Kompüter Steqanoqrafiyası və Onun Əsas Prinsipləri

Sakit Verdiyev[1], Ababil Nağıyeva[2]
[1,2] Azərbaycan Texnologiya Universiteti, Gəncə, Azərbaycan
info_tel@inbox.ru

***Xülasə*— Məqalədə steqanoqrafiya və steqosistemlərdə informasiyanın gizli ötürülmə kanallarının formalaşdırılması üsularının və vasitələrinin tədbiqi məsələləri araşdırılır və onların tətbiqi problemləri müəyyən olunur, üstünlükləri və çatışmazlıqları göstərilir.**

Açar sözlər— informasiya təhlükəsizliyi, şifrləmə, komputer steqanoqrafiyası, steqosistem, konteyner, gizli ötürmə

I. GİRİŞ

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

Qlobal kompüter şəbəkələrinin günbəgün inkişaf etməsi və daha geniş istifadə olunması ilə əlaqədar olaraq, steqanoqrafiya daha böyük əhəmiyyət kəsb etməyə başlayır. Kompüter steqanoqrafiyasının inkişaf tendensiyasının təhlili göstərir ki, kompüter steqanoqrafiyası üsulları artan tendensiya ilə inkişaf edir və yaxın zamanda bu üsulların inkişafına maraq getdikcə daha çox artacaqdır.

İnformasiyanın qorunması sahəsində reallaşdırılan kriptoqrafik üsullar müəyyən məsələləri həll etməyə imkan verir. Lakin qeyd olunmalıdır ki, ziyanverici proqramlar (kompüter virusları, troya atları, məntiq bombalar və s.), reklam, replika, spam xarakterli proqramlar və s. kimi informasiya silahlarının dağıdıcı təsirləri ilə bağlı məsələlər hələ də həll olunmamış qalır [1].

Bu baxımdan kompüter steqanoqrafiyası üsullarının kriptoqrafik üsullarla birləşdirilməsi və ya birgə tətbiqi yaxşı nəticələr əldə etməyə imkan verə bilər.

II. STEQOSİSTEM

Kriptosistemlərə analoji olaraq, steqanoqrafiyada steqosistem terminindən istifadə olunur. Steqosistem – informasiyanın gizli ötürülməsi kanalının formalaşdırılması üsul və vasitələr toplusudur.

Şəkil1-də ümumiləşdirilmiş steqosistem göstərilmişdir.

Şəkildən göründüyü kimi, müasir steqosistemlərdə(yəni kompüter steqanoqrafiyasında) əsas iki növ fayl mövcuddur:

- ***məlumat***. Gizlədilməsi tələb olunan fayl;
- ***konteyner***. Məlumatın gizlədilməsi üçün istifadə olunan fayl.

Qeyd etmək lazımdır ki, konteynerlərin iki növünü fərqləndirilər:"o*rjinal"*və "*boş*". Boş konteyner- tərkibində gizli informasiya olmayan konteynerdir. Bundan başqa "Yekun" və ya "doldurulmuş" konteyner vardır. "Yekun" və ya "doldurulmuş" konteyner- tərkibində gizli informasiya yerləşdirilmiş konteynerdir.

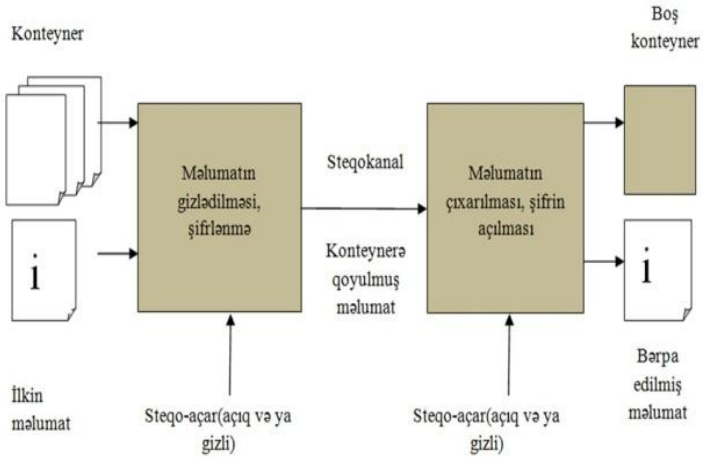
Steqanoqrafik açar dedikdə məlumatın konteynerə daxil edilməsi qaydalarını müəyyən edən məxfi element başa düşülür.

Kompüter steqanoqrafiyası iki əsas prinsip üzərində qurulur:

- mütləq dəqiqlik tələb edən digər növ məlumatlardan fərqli olaraq, öz funksionallığını itirmədən rəqəmli şəkil və ya səs fayllarının müəyyən dərəcədə dəyişdirilməsi mümkündür;
- insanın hissiyyat üzvləri şəklin rəngində və ya səsin kefiyyətində edilən cüzi dəyişikliyi fərqləndirmək qabiliyyətinə malik deyildir.

Müasir kompüter steqanoqrafiyasının əsas müddəaları aşağıdakılardır:

- informasiyanın gizlədilməsi üsulları onun autentikliyi (həqiqiliyini) və tamlığını təmin etməlidir;
- fərz edilir ki, rəqibə (bədniyyətli şəxsə) bütün mümkün steqanoqrafik üsullar tam məlumdur;
- üsulların təhlükəsizliyi açıq şəkildə ötürülən fayla məxfi məlumat daxil edilən zaman onun əsas xassələrinin, eləcə də rəqibə (bədniyyətli şəxsə) qeyri-məlum olan hər hansı informasiyanın, yəni açarın steqanoqrafik çevrilmələr vasitəsilə qorunmasına əsaslanmalıdır;



Şəkil 1. Steqosistemin ümumi modeli

- gizli məlumatın gizlədilməsi faktı hər hansı yolla rəqibə (bədniyyətli şəxsə) məlum olsa belə, məxfi məlumatın özünün əldə olunması mürrəkəb hesablama məsələsindən ibarət olmalıdır.

DOI: 10.25045/NCSoftEng.2017.19

III. KOMPÜTER STEQANOQRAFİYASININ ƏSAS İSTİQAMƏTLƏRİ

Müasir dövrdə kompüter steqanoqrafiyası iki əsas istiqamət üzrə inkişaf edir [2].

I. Kompüterlərdə istifadə olunan formatların xüsusi xassələrinin istifadəsinə əsaslanan üsullar:

1.1. Kompüter verilənlərinin formatlarının genişləndirilməsi üçün ehtiyat saxlanılan sahələrin istifadəsi üsulları. Nəzərə alınmalıdır ki, genişləndirmə üçün nəzərdə tutulmuş sahələr əksər multimedia formatlarında vardır. Bu sahələr sırf informasiya ilə doldurulur və adi proqramlar tərəfindən istifadə olunmurlar.

Üstünlükləri: istifadə üçün sadədirlər.

Çatışmazlıqları: gizlilik səviyyəsi aşağıdır və ötürülən informasiyanın həcmi məhduddur.

1.2. Mətn fayllarının xüsusi formatlaşdırılması üsulları. Bu üsullar da öz növbəsində bir neçə yerə bölünür.

1.2.1. Sözlərin, cümlələrin, abzasların yerlərinin dəyişdirilməsi üsulları. Bu üsullar sətirlərin yerlərinin və cümlələrdə sözlərin düzülüşünün müəyyən olunmuş qaydada dəyişdirilməsinə əsaslanır.

1.2.2. Hərflərin müəyyən mövqelərinin seçilməsi üsulu (sıfır şifr). Bu üsullar cümlələrdə, sətirlərdə və ya sözlərdə müəyyən mövqedə duran (məsələn, birinci) hərfləri istifadə etməklə məlumatın yazılmasına əsaslanır. Bu üsulların xüsusi halı kimi akrostic üsulunu (sətirlərin baş hərfləri məlumatı əmələ gətirir) göstərmək olar.

Üstünlükləri: istifadə üçün sadədirlər və sərbəst (pulsuz) yayılan reallaşdırılmış proqram təminatı mövcuddur

Çatışmazlıqları: gizlilik səviyyəsi zəif, məhsuldarlıq aşağı və ötürülən informasiyanın həcmi məhduddur.

1.3. disk, disket, flaş və digər yaddaş qurğularının istifadə olunmayan yerlərində məlumatların gizlədilməsi üsulları. Gizlədilən informasiya yaddaş qurğularının adi vəziyyətlərdə standart proqramlar tərəfindən istifadə olunmayan yerlərinə (məsələn, sıfırıncı cığıra, “korlanmış” sektorlara və s) yazılır[3].

Üstünlükləri: istifadə üçün sadədirlər və sərbəst (pulsuz) yayılan reallaşdırılmış proqram təminatı mövcuddur.

Çatışmazlıqları: gizlilik səviyyəsi zəif, məhsuldarlıq aşağı və ötürülən informasiyanın həcmi məhduddur.

1.4 Fayl identifikasiya edən başlığın pozulması üsulları. Gizlədilən fayl şifrlənir, alınan nəticə faylından onu identifikasiya edən başlıq pozulur və yalnız şifrlənmiş məlumat saxlanılır. Alan tərəf belə faylın xassələrini bilir və həmin pozulmuş başlığa malik olur.

Üstünlükləri: reallaşdırma sadədir və PGP şifrləmə alqoritmi vasitəsilə bu üsul reallaşdırmağa imkan verən çoxlu sayda proqram vasitələri (məsələn, White Noise Storm, S-Tools) mövcuddur.

Çatışmazlıqları: məlumatın gizlədilməsi proqblemi qismən həll edilir və faylın pozulan hissəsinin əvvəlcədən digər tərəfə göndərilməsi zərurəti yaranır [4].

II. Rəqəmli fotoşəkildə, rəqəmli səsdə və rəqəmli videoda izafiliyin istifadə edilməsinə əsaslanan üsullar:

2.1. Adətən, rəqəmli obyektlərdən istifadə olunan baytların kiçik bitləri (sağdan birinci bitlər) çox az faydalı informasiya daşıyırlar. Onların əlavə informasiya ilə doldurulması, praktiki olaraq, həmin rəqəmli obyektlərin qəbul edilməsinin kefiyyətinə təsir etmir ki, bu da məxfi informasiyanın gizlədilməsinə imkan verir [5].

Üstünlükləri: böyük həcmdə informasiyanı gizli göndərməyə imkan verir, müəlliflik hüququnun, əmtəə nişanının, qeydiyyat nömrələrinin və s. gizli təsvir edilməsi mümkündür.

Çatışmazlıqları: əlavə informasiyanın daxil edilməsi hesabına rəqəmli axınların statistik xarakteristikaların korreksiyası tələb olunur, alan tərəfə informasiyanın bir hissəsinin əvvəlcədən göndərilməsi zəruridir. Aşağıda nümunə kimi bəzi məhşur steqanoqrafik proqramlara nəzər salaq.

2.2. Steganos for Win 95 - windowsəməliyyat sistemi mühitində faylların şifrlənməsi və VOC, WAV, ASCII, HTML tipli faylların içində gizlədilməsi üçün güclü imkanlara malik proqram təminatıdır. İstifadəni sadələşdirmək üçün proqram master – proqram şəklində reallaşdırılmışdır

2.3. Contraband – windows əməliyyat sistemi mühitində istənilən faylı 24 bitli BMP formatlı qrafik fayllarda gizlətməyə imkan verən proqram təminatıdır.

2.3. Jsteg – DOS əməliyyat sistemi mühitində məşhur JPG formatlı qrafik faylda informasiyanın gizlədilməsi üçün nəzərdə tutulmuş proqramdır.

2.4. FFEncode – mətn fayllarında məlumatları gizlətməyə imkan verən DOS proqramıdır. Proqram müvafiq parametrlərlə əmrlər sətrindən yerinə yetirilir.

2.5. StegoDos – şəkili seçməyə, onun tərkibində məlumatı gizlətməyə və onu başqa qrafik formatda saxlamağa imakn verən DOS mühiti üçün nəzərdə tutulmuş proqram paketidir.

2.6.Wnstorm- DOS mühitində məlumatı şifrləməyə və PSX formatlı qrafik faylın içərisində gizlətməyə imkan verən proqram paketidir.

IV. RƏQƏMLİ STEQANOQRAFİYA

Rəqəmli steqanoqrafiya - klassik steqanoqrafiyanın rəqəmli obyektlərin müəyyən təhrif olunması hesabına onlarda 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 [6].

DOI: 10.25045/NCSoftEng.2017.19

NƏTİCƏ

Qeyd olunduğu kimi steqanoqrafiya elmi də informasiya təhlükəsizliyinin təmin edilməsi problemi ilə məşğul olur. Kompüter steqanoqrafiyasının vəzifəsi informasiyanın varlığını, saxlanılması, emal olunması və ötürülməsi faktını gizlətməkdən ibarətdir. Başqa sözlə, kompüter steqano-qrafiyasının əsas məqsədi qorunan məlumatın varlığının rəqibdən saxlanılmasıdır.

Beləliklə görünür ki,kompüter steqanoqrafiyası informasiya təhlükəsizliyi sahəsində çox mühüm və perspektivli bir sahə olaraq geniş tədqiq və tədbiq olunmalıdır..

ƏDƏBİYYAT

[1] P. Morillo, C. Padro, G. Saez, J. L Villar, “Weighted threshold secret sharing schemes”. Information Processing Letters, 211-216.

[2] A. Beimel, T. Tassa, E. Weinreb, “Characterizing ideal weightedthreshold secret sharing”, Journal on Discrete Mathematics, 2008, 22,360-397.

[3] T. Tassa və N. Dyn, “Multipartite secret sharing by bivariate interpolation”, 33rd international conference on Automata, Languages and Programming , 2006

[4] A. Shamir, “How to Share a Secret”. Communications of the Acm, 1979, pp. 612-613.

[5] G. R. Blakley, “Safeguarding cryptographic keys”. National Computer Conference, 313-317.

[6] O. Farras, C. Padro, “Ideal Hierarchical Secret Sharing Schemes”, Theory of Cryptography, 219-236.

DOI: 10.25045/NCSoftEng.2017.19