0098	0,0100	0,0109
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0085	0,0085	0,0092	0,0098

Kvorum funksiyasına əsaslanan informasiya gizlədilmə alqoritminin [3, 7, 11, 12] eksperimentləri təsvirlər bazasından götürülmüş 512x512 ölçülü təsvirlər üzərində aparılıb. Təklif olunan yeni alqoritmin effektivliyini və dəqiq nəticələr əldə etmək məqsədi ilə testlər müxtəlif uğurlu alqoritmlər üzərində 50 etalon təsvirlər istifadə etməklə aparılıb. Təsvirlər dissertasiya işində və əlavəsində yerləşdirilmişdir.

Etalon təsvirlər, təklif edilən alqoritmin giriş təsviri kimi istifadə edilib. Alınan nəticələrin doğruluğunu təsdiq etmək üçün sınaqlar müqayisə edilən alqoritmlərin istifadə etdiyi metdolarla test edilib. Eyni zamanda hər bir təsvir təklif edilən alqoritmə əsasən də yoxlanılıb. Müqayisə üçün son zamanlar bu sahə üzrə aparılan uğurlu tədqiqat işləri seçilmişdir.

Eksperimentlərin nəticələri cədvəl 9-da verilir. Cədvəldən göründüyü kimi hər iki göstəricilər üçün təklif etdiyimiz alqoritm daha yüksək göstəricilər nümayiş edir. Bu da öz növbəsində təklif edilən alqoritmin üstünlüyünün sübutudur.

İşlənilən məxfi informasiya gizlətmə alqoritminin əsas hədəfi steqo-təsvirdə yeni alqoritm ilə pozuntuları minimuma endirməklə daha çox məxfi informasiya biti yerləşdirmə həcminə nail olmaqdır. Cədvəl 5 dən göründüyü kimi məqsədə nail olunub. PSNR-ın qiyməti ilə yanaşı təsvirlər histoqram metodu ilə də sınaqdan keçirdilib. Histoqramlar dissertasiyada verilib. Verilən histoqramlardan məlum olur ki, giriş təsvirləri ilə steqo-təsvirlər arasında fərq nəzərə çarpmayacaq dərəcədə azdır.

Cədvəl 9. Steqo-təsvirlərin keyfiyyət göstəricilərinin müqayisəli cədvəli

İlkin təsvir	**Keyfiy-yət göstəric iləri**	**Yong-qing C.[8]**	**Malik A., Sikka G[6].**	**Jana B., Giri D[9].,**	**Sabeen G[4].**	**Təklif edilən alqorit m**
Lena	HC (bit) PSNR (dB)	226085 33,27	177777 31,67	223031 38,25	303318 48,01	301465 49,56
Baboon	HC (bit)	231401	262272	273235	191365	283115

	PSNR (dB)	23,70	22,57	35,85	48,21	50,47
Airplane	HC (bit) PSNR (dB)	213460 31,43	185676 30,01	211321 42,34	112721 46,05	256982 48,88
Peppers	HC (bit) PSNR (dB)	227493 31,13	175669 29,78	232563 35,12	296993 47,69	393216 49,32
Orta qiymət	**HC (bit) PSNR (dB)**	**224610 29,88**	**200349 28,50**	**235038 37,89**	**226099 47,49**	**308695 49,55**

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 10-da verilmişdir.

Cədvəl 10. 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 11-də verilib.

Eksperimental verilənlərin təhlili göstərir ki, müxtəlif həcmdə məxfi informasiya gizlədilməsi zamanı RS toplananlarının qiymətləri çox kiçik intervalda dəyişir və yüksək dayanıqlılıq qiymətləri həddi aşmır. Buna görədə təklif edilən alqoritm ilə informasiya gizlədilərsə

onun açıq komunukasiya kanalı ilə ötürülməsi zamanı steqo–sistem bədniyyətlinin hücumlarından tam qorunmuş olur.

Cədvəl 11. Steqo–təsvirlərin RS steqoanaliz nəticələri

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

Rəngli təsvirlərdə SIFT alqoritmi istifadə etməklə məxfi informasiyanın gizlədilmə alqoritmlərinin eksperimental tədqiqi. Eksperimentlərin doğruluğunu təmin etmək üçün müqayisə edilən alqoritmlərdə istifadə edilən rəngli eyni standart təsvirlər tədqiq edilib. Bu alqoritmdə məxfi informasiya bitləri rəngli təsvirin mavi kanalında SIFT alqoritmi ilə seçilmiş piksellərə gizlədilmişdir. Eksperimentlər zamanı məxfi informasiya bitlərinin təhrif olunmadığı aşakarlanıb.

