Steqoanaliz üsullarının icmalı

Sakit Verdiyev[1], Ababil Nağıyeva[2], Rəxşəndə Hüseynova[3], Zakir Hüseynov[4]
[1,2,4]Azərbaycan Texnologiya Universiteti, Gəncə, Azərbaycan
[3]Azərbaycan Dövlət Aqrar Universiteti, Gəncə, Azərbaycan
[1]*info_tel@inbox.ru,* [2]*nagiyevaababil@gmail.com,* [3] *huseynova.raxshanda@mail.ru*

***Xülasə*— Açıq qlobal kompüter şəbəkələrində müxtəlif media formatlarında istifadə edilən verilənlərin dövriy¬yəsi exponensial qanunla artdığı üçün informasiya müha¬fizəsi məsələləri daha çox aktuallaşır və yeni üsullarının işlənilməsi zərurəti yaranır. Məqalədə rəqəmli təsvirlərin şəbəkələrdə dövriyyəsi zamanı qorunması üçün steqanoqrafiya və onun əksi olan steqoanaliz üsulları təhlil edilmiş və konkret misalın həlli verilmişdir.**

Açar sözlər— steqanoqrafiya, steqoanaliz, steqoalqoritm, steqotəsvir, konteyner, xi kvadratı

I. GİRİŞ

Rəqəmsal məlumatların internetdə və digər rabitə kanallarında elektron dövriyyəsinin sürətlə artması verilənlərin mühafizəsinə həsr olunan steqanoqrafiya metodlarının işlənilməsinə təkan verir. Bununla yanaşı əks proses – ötürülən məxfi məlumatlara icazəsiz daxil olmalara, onların təhlilinə, modifikasiyasına həsr olunan hücum üsullarından olan steqoanaliz də inkişaf edir.

Steqanoqrafiya sözü yunan dilindən tərcümədə “stegano” örtülmüş, “graphia” yazı mənasını verir.

Steqanoqrafiya, məxfi məlumatları istənilən media fayllarında gizlətmə üsuludur ki, gödərəndən və alıcı-dan başqa heç kim gizli məlumatların mövcudluğunu bilməsin.

Steqanoqrafik üsulla örtük təsvirində konteyner təsvirə gizlədilən informasiyanı aşkarlamaq üçün steqoanaliz üsullarından istifadə olunur.

Steqosistemin riyazi modeli aşağıdakı kimi təqdim edilə bilər:

$$E: C \times M \times K \to S \tag{1}$$

$$D: S \times K \to M \tag{2}$$

$$D(E(c,k,m),k) = m, \quad \forall\, c \in C, \quad \forall\, k \in K, \quad \forall\, m \in M \tag{3}$$

Burada C – konteyner, M – gizli məlumat, K – steqo açar, S – dolu konteyner, yəni steqo təsvirdir [1].

Steqanoqrafiyada istifadə olunan alqoritmləri qiymətləndirilərkən aşağıdakı üç əsas xüsusiyyət nəzərə alınır:

- Daşıyıcıdakı (konteynerdəki) pozuntu (ing.distortion);
- Konteynerin tutumu (ing. capacity);
- Dayanıqlılıq (ing. robustness).

Steqanoqrafik alqoritmlərin qiymətləndirilməsi zamanı örtük obyektində dəyişikliyin qiymətləndirilməsi çox vacibdir. Konteynerin dəyişməsini və ya təsvirdəki pozulma dərəcəsini təyin etmək üçün müxtəlif ölçmə metodları var. Bu metodlardan ən çox tanınanlar MSE (mean squared error), PSNR (peak signal to noise ratio), RMSE (root mean squared error)-dir [2].

MSE orta kvadratik xətanı hesablayır. MSE adətən σ^2 kimi göstərilir. RMSE isə MSE-nın kvadrat köküdür.

$$\sigma^2 = \frac{1}{M \times N} \sum_{i=1}^{M \times N} \left(P(i,j) - S(i,j)\right)^2 \tag{4}$$

Burada M və N sətir və sütunların sayı, $P(i,j)$ konteyner təsvir, $S(i,j)$ və isə stego təsvirdir.

Bəzən MSE əvəzinə xətanın böyüklüyünün original piksel qiymətinin ən böyüyü ilə olan əlaqəsi əhəmiyyət daşıyır. Belə olan halda PSNR (ing. peak signal to noise ratio) hesablanır.

$$PSNR(dB) = 10 \log_{10} \frac{x_{peak}^2}{\sigma_d^2} \tag{5}$$

Burada χ^2 təsvir pikselinin mümkün olan maksimum qiymətidir.

Ardıcıl LSB üsullarında təsvirin həcmi onun ölçüsü ilə sıx bağlıdır. Həcm baxımından BMP (Bitmap) formatları daha əlverişli hesab olunur, çünki daha çox informasiya yerləşdirmək olur. Belə ki, JPEG (Joint Photographic Experts Group) formatında olan təsvirlərdə 8x8 bloklara sadəcə 4 və ya 5 bit gizlədilə bilir. Buna görə də gizlədiləcək informasiya miqdarı kifayyət qədər azdır [3]..

II. STEQOANALİZ

Steqanoqrafik alqoritmlərin dayanıqlılığını ölçmək üçün steqoanaliz metodlarından istifadə olunur. Hər bir müxtəlif steqoanaliz metodlarıüçün ayrı ayrı steqo-analiz metodları işlənilmişdir. Bir alqoritm üçün istifadə olunan steqoanaliz metodu ola bilər ki, digər alqoritm üçün əlverişsiz hesab olunsun.

Steqoanaliz hər hansı bir konteyner içərisində məlumat olub olmadığını aşkar etmək və əgər məlumat varsa o məlumatı əldə etmək məqsədilə istifadə olunan steqoalqoritmə hücüm metodudur.

DOI: 10.25045/NCInfoSec.2019.50

Adətən steqoanaltikin istifadə olunan bütün steqanoqrafik üsullardan xəbərdar olduğu hesab olunur (Kerchofs prinsipi). Əgər steqoanaltik istifadə olunan steqanoqrafik üsulllardan xəbərsizdirsə onda onun işi çətinləşir [4].

Steqoanaltikin hücüm edə bilməsi üçün bəzi verilən¬lərə sahib olmalıdır. Sahib olduğu verilənlərə görə o, hücüm modellərindən birini seçərək işini davam edir. Hücum modellərindən ən geniş yayılanları aşağıdakılardır:

- Sadəcə steqo hücumu: Analiz üçün sadəcə steqo-obyekt bilinir;
- Bilinən konteyner hücumu: konteynerin içərisinə məlumat yerləşdirilmədən əvvəlki halı bilinir;
- Bilinən gizli məlumat: steqoanaltik gizlədilən məlumatdan əvvəlcədən xəbədar olur;
- Bilinən steqo hücumu: konteyner obyekti, steqo obyekt və steqanoqrafik açarlar bilinir.

Hər bir steqanoqrafik metod üçün ayrı-ayrı steqoanaliz metodlarına ehtiyac vardır. Yəni hər bir steqoalqoritm metodu üçün ayrı bir steqoanaliz metodu işlənilmişdir və hər bir alqoritmin analizi yalnız həmin alqoritmə uyğun hazırlanmış analiz metdoun¬dan istifadə zamanı düzgün nəticə verir.

Əgər kiçik həcmdəki məlumat böyük həcmli konteyner içərisinə yerləşdirilərsə bu zaman konteynerdə məlumat olması nəzərə çarpmayacaqdır.

Steqoanaliz metodlar içərisində məlumatın nəzərə çarpmasına əsaslanan bir çox üsüllar vardır. Onlara aşağıdakıları misal göstərə bilərik:

- Statistik steqoanalizi
- Histoqram analizi
- RS (Regular and Singular analysis) steqoanalizi
- Bitlər müstəvisi (Bit plane) analizi
- χ^2 testi və s. [5].

III. STEQOANALİZ METODLARI

Steqoanaliz aparılarkən təsvirlərin xarakteristikalarından istifadə edərək qeyri adi xassələri aşkarlanırlar. Həmin xassələrin xüsusiyyətləri istənilən steqanoqrafik üsulla əlaqəlidir. Bu üsullar asanlıqla məxfi verilənin mövcudluğunu üzə çıxardır və hətta onun ölçüsünü qiymətləndirə bilir:

A. Histoqram əsaslı analiz

Bu həmçinin steqotəsvirin testləşdirilməsi üçün effektiv hesab edilir. Piksellərin paylanmasını və yaxud qeyri adi formalarını identifikasiya etmək üçün örtük və steqotəsvirin histoqramları müqayisə edilir. Bir çox hallarda PVD (pixel value difference) əsaslı steqonoqrafik üsullar histoqram analizinin müxtəlif dəyişmələri ilə qiymətləndirilir. Misal üçün piksel fərqləri histoqram analizi, Histoqram Characteristic Function-Center of Mass (HCF-Com) analizi.

B. RS steqoanaliz

Regular və singular (RS) analiz RS üsulu kimi təsadüfi LSB yerləşdirilməsi metodlarında aşkarlama etmək üçün işlənilib. Bu üsul piksellərin LSB-sində kiçik dəyişmələrdən istifadə edir. Bu dəyişmələrlə və diskriminasiya funksiyasını piksellərin regular və singular qruplara bölünməsini təmin edir. Bu qrupların tezliyi steqotəsvirin içindəki məxfi mesajın uzunluğunu müəyyən edir [6].

C. Bit plane analizi

Ümumi təsvirin hər bir bit plane-i digər qonşu bit plane ilə korellyasiya olur. Steqanoqrafik üsul tətbiq edildikdən sonra korellyasiyalar dəyişə bilər və buna görədə bit plane analizi vasitəsilə görünə bilər. Bit plane analizi çox əhəmiyyətli dərəcədə əvəz¬etməyə əsaslanan yerləşdirmə üsulları ilə dəyərləndirilə bilər [7].

D. Qeyri-struktur steqoanaliz

Qeyri-struktur steqoanalizdə aparılarkən örtük təsvirin modelindən istifadə edir və daha sonra steqo və örtük təsvir arasında baş verən pozuntular qiymətlən¬dirilərək məxfi verilənlərin mövcudluğunu aşkarlamaq üçün istifadə edilir. Ümumən Machine Learning-ə əsaslanan sinifləşdirici xüsusiyyətlər çoxluğunu elə üsulubla təqdim edir ki, örtük təsvir böyük data çoxluğu ilə steqotəsvir arasındakı xüsusiyyətlər fərqini öyrədir [8].

E. χ^2 analizi

Bu üsul qiymətlər cütlüyü PoVs (pairs of values) statistik analizinə əsaslanır və bu məxfi verilənin daxil edilməsi zamanı dəyişirilir. Bu üsul LSB əsaslı daxil edilmənin aşkarlanması üçün işlənilib. Daxil edilmə metodlarının sayı Xi kvadrat üsulu ilə aşkarlanır [9].

Hər baytın 8 bit ilə təmsil olunduğunu nəzərə alsaq, onda 256 qiymətimiz və 128 PoV cütümüz olacaqdır.

χ^2-testinin nəticəsi 1-ə bərabər olarsa bu təsvirin içərisində məlumat yerləşdirildiyini göstərir. Əgər nəticə 0 olarsa onda təsvirin içərisində məlumatın yerləşdirilmədiyini göstərir [10].

$$\chi^2 = \sum \frac{(f_0 - f_e)^2}{f_e} \quad (6)$$

Burada f_0 təsvirin müəyyən bir pikselində müşahidə olunan tezlik, f_e isə təsvirin piksellərində müəyyən olan pozulmanın tezliyidir.

Gizli mesaj steqokonteynerə mükəmməl yerləşdirildikdə insan gözü ilə ayırd edilə bilmədiyinə görə analtik hesablama üsullarından istifadə edilir. Misal üçün aşağıdakı təsvirlərə aid hesablamalara nəzər salaq .

Şəkil 1. Boş konteyner və stegotəsvir

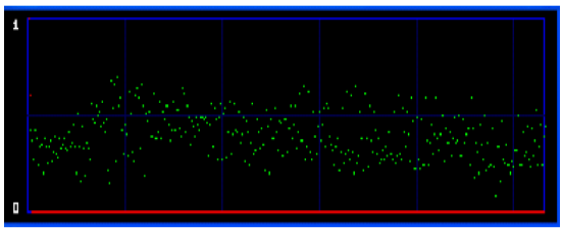
Şəkil 1 də 512x512x3 ölçülü boş konteyner, və 512x512x3 ölçülü stegotəsvir verilib. Vizual analiz zamanı heç bir fərq

nəzərə çarpmır. Ona görə də aşağıdakı qayda ilə PSNR və MSE hesablayaq. Hesablama Matlab mühitində aparılır.

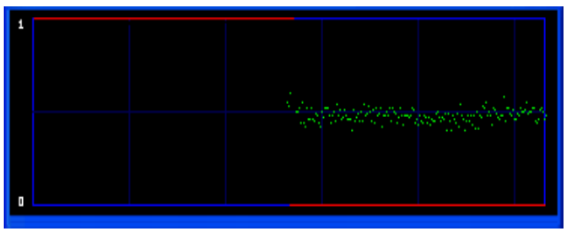
```
>> n=size(im1);
>> M=n(1);
>> N=n(2);
>> MSE=sum(sum((im1-im2).^2))/(M*N);
>> PSNR=10*log10(256*256/MSE);
>> fprintf('\nMSE:%7.2f', MSE);

MSE:    0.00
MSE:    0.00
MSE:    0.00
>> fprintf('\nPSNR: &9.7f dB', PSNR);

PSNR: &9.7f dB
```

Hesablamanın nəticəsində orta kvadratik xətanın qiyməti 0-a bərabərdir. Bu onu göstərir ki, steqoalqoritm effektivdir və təsvirin piksellərində heç bir pozuntu yoxdur, PSNR-in qiyməti isə boş və dolu konteyner arasındakı oxşarlığı əks etdirir.

χ^2hesablanaraq əldə olunan nəticələr şəkil 2 və şəkil 3-də nümayiş olunub



Şəkil 2. Boş konteynerin χ^2testinin nəticəsi



Şəkil 3. Dolu konteynerin χ^2 testinin nəticəsi.

Şəkil 2-də χ^2 -nın nəticəsi 0 alınıb. Bu təsvirin boş olduğunu göstərir. Şəkil 3-də isə χ^2-nın nəticəsi 1 alınıb və məlum olur ki, təsvirdə informasiya yerləşdirilmişdir

NƏTİCƏ

Bu məqalədə təsvir steqanoqrafiyası üsulu ilə örtük təsvirində gizlədilmiş informasiyanın aşkarlanması üçün istifadə olunan müxtəlif steqoanaliz metodları təhlil edilib. Təhlil nəticəsində məlum olub ki, hər bir üsul konkret olaraq tətbiq edilən steqanoqrafik alqoritmin xüsusiyyətlərindən asılıdır. Təsvirin daxilində məxfi məlumatın mövcudluğunu açkarlamaq üçün steqoanaliz üsulu ilə hesablama aparılaraq steqotəsvirdə məlumatın olması müəyyən edilib. Gizli məlumatın konteynerə yerləşdirilməsi zamanı steqotəs¬virdə baş verən pozuntuların miqdarını müəyyən etmək üçün PSNR üsulunun istifadə nümunəsi verilərək, boş konteynerlə dolu konteyner arasındakı fərqi MATLAB-da hesablanan konkret rəqəmlə verilib. Hesablamaların nəticəsi məxfi məlumatın konteynerə yerləşdirmə prosessinin uğurlu olduğunu təsdiq edir

İSTİNADLAR

[1] С.М. Сейеди, В.С. Садов, Стеганографические алгоритмы на основе вейвлет- преобразований, Минск: РИВШ, с.2014-110.

[2] K.H. Jung, K.Y. Yoo, Steganographic method based on interpolation and LSB substitution of digital images, Springer,

[3] Multimedia Tools and Applications, 2015, vol. 74, pp. 2143-2155.

[4] N. Zaker, A. Hamzeh, A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram, Springer, Multimedia Tools and Applications, 2012, vol 3, no.1, pp. 147-166.

[5] X. Liao, S. Guo, J. Yin, H. Wang, X. Li, A.K., Sangaiah, New cubic reference table based image steganography, Springer, Multimedia Tools and Applications, 2017, vol. 25, pp. 1-18.

[6] A. Nissar, A. Mir, Classification of steganalysis techniques: A study, Digital Signal Processing, 2010, vol. 20, pp. 1758-1770.

[7] M. Hussain, T.S. Antony, Ki-Hyun Jung, İmage steganography in spatial domain: A survey, Signal processing: İmage commu¬nication, 2018, vol. 65 , pp. 46-66

[8] N. Zaker, A. Hamzeh, A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram, Springer, Multimedia Tools and Applications, 2012, vol. 58 pp. 147-166.

[9] J. Fridrich, J. Kodovsky, Rich models for steganalysis of digital images, IEEE Transactions on Information Forensics and Security, 2012, vol.7, pp. 868-882.

[10] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, J. Fridrich, Selection-channel-aware rich model for steganalysis of digital images, IEEE International Workshop on Information Forensics and Security, 2014, pp. 48-53.

[11] V. Sedighi, R. Cogranne, J. Fridrich, Content-adaptive steganography by minimizing statistical detectability, IEEE Transactions on Information Forensics and Security, 2016, vol. 11, pp 221-234.

AN OVERVIEW OF STEGOANALYSIS METHODS

Sakit Verdiyev[1], Ababil Nagiyeva[2], Raxshanda Huseynova[3], Zakir Huseynov[4]

[1,2,4]Azerbaijan Technological University, Ganja, Azerbaijan

[3]Azerbaijan State Agricultural University, Ganja, Azerbaijan

[1]*info_tel@inbox.ru*, [2]*nagiyevaababil@gmail.com*,
[3]*huseynova.raxshanda@mail.ru*

Abstract – Information securitiy in global public computer networks is became more important nowaday because there circulate a big quantity of various media data and it grows by exponensial tend every day. Therefore up to day there was developed a lot of different security methods. Here is considered and analised steganography technics what is used for digital image protection in open networks. In the same time here is demonstrated the concrete sample of stego-analise method caculating

Keywords *– steganography, stegooanalysis, stegoalgorithm, stegoimage, container, Chi-square.*