İnformasiyanın steqanoqrafik gizlədilməsi metodlarının eksperimental analizi

Ababil Nağıyeva[1], Sakit Verdiyev[2]

[1,2]Azərbaycan Texnologiya Universiteti, Gəncə, Azərbaycan

[1]info_tel@inbox.ru , [2]nagiyevaababil@gmail.com

***Xülasə*— Steqanoqrafiya gizli kommunikasiya üsullarından biri olaraq məxfi ismarıcların gizlədilərək ötürülməsini təmin edir və bu zaman gizlədilmiş ismarıcların mövcudluğu nəzərə çarpmır. Gizlədilən ismarıc qismində mətn, təsvir, audio, video və s. ola bilər. İnernet şəbəkəsində kompüter istifadəçilərinin və bununla əlaqədar ötürülən verilənlərin sayının günü gündən artması steqanoqrafiyanın əhəmiyyətini dəfələrlə artırır. Steqanoqrafiyanının potensialının hələ tükənməməsi məlumatın yeni gizlədilmə metodlarının işlənilməsinə zəmin yaradır. Burada biz məlumatın müxtəlif steqanoqrafik üsulların icmalını verərək hər birinin üstünlüklərini və çatışmazlıqlarını oxucuya çatdırmağa çalışdıq. Matlab mühitində informasiyanın gizlədilməsi prosedurunun metodikası verilib.**

***Açar sözlər*— rəqəmsal steqanoqrafiya; gizli ötürmə; steqosistem; piksel; LSB; matlab; histoqram**

I. GİRİŞ

Müasir rəqəmsal dünyada, İnternetə əsaslanan texnologiyalar özünə yeni tətbiq sahələri taparkən verilənlərin mübadiləsi zamanı informasiya təhlükəsizliyi məsələləri ön plana çıxaraq yeni üsulların işlənməsini tələb edir. Bu məqsədə nail olmaq üçün iki istiqamət var:

- Kriptoqrafiya: Göndərən şifrləmə açarından istifadə edərək göndərilən mətni şifrləyir və həmin mətn ümumi istifadəyə açıq kanaldan ötürülərək qəbul edən, şəxs tərəfindən xüsusi deşifrləmə alqoritmi ilə mətni deşifrə edir. Bir şərtlə ki, o deşifrləmə açarına malik olsun.

Steqanoqrafiya:“Setqanoqrafiya” sözünün yunan dilindən tərcüməsi “məxfi yazı” (steganos – sirr, məxfi görülən iş, graphy – yazı) mənasını verir [1]. Burada məxfi ismarıc digərinin daxilində yerləşdirilir. İnternet vasitəsilə əlaqələndirilən, potensial kompüter istifadəçilərinin sayının günü gündən artması steqanoqrafiyanın tədbiqinin əhəmiyyətini artırır. Steqanoqrafiya yeni müasir texnologiyalardan istifadə etməklə ötürülən məxfi verilənləri müvafiq daşıyıcının içində gizlədilərək ötürülməsini təmin edən elm sahəsidir. Daşıyıcı kimi adətən təsvir, audio, video və yaxud mətn faylı ola bilər. Steqnoqrafiya kriptoqrafiyadan fərqlidir.

Steqanoqrafiya elmi də informasiya təhlükəsizliyinin təmin edilməsi problemi ilə məşğul olur. Steqanoqrafiyanın vəzifəsi informasiyanın yığılması, saxlanması, emal olunması və ötürülməsi faktını gizlətməkdən ibarətdir. Başqa sözlə, steqanoqrafik üsulların əsas məqsədi qorunan (o cümlədən məxfi) məlumatın varlığının rəqibdən gizli saxlanmasıdır.

Məlum olduğu kimi əksər ölkələrdə kriptoqrafik üsul və vasitələrin reallaşdırılmasına, istifadəsinə və tətbiqinə qanunvericiliklə müəyyən ciddi məhdudiyyətlər, qadağalar qoyulur. Adətən, istifadə olunan şifrləmə sistemlərinin açarlarının dövlətə verilib - verilməməsi, aparat və ya proqram vasitələri şəkilində reallaşdırılmasından asılı olmayaraq kripto-qrafik sistemlərin məcburi qeydiyyatı və lisenziya-laşdırılması kimi tələblər qoyulur.

Kriptoqrafiyadan fərqli olaraq müasir dövrdə steqanoqrafiyanın istifadəsinə belə məhdudiyyətlər, qadağalar qoyulmur və praktikada informasiyanın gizlədilməsi üçün effektiv vasitə kimi istfadə olunmaqda davam edir.

Qeyd edilməlidir ki, steqanoqrafiya kriptoqrafiyanı əvəz etmir, onu tamamlayır və məxfi informasiyanın bədniyyətli şəxslərdən daha ciddi qorunmasını təmin edir.

Aydındır ki, hər hansı məlumatın varlığını daha böyük həcmli informasiya massivində gizlətmək daha asandır. Müasir dövrdə steqanoqrafiya məxfi məlumatın tamamilə başqa məzmunlu daha böyük həcmli informasiyanın içində gizlədilməsi prinsipinə əsaslanır [2].

II. RƏQƏMSAL STEQANOQRAFİYA

Kompüter texnologiyaları steqanoqrafiyanın inkişafına və təkminlləşməsinə yeni təkan verdi və informasiya təhlükəsizliyi sahəsində yeni bir istiqamətin – kompüter steqanoqrafiyasının yaranmasına səbəb oldu.

Bundan başqa rəqəm steqanoqrafiyası anlayışı vardır. Rəqəm steqanoqrafiyası - klassik steqanoqrafiyanın rəqəmli obyektlərin müəyyən hissəsində məxfi informasiyanın gizlədilməsi və ya yeridilməsi prinsiplərinə əsaslanan yeni istiqamətidir. Lakin bir qayda olaraq, qeyd olunan rəqəmli obyektlər multimedia (şəkil, video, audio, 3D – obyektlərin teksturası və s.) obyektləri olduğundan və edilən təhriflərin insanın hissiyyat oraqnlarının orta statistik həddini aşmadığından bu obyektlərin gözə çarpan dəyişikliyinə gətirib çıxarmır.

Rəqəm steqanoqrafiyasının tətbiq sahələrindən biri də müasir dövrdə daha çox tələb olunan yeni istiqamətin müəlliflik hüququnun qorunması sistemlərinin əsasını təşkil edən rəqəmli su nişan-larının (ing. watermarking) rəqəmli obyektlərə qoyulması texnologiyasının istifadəsi ilə bağlıdır. Bu istiqamətdə reallaşdırılan üsullar konteynerə müxtəlif

DOI: 10.25045/NCInfoSec.2017.10

çevrilmələrə (hücumlara) davamlı gizli nişanların (markerlərin) daxil edilməsinə əsaslanır.

Məsələn, Adobe Photoshop redaktoruna əlavə işlənilib hazırlanmış Digimark proqram bloku bu redaktor vasitəsilə hazırlanan təsvirin özünə müəllif haqqında məlumatı daxil etməyə imkan verir. Təəssüf ki, belə nişan dayanıqlı deyil. Belə ki, Fabien Petitkolas adlı alim tərəfindən işlənib hazırlanmış Stirmark proqramı belə sistemlərə müvəffəqiyyətlə hücum edir və steqoqoyuluşu sındırır [3].

Rəqəm steqanoqrafiyası üsullarına bir nümunə kimi ən kiçik qiyməti olan bit (Least Significant Bit, LSB) üsulunu göstərmək olar – konteynerdə (şəkil, səs və ya videoyazı) daha az əhəmiyyətə malik olan ən kiçik mövqeli (sağdan birinci) bitlərin gizlədilən məlumatın bitləri ilə əvəz edilməsi prinsipi əsasında qurulmuşdur. Bu zaman boş və doldurulmuş konteynerlər arasındakı fərq insanın qavrama orqanları tərəfindən hiss ediləcək dərəcəni aşmamalıdır. LSB üsulunun istifadəsi haqqında geniş məlumatlar vardır.

LSB hücumu bütün növ hücumlara qarşı dayanıqlı deyil və yalnız məlumatların ötürülməsi kanalında səs - küy olduqda istifadə oluna bilər.

Ümumiyyətlə gizli informasiyanın rəqəmli obyektlərdə yerləşdirilməsi alqoritimlərini bir neçə alt qrupa bölmək olar:

- Rəqəmli nişanlarla işləyən üsullar (məsələn, LSB üsulu);
- Gizli informasiyanın “lehimlənməsi”- gizlədilən şəkil (səs, təsvir, mətn) orjinal şəklin (səsin, təsvirin, mətnin) üzərinə qoyulur (məsələn rəqəmli su nişanlarının qoyulması);
- Fayl formatının xüsusiyyətlərinin istifadəsi- bu zaman gizlədilən informasiya metaverilənlərə və ya faylın digər müxtəlif istifadə olunmayan ehtiyat sahələrinə yazılır.

III. LSB ÜSULU

LSB üsulunun tətbiqi ilə bağlı olaraq bir neçə tədqiqata nəzər yetirək.

Şamirin gizli paylaşma sxemi şəbəkədə gizli təsvirlərin ötürülməsində istifadə edilir ki, buna gizli şəkil mübadiləsi metodu deyə bilərik. Gizli şəkil mübadiləsi metodu səhvlərə və qrup təhlükəsizlik siyasətinə tolerantlıq təmin edir. Steqanoqarfiyada tətbiq olunan metodların əksəriyyəti LSB metodunu təklif edir [4].

İlk dəfə olaraq 2002-ci ildə Thien və Lin gizli təsvirlərin ötürülməsi zamanı steqanoqrafiyadan və ya kriptoqrafiyadan istifadə edərək yaranan problemləri vurğuladı [5]. Hər iki üsulla yaradılan stego təsvirlər və ya şifrələnmiş təsvirlər tək bir mühitdə saxlanılırdı. Şəbəkə ilə ötürülməsi zamanı təhrif ediləcəyi təqdirdə, məxfi məlumatları bərpa etmək şansı yoxdur. Thien və Lin gizli təsvirlərin yaradılmasında LSB metodundan istifadə etmişdirlər.

Selda Berkerin apardığı tədqiqatda LSB üsulu ilə bağlı aşağıdakı fikirləri irəli sürülmüşdür.

LSB üsulunun çox sadə bir üsul olmasına baxmayaraq diqqətsiz tətbiq olunarsa, məlumatların itirilməsi baş verə bilər. Bu üsulda, gizli tutulacaq məlumatların hər biti rəqəmsal görüntü verilənlərinin bir baytının son bitinə yazılır. Məsələn, "A" -map ilə 24 piksellik bir görüntü faylını üç pikselin ilk səkkiz baytına necə yerləşdirəcəyimizi göstərək:

Piksellər: (00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

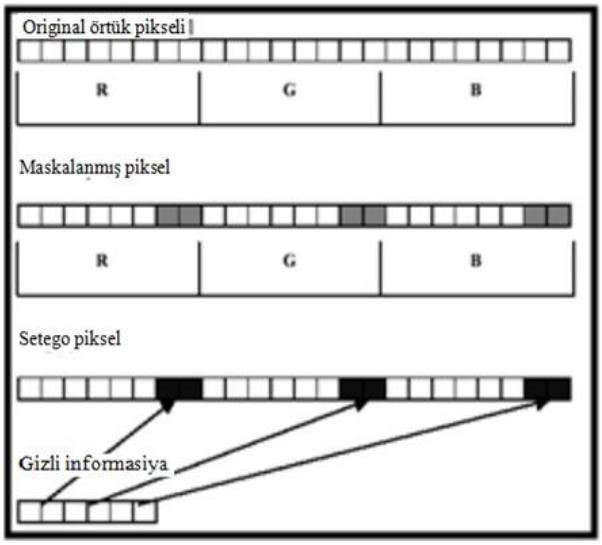
A: 01000001

Nəticə: (0010011**0** 11101001 11001000)

(0010011**0** 11001000 1110100**0**)

(11001000 00100111 11101001)

Altından xətt çəkilmiş üç bit dəyişdirilmişdir. Yəni bitlərin əlavə olunduğu səkkiz baytın yalnız üçündə dəyişiklik meydana gəlmişdir. LSB insertion üsulunda ümumi olaraq son bitlərə əlavələr olunduğunda içərisinə verilənlər yerləşdirilmiş rəqəmsal şəkildəki dəyişmə sadəcə 50%–dir. Bu texnikanın başqa bir versiyası son biti dəyişmək əvəzinə hər baytın son 2 və ya daha çox bitini əvəz etməkdir. Bu, örtülü obyektdə gizl məlumatların potensialını artıracaq, lakin əhatə olunan obyektin pisləşməsi daha çox olacaq və insan gözünün dəyişməni qəbul edəcəyi ehtimalı artır. Lakin rəng spektri 24 bit rəngli şəkillərdə daha geniş olduğundan, dəyişikliklər hələdə insan gözünün qəbul edəcəyi ölçülərə çata bilməz (şəkil 1, şəkil 2.).



Şəkil 1.Son iki yükləmələrin yerləşdirilməsi

Orginal təsvir

	LSB 1 bit
	LSB 2 bit
	LSB rəng cycle

Şəkil 2. LSB üsulu ilə bir sıra bitlərin yerləşdirilməsi

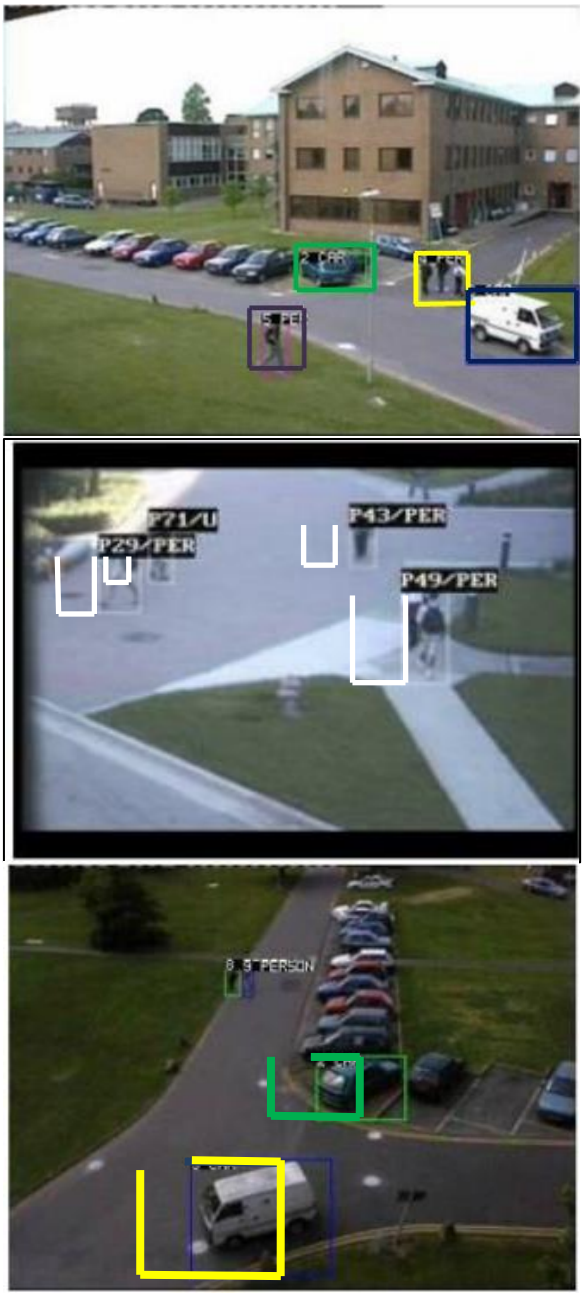
Gördüyünüz kimi original rəsm və stego rəsmləri arasındakı fərqlər insan gözü ilə seçilmir. Bununla yanaşı bazarda bunun üçün bir çox proqram var. Məsələn, bazarda Java dilində yazılmış StegCure adlı proqram bitləri hex redaktorunu istifadə edərək hexa decimal olaraq təqdim edir və dəyişiklikləri aşkar edə bilər [6].

IV. LSB ÜSULUNUN MATLABDA İSTİFADƏSİ

Selda Berkerin məqaləsində LSB üsulu ilə yanaşı onun modifikasiyası olan digər üsuldanda bəhs edilir [5]. Hazırda bir çox ölkələrdə LSB üsulunun reallaşdırılması üçün müxtəlif proqramlaşdırma dillərindən istifadə olunur. Məqalədə adı keçən proqramlaşdırma dilindən başqa matlab sistemindən də istifadə edərək LSB üsulunu reallaşdıra bilərik [7].

Steqanoqrafik metodların matlab sistemində reallaşdırılması üçün ilkin olaraq müəyyən addımları bilmək lazımdır. Əgər biz matlab sistemində LSB üsulunu tətbiq etmək istəsək ilkin olaraq matlabda təsvirlər üzərində aparıla biləcək bəzi zəruri əməliyyatlara nəzər salmalıyıq.

Təsvirlər üzərində LSB metodunu tətbiq etmək üçün mütəxəssislər təsvirdə olan piksellərə nəzər yetirirlər. Məqsəd sayı ən çox olan rəngin piksellərini tapmaqdır. Məlumdur ki, təsvirdə hansı rəngin pikseli daha çox olarsa biz həmin çox olan piksellərdən birini dəyişdirərkən, edilən dəyişiklik insan gözü ilə seçilməməlidir.Təsvirlərdə eyni nöqtələrin müəyyən edilməsi əməliyyatına təsbit etmə deyilir. Şəkil 3-də təsbit etmə əməliyyatı aparılmışdır və aparılan əməliyyatın nəticəsi olaraq, oxşar mövqelər kvadrat ilə göstərilmişdir [8].



Şəkil 3. Təsbit etmə

Aydındır ki, təsvirlər RGB rəng sxemi əsasında olurlar. Lakin təsvirlərin RGB rəng sxemi bizim işimizi müəyyən dərəcədə çətinləşdirə bilər. Bu problemi aradan qaldırmaq üçün təsvirlər bir çox halda boz və ya ağ qara rəngə çevrilərək üzərində əməliyyat aparılır (şəkil 4) .

Matlabda təsvirin alınması və boz rəngə çevrilməsi aşağıdakı kimi olacaq:

```
>>I=imread ('bənövşə.tif”);
>>I2 = rgb2gray(I);
```

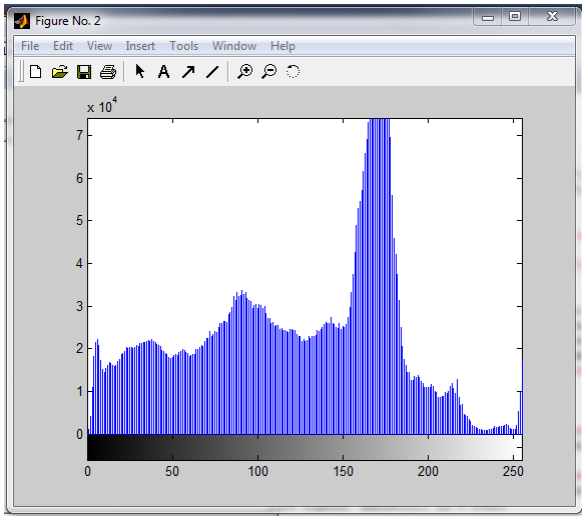
```
>> figure; imshow(I2);
```

Şəkil 4. Təsvirin boz rəngə çevrilməsi

Təsvir boz və ya ağ qara hala gətirildikdən sonra təsvirin piksellərində hansı rəngin daha çox olması müəyyən edilir və təsvirin piksellərinin rəng çalarını əks etdirən histoqram qurulur (şəkil 5) [9].

Matlabda histoqramın qurulması:

```
>> İ=imread("bənövşə.tif');
>>figure; imhist(I); I2 = I+60;
>>figure; imhist(I2); I3 = I *0.5;
>>figure; imhist(I3);
```



Şəkil 5. Təsvirin histoqramı

Qurulan histoqram əsasında hansı rəng çaları daha çoxdursa həmin piksel üzərində əməliyyatlar aparılır.

Növbəti mərhələdə isə hisqtoqrama əsasən müəyyən etdiyimiz eyni piksellər üzərində LSB metodunu tətbiq etmək üçün xüsusi alqoritimlər yaradılır. Alqoritimlərin proqramlarının tərtibində C, C++, C#, Java dillərindən istifadə olunur. Matlab sistemindədə biz həmin proqramları tərtib edə bilərik. Digər dillər ilə müqayisədə matlab sistemində LSB üsulunun alqoritminin qurulması daha sadə və əlverişlidir [10].

NƏTİCƏ

Məqalədə informasiya təhlükəsizliyində geniş istifadə edilən LSB steqnoqrafik üsulunun tətbiq etmə sahələrinin icmalı verilib. Göstərilib ki, istifadə edilən hər bir tətbiq sahəsi özünə məxsus gizlədilmə proseduraları ilə fərqlənərək müəyyən üstünlüklərlə və çatışmazlıqlarla səciyyələnir. Deməli hər bir metodikanın öz spesfik xüsusiyyətlərinə görə hər bir hal üçün fərdi qaydada istifadə olunmalıdır və hər hansı halda çox faydalı ola bilən metodika digər halda yararsız ola bilər.

Beləliklə demək olar ki, steqanoqrafik üsulların inkişaf etdirilməsi potensialı hələ tükənməyib və yeni üsulların işlənilməsinə ehtiyac vardır. Yəni informasiyanın gizlədilmə proseduralarının metodikalarının işlənilməsi üçün Matlab mühitində alqoritimlərin qurulmasının məqsədə uyğun olması göstərilərək tədqiqat metodologiyasının nümunəsi verilib.

ƏDƏBİYYAT

[1] P. C. Mandal, B.P. Poddar, “Modern Steganographic technique: A survey”, International Journal of Computer Science & Engineering Technology (IJCSET), 2012, vol. 3, no. 9, pp. 444-448.
[2] S.Q. Verdiyev, A. F. Nağıyeva, “Kompüter steqanoqrafiyası və onun əsas prinsipləri”, “Proqram mühəndisliyinin aktual elmi-praktiki problemləri” I respublika konfransı, Bakı, 17 may 2017-ci il.
[3] V.Ə. Qasımov, İnformasiya təhlükəsizliy: kompüter cinayətkarlığı və kiberterrorçuluq, Elm, 2007, 192 s.
[4] G.Ulutaş, M.Ulutaş., V.V.Nabiyev, “A new casccaded secret image sharing scheme,” 20th IEEE Signal Processing and Communications Applications Conference (SIU), pp. 1-4, 2012.
[5] S. Berker, “Steganografi ve LSB”, http://bilgisayarkavramlari. sadievren seker.com /2009 /06/05/steganografi-ve-lsb/
[6] A. Ertürk, “Matlab ve imge işleme”, Istanbul, Ders notları, 2009, 162 s.
[7] J. Lenti, “Steganographic methods,” Periodica Polytechnica Electrical Engineering, vol. 44, no. 3–4, pp. 249–258, 2000.
[8] R. Yadav, and R. Saini, “Cyclic combination method for digital image steganography with uniform distribution of message“, Advanced Computing: An International Journal (ACIJ), vol. 2, no. 6, pp. 29-43, 2011.
[9] R. Radhakrishnan, K. Shanmugasundaram and N. Memon, “Data masking: a secure- covert channel paradigm”, IEEE Workshop on Multimedia Signal Processing, pp. 339-342, 2002.
[10] V. Singhal, D. Yadav, D. Bandil, “Steganography and steganalysis: a review”, International Journal of Electronics and Computer Science Engineering, vol. 1, no. 2, pp. 399-404, 2012.

EXPERIMENTAL ANALYSIS OF STEGANOGRAPHY METHODS OF INFORMATION HIDING

Ababil Nagıyeva[1], Sakit Verdiyev[2]
Azerbaijan Technology University
info_tel@inbox.ru , nagiyevaababil@gmail.com

Abstract – Concealed message as usually may be text, image, audio, video and other. Nowadays amount of computer users and transmitted dates accordingly on Internet are increasing day by day. In conjunction with them increase a role of steganography. A potential of steganography as a direction of science methodology isn’t exhausted. Therefore it needs to develop new methods and procedures for information security. Here we made attempt to give

readers overview of different steganography methods and described both advantages and disadvantages for each modes. Methods of information hiding procedures on Matlab is given.

Keywords – digital steganography, concealed transmission, stegosystem, pixel, LSB, Matlab, histogram.