Hücüm növlərinin yoxlanılmasından sonra belə qənaətə gəlmək olur ki, təklif edilən alqoritmdə SIFT alqoritminin istifadəsi bu növ hücumlara qarşı dayanıqlılığı təmin edir. Təklif edilən alqoritmlər eyni zamanda aşağıdakı bölmədə təqdim edilən analiz növləri ilə də

yoxlanılıb.

Vizual keyfiyyəti ölçmək üçün PSNR istifadə edilib.

Təklif edilən alqoritmin digər mövcud alqoritmlərlə müqayisəsi cədvəl 12 - 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 metodlarla PSNR və steqo−təsvirə yerləşdirilmiş məxfi informasiya bitlərinin həcmlərinin (HC) müqayisəsi göstərilib.

Cədvəl 12. Steqo−təsvirlərin keyfiyyət göstəricilərinin müqayisəsi

Giriş təsvirləri	**Keyfiyyət göstəriciləri**	**Yong-qing C.[8]**	**Malik A., Sikka G[6].**	**Jana B., Giri D[9].,**	**Təklif olunan alqoritmlər**	
					IV alqo-ritm [7]	**V alqo-ritm [7]**
Lena	HC (bit) PSNR (dB)	226085 33,27	177777 31,67	223031 38,25	464744 41,03	398562 43,23
Baboon	HC (bit) PSNR (dB)	231401 23,70	262272 22,57	273235 35,85	663791 40,43	593652 45,32
Barbara	HC (bit) PSNR (dB)	213460 31,43	185676 30,01	211321 42,34	423719 43,08	412356 48,03
Peppers	HC (bit) PSNR (dB)	227493 31,13	175669 29,78	232563 35,12	399511 39,32	386592 42,02
Orta qiymətlər	**HC (bit) PSNR**	**224609 29,88**	**200348 28,50**	**235037 37,89**	**487941 40,96**	**447791 44,65**

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

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

Cədvəldən məlum olur ki, təklif olunan alqoritmlərin digər

müqayisə edilən alqoritmlərdən daha böyük həcmdə məxfi informasiya biti yerləşdirdiyi təqdirdə konteyner təsvir ilə steqo−təsvir arasında daha yüksək oxaşarlıq 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.

PSNR qiymətlərinə əlavə olaraq, giriş təsviri və steqo – təsvirin müqayisəsini və alqoritmlərin dayanıqlılığını daha dəqiq yoxlamaq üçün histoqram steqoanalizindən istifadə edilir.

Histoqram steqoanalizi etalon təsvir və steqo−təsvirlər üzərində aparılıb. Histoqramlarda steqo–təsvirlərin effektiv yoxlanılması təmin edilib və konteyner təsvir histoqramları ilə müqayisədə ciddi dəyişiklik nəzərə çarpmayıb.

Təklif edilən alqoritmlərin dayanıqlılığının yoxlanılması üçün yuxarıda təqdim edilən steqoanalizlərdən başqa RS steqoanalizindən istifadə edilmişdir.

Hər bir təsvirdə RS göstəriciləri sıfırdan azdır və bir-birinə çox yaxındır. Bu da öz növbəsində alqoritmin yüksək dayanıqlığnı təşkil edən əsas amil hesab olunur.

Konteyner təsvirinə müxtəlif həcmdə məxfi informasiya bitləri müvafiq alqoritmlər vasitəsilə yerləşdirildikdən sonra RS steqoanalizi tətbiq edilərək dayanıqlılığı test edilib. Steqonalizin nəticələri dissertasiya işində cədvəl 4.4.2-də və cədvəl 4.4.3-də göstərilib.

Nəticələrdən məlum olur ki, informasiyanın həcminin artırılması təklif edilən alqoritmlərin dayanıqlılığına təsir etmir. Məxfi informasiya görünməz olduğuna görə açıq komunikasiya kanalı ilə ötürülə bilər. Təklif edilən alqoritmlərin hər birinin realizə müddətləri yoxlanılıb və digər alqoritmlər ilə müqayisədə daha qısa müddətdə realizə olunması təsdiq 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 [1, 2, 7, 8, 11, 13]. Aparılın icmalın əsasında mövzunun işlənmə

səviyyəsi və dissertasiya işində həll edilməli olan problemlər müəyyən edilib [7, 11, 13]. Son illərdə təsvir steqanoqrafiyası sahəsində aparılan tədqiqatlar içərisindən yüksək göstəricilərə malik və dissertasiya mövzusuna oxşar alqoritmlər nümunə kimi seçilərək geniş tədqiq edilib [4, 7].

- Təsvirin vizual keyfiyyəti prioritetli, steqo−hücumlara qarşı yüksək dayanıqlılığa malik, böyük həcmdə məxfi informasiya gizlədilməsini təmin edən steqanoqrafik alqoritm işlənilib [8, 9].
- Konteyner təsvirin, heç bir pozuntu baş vermədən,yenidən bərpa olunmasını təmin edən, interpolyasiya əsaslı steqanoqrafik alqoritm işlənilib [10].
- Yüksək göstəricilərə malik üç girişli kvorum funksiyasına əsaslanan steqanoqrafik alqoritm işlənilib [3,12]. Alqoritmin yüksək dayanıqlılığını təmin etmək üçün AES şifrləmə standartı tətbiq edilib [3].
- Rəngli RGB rəng sxemində olan təsvirlərdə SIFT alqoritmindən istifadə etməklə açar nöqtə piksellərində məxfi informasiyanın gizlədilməsi üçün iki yeni effektiv alqoritm təklif edilib [6, 11].

DİSSERTASİYA MATERİALLARI ÜZRƏ AŞAĞIDAKI ELMİ ƏSƏRLƏR DƏRC EDİLMİŞDİR:

1. Verdiyev, S.Q., Nağıyeva, A.F. Kompüter Steqanoqrafiyası və onun əsas prinsipləri // **Proqram mühəndisliyinin aktual elmi-praktiki problemləri üzrə I respublika konfransı**, - Bakı: İnformasiya Texnologiyaları, – 17 may 2017, – s. 79-81.

2. Вердиев, С.Г., Нагиева, А.Ф., Гусейнов З.Н. Симметричное (одноключевое) шифрование данных при защите информации в компьютерных сетях // **VII Международная научная конференция** Технические науки в России и за рубежом, – Москва: Издательский дом Буки-Веди, – 20–23 ноября, – 2017, – с. 5-7.

3. Вердиев, С.Г., Нагиева, А.Ф. О возможностях использования стандарта AES в Корпоративных сетях для защиты информации // Самара: **Инфокоммуникационные технологии**, – 2017. № 4.– с. 366-370.

4. Verdiyev, S.Q., Nağıyeva, A.F. İnformasiyanın steqanoqrafik gizlədilməsi proseduralarının eksperimental analizi // **İnformasiya təhlükəsizliyinin aktual problemləri III respublika elmi - praktik seminarının əsərləri**, – Bakı: İnformasiya Texnologiyaları,– 8 dekabr, – 2017, – s. 51-56.
5. Алмадатова, А.Ф., Вердиев, С.Г., Нагиева, А.Ф. Защита информации криптографическим методом разделения секрета // **VII Международная научно-техническая и научно-методическая конференция** Актуальные проблемы инфотелекоммуникаций в науке и образовании, – Санкт-Петербург: – 28 февраля-1 марта, – 2018, – с. 29-33.
6. 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. 53-58.
7. Verdiyev, S.Q., Nağıyeva, A. F., 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.
8. Verdiyev, S.G., Naghiyeva, A.F. A brief overview of data hiding methods in digital images // – Самара: **Инфокоммуникационные технологии**, – 2020, vol. 18, No. 4, – с. 427-437.
9. Naghiyeva, A.F., Akbarzadeh, K., Verdiyev, S.G. New steganography method of reversible data hiding with priority to visual quality of image // **IEEE II International Conferance on Advances in computing, communication, embedding and secure systems,** – India: – 2-4 september, – 2021, – p. 329-333. (Scopus)
10. Нагиева, А.Ф., Вердиев, С.Г. Реверсивный стеганографический метод сокрытия информации основанный на интерполяции изображений // – Москва: **Компьютерная оптика**, – 2022. Том 46, № 3,– с. 465-472. (Scopus)
11. Verdiyev, S.G., Naghiyeva, A.F., Ajay, K. Experimental study of a novel technique of data hiding with high PSNR // **IEEE III International Conferance on Advances in Computing Communication, Embedding and Secure Systems,** – India: – 18-20

may, – 2023, – p. 77-80. (Scopus)
12. Nağıyeva, A.F. Məxfi informasiyanın ötürülməsində informasiya gizlədilmə metodu // – Bakı: **Elmi əsərlər**, Azərbaycan Texniki Universiteti, - 2023. № 2,– s. 60-66.
13. Nağıyeva, A.F., İnformasiya təhlükəsizliyində steqanoqrafik metodlar // **Elmi xəbərlər məcmuəsi**, Azərbaycan Texnologiya Universiteti, – 2023. № 4, – s. 98-104.

Həmmüəliflərlə dərc olunmuş işlərdə iddiaçının şəxsi rolu

[1] – Kompüter steqanoqrafiyası və steqosistemlərdə informasiyanın gizli ötürülmə kanallarının formalaşdırılması metodlarının və vasitələrinin tədbiqi məsələləri araşdırılıb və onların tətbiqi problemləri müəyyən edilib, üstünlükləri və çatışmazlıqları göstərilib;
[2] – Açıq rabitə kanallarında məxfi informasiyanın ötürülməsi zamanı simmetrik şifrələmə yolu ilə mühafizəsi üsulları və vasitələri, tətbiqi problemləri müzakirə olunub və nəticəsi verilib. Onların üstünlükləri və çatışmazlıqlarının müqayisəli təhlili verilib;
[3] – Şifrələmə prosesinin dövlət strukturlarının hər hansı birində yerinə yetirilən iterasiya ardıcıllığı verilib. Eyni zamanda poçt rabitəsində istifadə olunan sənədin açıq mətnindən və qabaqcıl şifrələmə standartından istifadə etməklə tərtib edilmiş müvafiq kriptoqramın şifrələnmə nümunəsi verilmişdir;
[4] **–** Mövcud steqanoqrafik üsulların icmalı və eksperimental analizi yerinə yetirilib. İcmala aid hər bir üsulun ayrı ayrılıqda üstünlükləri və çatışmazlıqları təhlil edilib. Matlab mühitində informasiyanın gizlədilməsi prosedurunun metodikası verilib;
[5] **–** Məxfi informasiyaların müxtəlif multimedia fayllarının içərisində gizlədilərək ötürülməsi metodları verilib;
[6] – Təsvirlərin konteyner kimi istifadəsinin effektivliyini artırmaq məqsədi ilə emalı üsullarından biri olan seqmentləşdirilmənin istifadəsi təqdim olunub. Konkret olaraq suayırıcı (watershed) metodunun xüsusiyyətləri və matlabda işləmə metodikası verilib. Nümunə kimi rəngli, rəqəmsal təsvirin qradiyent metodu ilə seqmentləşdiriməsi istifadə edilib. Seqmentləşmə metodunun rəngli təsvirlərin emalı zamanı istifadə edilməsi müəyyən edilib;
[7] – Rəqəmsal konteyner təsvirlərin açıq şəbəkələrdə dövriyəsi

zamanı qorunması üçün steqanoqrafiya və onun əksi olan steqoanaliz üsullarının icmalı aparılaraq təhlil edilmiş və konkret misalın həlli verilib;
[8] – Son illərin tədqiqatı əsasında steqanoqrafik metodların təsnifatı verilib. Təsvir steqanoqrafiyasının ən geniş yayılmış və istifadə olunan üsulları onların üstünlükləri və çatışmazlıqları araşdırılıb. Məlumatların gizlədilməsinin müxtəlif üsullarının müzakirələri aparılıb və müzakirələrin nəticəsi verilib. İlkin təsvir və steqo təsvir arasında statistik fərqlərin hesablanması üçün steqoanalitik üsullar araşdırılıb və nəticəsi verilib;
[9] – Steqanoqrafiya elm sahəsində LSB metodundan istifadə etməklə daha yüksək göstəricilərə malik məxfi informasiya gizlətmə alqoritmi işlənilib;
[10] – Təsvirin interpolyasiyası əsasında məlumatın gizlədilməsi üçün yeni stenoqrafiya metodunun işlənib hazırlanması problemi qoyulmuş və həll edilmişdir. Dayanıqlı və təsvirin vizual keyfiyyətini təmin edən daha yüksək həcmli məxfi informasiya gizlədilmə metodu təklif edilib;
[11] – Məxfi informasiyanın mühafizəsi problemini həll etmək üçün işlənib hazırlanmış müxtəlif steqanoqrafik metodların dayanıqlığının eksperimental tədqiqi verilib. Steqo analitik hücumlar üçün alqoritmin etibarlığı RS steqanaliz üsulu ilə tədqiq edilmişdir. Alqoritmin hesablama mürəkkəbliyi araşdırılıb və nəticəsi verilib.

Dissertasiyanın müdafiəsi _____**2025**-ci il tarixdə saat_____Azərbaycan Elm və Təhsil Nazirliyinin İnformasiya Texnologiyaları İnstitutunun nəzdində fəaliyyət göstərən ED1.35 Dissertasiya şurasının iclasında keçiriləcək.

Ünvan:Az 1141, Bakı şəhəri, B.Vahabzadə küçəsi,9a

Dissertasiya ilə Azərbaycan Elm və Təhsil Nazirliyinin İnformasiya Texnologiyaları İnstitutunun kitabxanasında tanış olmaq mümkündür.

Dissertasiya və avtoreferatın elektron versiyaları Azərbaycan Elm və Təhsil Nazirliyinin İnformasiya Texnologiyaları İnstitutunun rəsmi internet saytında yerləşdirilmişdir.

Avtoreferat_____**2025**-ci il tarixində zəruri ünvanlara göndərilmişdir

Çapa imzalanıb:
Kağızın formatı:
Həcm:
Tiraj: