AZƏRBAYCAN RESPUBLIKASI

Əlyazması hüququnda

INTERNET KANALLARINDA XİDMƏTİ İNFORMASİYANIN GİZLİ ÖTÜRÜLMƏSİ ÜSULLARININ VƏ TEXNOLOGİYALARININ İŞLƏNMƏSİ

İxtisas: 3338.01 – Sistemli analiz, idarəetmə və informasiyanın işlənməsi

Elm sahəsi: Texnika elmləri

İddiaçı: **Esmira Əli qızı Mustafayeva**

Fəlsəfə doktoru

elmi dərəcəsi almaq üçün təqdim edilmiş

A V T O R E F E R A T I

Bakı – 2022

Dissertasiya işi AMEA-nın İdarəetmə Sistemləri İnstitutunun "Kütləvi xidmət və ehtiyatların idarə edilməsi sistemlərinin modelləşdirilməsi" laboratoriyası nəzdində yerinə yetirilmişdir.

Elmi rəhbər: texnika elmləri doktoru, professor
Vaqif Əlicavad oğlu Qasımov

Rəsmi opponentlər: AMEA-nın müxbir üzvü,
texnika elmləri doktoru, professor
İsmayıl Mahmud oğlu İsmayılov

texnika elmləri doktoru, professor
Ələkbər Əli Ağa oğlu Əliyev

texnika elmləri doktoru, professor
Ramin Rza oğlu Rzayev

Azərbaycan Respublikasının Prezidenti yanında Ali Attestasiya Komissiyasının AMEA-nın İdarəetmə Sistemləri İnstitutunun nəzdində fəaliyyət göstərən ED 1.20 Dissertasiya şurası

Dissertasiya şurasının sədri: akademik,
texnika elmləri doktoru, professor
Əli Məhəmməd oğlu Abbasov

Dissertasiya şurasının elmi katibi:
texnika elmləri doktoru, professor
Nailə Fuad qızı Musayeva

Elmi seminarın sədri:
texnika elmləri doktoru, professor
Fərhad Heydər oğlu Paşayev

İŞİN ÜMUMİ XARAKTERİSTİKASI

Mövzunun aktuallığı və işlənmə dərəcəsi. Müasir dövrdə informasiya təhlükəsizliyin tələb olunan səviyyədə təmin edilməsi üçün informasiya ehtiyatlarının müvafiq infrastrukturunun, eləcə də təhlükəsizlik sisteminın yaradılması, inkişaf etdirilməsi və təkmilləşdirilməsi vacibdir. Lakin heç kəsə sirr deyil ki, informasiya texnologiyaları sahəsində müsair elmi-texniki tərəqqi müsbət nailiyyətlərin əldə olunması ilə yanaşı informasiya təhlükəsizliyi sahəsində bir sıra ciddi problemlərin meydana gəlməsinə səbəb olmuşdur. Belə problemlərə kompüterlərin, kompüter sistemlərinin və şəbəkələrinin işinə qeyri-qanuni müdaxilə, kompüter informasiyasının oğurlanması, mənimsənilməsi, gizli əldə olunması (tutulması), ötürülməsi (sızması və ya sızdırılması) kimi təhlükəli təzahürləri aid etmək olar.

Hazırda informasiya mübadiləsi məqsədilə Internet şəbəkəsindən, onun informasiya xidmətlərinin imkanlarından bütün dünyada geniş istifadə olunur. Internet şəbəkəsi onun xidmətlərindən istifadə edən bütün insanlar və təşkilatlar, o cümlədən cinayətkar və terrorçu qruplar və şəxslər üçün eyni dərəcədə imkanlar yaradır. Telekommunikasiya sistemləri, kompüter və informasiya şəbəkələri, o cümlədən Internet ayrı-ayrı fərdlər, siyasətçilər, iş adamları, dövlət, özəl və dini təşkilatlar, cinayətkar terrorçu qruplar və rəqib (düşmən) ölkələrin xüsusi xidmət orqanları tərəfindən xidməti fəaliyyətdə geniş istifadə edilməklə yanaşı, həmçinin, informasiya mübarizəsi, qarşıdurması, müharibəsi, kibercinayət və kiberterrorçuluq alətləri və vasitələri kimi çıxış edir. Bu baxımdan informasiya təhlükəsizliyi sahəsində kompleks tədbirlərin görülməsi zəruridir.

Təcrübədə təhlükəsizliyin təmin edilməsi baxımından konfidensial informasiyanın rabitə kanalı ilə ötürülməsi zamanı onun məzmunun və ötürülməsi faktının gizlədilməsinə ciddi zərurət yaranır. Məlum olduğu kimi, informasiyanın gizli ötürülməsi məsələləri ilə steqanoqrafiya elmi məşğul olur. Aydındır ki, steqanoqrafiya kriptoqrafiyanı əvəz etmir, yalnız onu tamamlayır.

Qeyd edilməlidir ki, bir çox ölkələrdə kriptoqrafiyanın lisenziyasız (və ya icazəsiz) reallaşdırılmasına və istifadəsinə müəyyən məhdudiyyətlərin, hətta qadağaların qoyulması steqanoqrafiyanın inkişafına xüsusilə təkan verdi. Eyni zamanda

ümumi təyinatlı Internet şəbəkəsinin hərtərəfli inkişafı və geniş yayılması, Internet vasitəsilə informasiya mübadiləsi zamanı tələb olunan müəlliflik hüququnun qorunması, şəxsi sirrsaxlama hüququnun qorunması, elektron ticarətin təşkili, elektron bank əməliyyatlarının həyata keçirilməsi, hakerlərin, terrorçuların fəaliyyətinin qarşısının alınması və s. kimi axıra qədər həll edilməmiş məsələlər informasiyanın qorunmasının yeni üsul və vasitələrinin reallaşdırılmasını zəruri edir. Digər tərəfdən, informasiya texnologiyalarının, Internetin sürətli inkişafı təklif olunan yeni üsulların reallaşdırmasına, gizli informasiya mübadiləsi kanallarının yaradılması və istifadəsinə imkanlar yaradır.

Dissertasiya işində Internetdə informasiyanın gizli mübadiləsi kanalların yaradılması üsulları araşdırılmış, xidməti informasiyanın ötürülməsi üçün belə kanalların istifadəsi, eləcə də müxtəlif məzmunlu məlumatların gizli ötürülməsi imkanları, üsulları və texnologiyaları tədqiq edilmişdir.

Tədqiqatın obyekti xidməti informasiya, onun emal olunduğu və ötürüldüyü şəbəkədir.

Tədqiqatın predmeti isə xidməti informasiyanın gizli ötürülməsi kanallarının yaradılması və analizindən ibarətdir.

Tədqiqatın məqsədi Internet şəbəkəsində xidməti informasiyanın etibarlı və təhlükəsiz ötürülməsini təmin etmək üçün steqanoqrafik üsullar əsasında gizli kanalların yaradılması üsullarının və texnologiyalarının işlənməsindən ibarətdir.

Tədqiqat metodları. Yerinə yetirilmiş dissertasiya işində aparılan tədqiqatlarda informasiya nəzəriyyəsi, sistemli analiz, riyazi modelləşdirmə, ehtimal nəzəriyyəsi, çoxluqlar nəzəriyyəsi, verilənlərin sıxılması alqoritmləri və eksperimentlərdən istifadə edilmişdir.

Müdafiəyə çıxarılan əsas müddəalar.

1. Steqanoqrafik sistemin və gizli kanalın modeli;
2. Gizlədilən məlumatların xarakteristikasından asılı olaraq, gizli kanalın və yeridilmə alqoritminin seçilməsi üsulu;
3. Sosial şəbəkələr (o cümlədən Whatsapp) və elektron poçt xidməti üzərindən gizli kanalların yaradılması üsulları;
4. İnternet protokollarında reallaşdırılan gizli kanalların buraxıcılıq qabiliyyətinin qiymətləndirilməsi üsulu;

5. Steqanoqrafik sistemlərin dayanıqlığının və steqokonteynerlərin davamlığının təhlili və qiymətləndirilməsi üsulları;

6. İnformasiyanın qrafik fayllarda daha etibarlı şəkildə gizlədilməsini təmin edən modifikasiya olunmuş LSB üsulu;

7. Mətn tipli konteynerlərdə informasiyanın gizlədilməsi üçün simvollararası intervallar üsulu;

8. Mətnlərdə informasiyanın gizlədilməsinin simvollararası intervallar üsulunun etibarlığının yüksəldilməsi üçün xətti konqruyent üsuldan və Feygenbaumun kvadratik funksiyasından birgə istifadə etməklə simvolların psevdotəsadüfi ardıcıllıqla seçilməsi alqoritmi.

Tədqiqatın elmi yeniliyi.

1. Xidməti informasiyanın etibarlı ötürülməsini təmin edən steqanoqrafik sistemin və gizli kanalın modeli təklif olunmuşdur.

2. Internetin sosial şəbəkələrində gizli kanalların yaradılması texnologiyaları təhlil edilmiş, Whatsapp və elektron poçt xidmətləri üzərindən gizli ötürmə kanallarının yaradılması üsulları işlənmişdir.

3. Gizlədilən məlumatların xarakteristikasından asılı olaraq, konteynerlərin, gizli kanalların və yeridilmə alqoritmlərinin seçilməsi üsulları işlənmişdir.

4. Internet protokollarında paketin uzunluğunun dəyişdirilməsinə əsaslanan gizli kanalın buraxıcılıq qabiliyyəti tədqiq edilmiş və müvafiq analitik ifadə alınmışdır.

5. Internet kanallarında informasiyanın gizli ötürülməsi üçün istifadə olunan steqokonteynerlərin davamlılığının qiymətləndirilməsi üçün yanaşma təklif olunmuşdur.

6. Qrafik fayllarda informasiyanın gizlədilməsinin etibarlığını artırmaq üçün modifikasiya olunmuş LSB üsulu və onun reallaşdırılması üçün müvafiq alqoritm işlənmişdir.

7. Mətn tipli konteynerlərdə informasiyanın səmərəli və effektiv gizlədilməsi üçün simvollararası intervallar üsulu işlənmiş, onun etibarlığının yüksəldilməsi üçün xətti konqruyent üsuldan və Feygenbaumun kvadratik funksiyasından birgə istifadə etməklə simvolların psevdotəsadüfi ardıcıllıqla seçilməsi alqoritmi işlənmişdir.

Tədqiqatın nəzəri və praktiki əhəmiyyəti. Internet üzərindən gizli kanalların yaradılması texnologiyalarının inkişaf etdirilməsi, xidməti informasiyanın qorunması, gizli ötürülməsi üsullarının

işlənməsi və praktikada tətbiqi ilə informasiya təhlükəsizliyi problemlərinin həllinə imkan yaradır. Eyni zamanda, elmi tədqiqatların nəticələri, neqativ məqsədlərlə yaradılan gizli informasiya ötürmə kanallarının aşkarlanması üçün istifadə oluna bilər.

Aprobasiyası və tətbiqi. Dissertasiya işinin əsas nəticələri aşağıdakı elmi-texniki konfranslarda müzakirə edilmişdir:

- Информационные процессы и технологии «Информатика-2014» VII Международной научно-практической конференции, Севастополь, 2014;
- Qafqaz Universiteti, Gənc tədqiqatşıların III beynəlxalq elmi konfransı, Bakı, 2015;
- Milli Aviasiya Akademiyası, Gənclərin yaradıcı potensialı aviokosmik məsələlərin həllində Beynəlxalq iştirakla II elmi-praktiki gənclər konfransı, Bakı, 2017;
- Информационные технологии и математическое моделирование (ИТММ-2017) XVI Международной конференции имени А.Ф.Терпугова, Томск, 2017.

Dissertasiya işi üzrə aparılmış elmi tədqiqatlar zamanı alınmış elmi-praktik nəticələr Milli Aerokosmik Agentliyinin Kosmik Cihazqayırma Məxsusi Konstruktor Bürosunun və Təbii Ehtiyatların Kosmik Tədqiqi İnstitutunun xidməti fəaliyyətində konfidensial informasiyanın gizli ötürülməsini təmin etmək məqsədilə tətbiq olunmuşdur. Bu barədə müvafiq tətbiq aktları alınmışdır.

Dissertasiya mövzusu üzrə nüfuzlu jurnallarda 8 elmi məqalə, o cümlədən 5 məqalə xaricdə dərc olunmuşdur. Onlardan 1-i Web of Science, 1-i Ulakbim (TrDizin) bazasına, 2 məqalə isə Ukrayna AAK-ın siyahısına daxil olan elmi jurnallarda çap olunmuşdur.

Dissertasiya işi Azərbaycan Milli Elmlər Akademiyasının İdarəetmə Sistemləri İnstitutunda yerinə yetirilmişdir.

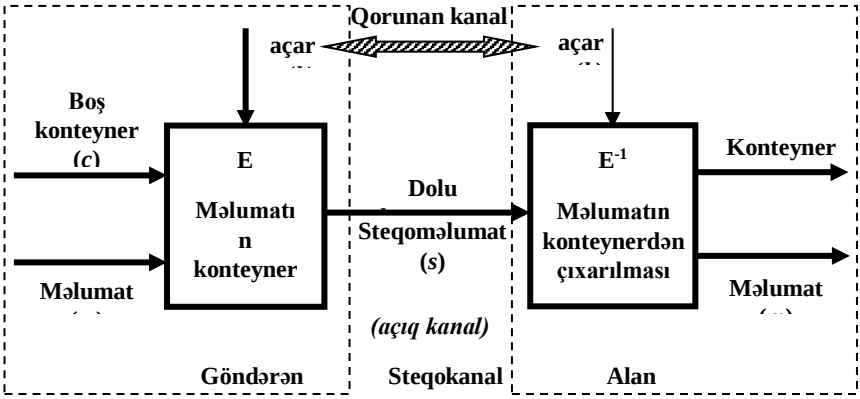
Dissertasiya işi girişdən, dörd fəsildən, nəticədən və ədəbiyyat siyahısından ibarətdir. Giriş 7045 (7872), I fəsil 46307 (52383), II fəsil 36945 (41798), III fəsil 45272 (51217), IV fəsil 43081 (49159), nəticə 1446 (1608) işarədən ibarət olmaqla dissertasiyanın işarələrlə ümumi həcmi 180596 (204037) işarə təşkil edir.

İŞİN QISA MƏZMUNU

Girişdə mövzunun aktuallığı əsaslandırılmış, tədqiqatın məqsəd və vəzifələri müəyyənləşdirilmiş, alınan elmi nəticələrin yeniliyi, praktiki əhəmiyyəti, işin nəticələrinin realizə olunması şərh edilmişdir.

Birinci fəsil informasiya təhlükəsizliyi sistemində xidməti informasiyanın qorunması problemi qeyd edilmiş və bu problemlərin həlli istiqamətində steqanoqrafiyanın rolundan bəhs edilmişdir. Bu məqsədlə steqanoqrafik üsul və vasitələrin inkişafının müasir vəziyyətinin təhlil olunmuşdur. Təhlillər əsasında bəzər müasir steqanoqrafik üsulların çatışmazlıqlarının aradan qaldırılması məsələləri dissertasiya işində öz həllini tapmışdır. Belə ki, mətn steqanoqrafiyasının intervallar üsulu, rəqəmsal steqanoqrafiyanın LSB üsulu və şəbəkə steqanoqrafiyasına baxılmışdır. Bundan əlavə bu fəsildə steqanoqrafik sistemlər, gizli kanallar və onların modeli qurulmuş, gizli kanalların yaradılması üsulları təhlil edilmişdir.

Steqanoqrafiyanın əsas anlayışlarından biri steqanoqrafik sistem (steqosistem) anlayışıdır. Steqanoqrafik sistem (steqosistem) informasiyanın gizli ötürülməsi kanalının yaradılması üçün istifadə olunan üsul və vasitələr toplusudur. Başqa sözlə, steqanoqrafik sistem – məlumatlar, konteynerlər və onları birləşdirən çevirmələr toplusudur.



Şək.1. Steqanoqrafik sistemin struktur sxemi

Ümumi halda, steqanoqrafik sistem – məlumatlar, konteynerlər və onları birləşdirən çevirmələr toplusudur (şək.1.).

Məlumat (*M*) – varlığının və ya ötürülməsi faktının gizlədilməsi tələb olunan qorunan məlumatdır. $M=\{m_1,m_2,...,m_n\}$ – qorunan məlumatlar çoxluğudur.

Konteyner (*C*) dedikdə məlumatın gizlədilməsi üçün istifadə olunan qeyri-məxfi xarakterli obyekt (maddi obyekt, informasiya daşıyıcısı, informasiya ehtiyatı, fayl və s.) nəzərdə tutulur. $C=\{c_1,c_2,...,c_q\}$ – konteynerlər çoxluğudur, harada ki, q>>n. Məlumat və konteyner qismində adi mətn kimi multimediya fayl formatları da ola bilər.

Məlumat yeridilməmiş konrteyner *boş konteyner* və ya orijinal-konteyner adlanır. Məxfi məlumat daxil edilmiş (yeridilmiş) konteyner isə *dolu konteyner* (nəticə-konteyner) adlanır, yəni hər hansı qorunan *m* məlumatını özündə saxlayan konteynerdir (c_m). Bir qayda olaraq, dolu konteyneri *steqoməlumat* adlandırırlar.

Steqoməlumatlar (doldururlmuş konteyner) çoxluğunu aşağıdakı kimi işarə edirlər:

$$S=\{(c_1,m_1), (c_2,m_2) ,..., (c_q,m_q)\} = \{s_1,s_2,...,s_q\}.$$

Steqanoqrafik konteynerlərə qoyulan əsas tələblərdən biri ondan ibarətdir ki, vizual olaraq dolu konteyner orjinal konteynerdən seçilməməlidir və ya insanın hissiyyat orqanları (göz, qulaq) bu fərqi hiss etməməlidir.

Steqanoqrafik sistemin modelini aşağıdakı kimi vermək olar:

$$SteqoSys = (M, C, S, K, E, E^{-1}). \quad (1)$$

Burada

K – steqanoqrafik açarlar çoxluğudur.

E və E^{-1} – steqanoqrafik çevirmələrdir (məlumatın gizlədilməsi və çıxarılması prosesləri).

Steqanoqrafik açar ($k \in K$) dedikdə konkret məxfi məlumatın konteynerdə gizlədilməsi və konteynerdən çıxarılması üçün istifadə olunan əlavə məlumat nəzərdə tutulur.

Steqanoqrafik açarı tərəflər əvvəlcədən qorunan kanal vasitəsilə bir-birinə çatdırır.

E – gizlətmə üsulu olub, steqanoqrafik açarın köməyi ilə məlumatın konteynerə yerləşdirilməsini, E^{-1} isə steqanoqrafik açarın

köməyi ilə gizlədilən məlumatın steqoməlumatdan çıxarılmasını yerinə yetirən steqanoqrafik çevirmələrdir:

$$E:\ M \times C \times K \to S,\ \text{yəni}\ \ S = E(M,C,K),$$
$$E^{-1}:\ S \times K \to M,\ \text{yəni}\ \ M = E^{-1}(S,K). \qquad (2)$$

İkinci fəsildə Internet üzərindən gizli informasiya ötürmə kanalının yaradılması imkanlarına baxılmış, Facebook, Google+ sosial şəbəkəsində, Bulud xidmətlərində, Web üzərindən gizli kanalların yaradılması təcrübədən keçirilmişdir. Bundan əlavə, elektron poçt xidməti vasitəsilə informasiyanın gizli ötürülməsi kanalları reallaşdırılmışdır.

E-mail vasitəsilə istifadəçilər arasında konfidensial informasiya mübadiləsini həyata keçirmək üçün gizli kanallar reallaşdırmaq mümkündür. Burada bir neçə üsuldan istifadə etmək olar:

1. E-mail məktubunun məzmununda (mətnində) məlumatın gizlədilməsindən ibarətdir. Məktuba daxil edilən mətnin formatlaşdırılması üçün xüsusi redaktordan istifadə olunur. Bu redaktor məktubun mətninin formatlaşdırılması ilə yanaşı, məktuba xüsusi simvolların, animasiya və işarələrin daxil edilməsi imkanlarını təqdim edir. Bu imkanlar vasitəsilə mətn steqanoqrafiyasının intervallardan, sinonimlərdən və şərtləşdirilmiş ifadələrdən istifadə etməklə elektron məktubun açıq məzmununda məlumat gizlətmək olar. Həmçinin, ekektron poçtun mətn sahəsinin fonuna uyğun şriftin rəngini seçməklə informasiyanı gizli şəkildə ötürmək olar.

2. Elektron poçta hər hansı faylın (şəklin, qrafikin, videonun, sənədin, pdf faylın, cədvəlin və s.) əlavə edilməsindən (attach) ibarətdir. Bu halda elektron məktuba əlavə edilən fayl kimi əvvəlcədən hər hansı steqanoqrafik üsulun köməyi ilə konfidensial informasiya gizlədilmiş steqokonteyner çıxış edə bilər, yəni əvvəlcədən hazırlanmış steqokonteyneri məktuba əlavə etmək mümkündür.

3. Elektron məktubun hazırlanması və qaralama (draft) kimi poçt qutusunda saxlanması prinsipinə əsaslanan üsul. Bu üsulda konfidensial informasiya mübadiləsi aparmaq istəyən tərəflər öz aralarında poçt serveri, elektron poçt identifikatoru (istifadəçi adı) və parolu, eləcə də mübadilə tarixi və vaxtı barədə əvvəlcədən razılaşırlar.

Konfidensial informasiya mübadiləsi aşağıdakı ardıcıllıqla həyata keçirilir:

- Məlumatı göndərən tərəf əvvəlcədən müəyyən edilmiş poçt serverində razılaşdırılmış ad və parola (username və password) uyğun elektron poçt ünvanı yaradır, məsələn, mail.ru serverində "esmira.mustafayeva" adlı poçt qutusu;
- Məlumatı göndərən tərəf əvvəlcədən müəyyən edilmiş vaxtda ad və paroldan (username və password) istifadə etməklə həmin serverə daxil olur;
- Ötürülməsi lazım olan konfidensial informasiyaya uyğun məzmuna malik elektron məktubu hazırlayır, göndəriləcək ünvanı daxil etmədən həmin məktubu qaralama (draft) qovluğunda saxlayır və elektron poçtdan çıxır;
- Konfidensial informasiyanı alan tərəf əvvəlcədən razılaşdırıldığı kimi müəyyın olunmuş vaxtda elektron poçt qutusuna daxil olur;
- Qaralama (draft) qovluğunda saxlanılmış qaralama məktubu götürür (oxuyur və ya surətini çıxarır) və qovluqdan silir;
- Elektron poçt xidmətindən çıxır. Bununla da gizli informasiya mübadiləsi həyata keçirilmiş olur.

Qeyd edilməlidir ki, bu üsul çox qısa müddətdə həyata keçirilir. Başqa sözlə, qaralama məktubun yaradılması və onun oxunaraq silinməsi təxminən eyni vaxtda baş verir. Həmin məktub Internet vasitəsilə digər istifadəçiyə, onun serverinə ötürülmür. Bu səbəbdən informasiyanın (elektron məktubun) kənar şəxsin əlinə keçməsi mümkünsüz olur. Bir qayda olaraq, belə poçt qutuları birdəfəlik istifadə üçün nəzərdə tutulur, yəni istifadə olunduqdan sonra gizliliyin təmin edilməsi üçün poçt qutusu ya serverdən silinir, ya da bir daha istifadə olunmur.

Daha sonra 2-ci fəsildə Whatsapp üzərindən informasiyanın gizli ötürülməsi kanalının reallaşdırılması məsələsinə baxılmışdır. Whatsapp üzərindən gizli kanalın reallaşdırılması istiqamətində araşdırmalar aparılmış və təcrübi yoxlamalar həyata keçirilmişdir. Təcrübələr zamanı konteyner qismində təsvir fayllarından istifadə edilmişdir. Məlum olmuşdur ki, mübadilə zamanı konteyner qismində ötürülən gif, bmp, png və s. formatlı şəkillər alan şəxsə JPEG formatında çatır. Bu səbəbdən JPEG formatlı şəkillərdən istifadə

olunması məqsədəuyğun hesab edilmişdir. Digər formatlı şəkillərin WhatsApp vasitəsilə ötürülməsi zamanı onların dəyişikliyə məruz qalması və yeridilmiş məlumatın itməsi faktı müəyyən edilmişdir. Bu səbəbdən eksperimentlərdə yalnız JPEG formatlı faylları dəstəkləyən steqanoqrafik proqramlardan istifadə olunmuşdur. Bundan əlavə bu steqanoqrafik proqramların təhlili zamanı müəyyən olundu ki, əksər tətbiqlər LSB üsulu əsasında reallaşdırlmışdır.
Təcrübə müxtəlif vaxtlarda, müxtəlif versiyalar üçün aparılmışdır. Android əməliyyat sistemi üçün nəzərdə tutulmuş proqramlar içində Stegais və Stegos proqramları WhatsApp vasitəsilə reallaşdırılan steqokonteynerlərdə informasiya mübadiləsi zamanı şəkillərin ölçüsündə dəyişiklik baş vermir və yeridilən informasiya heç bir dəyişikliyə, itkiyə uğramadan müvəffəqiyyətlə ünvana çatır. Beləliklə, WhatsApp kanalında konteyner qismində şəkil fayllarına informasiya yeritməklə gizli kanal yaratmaq mümkündür.

Windows əməliyyat sistemi üçün hazırlanmış steqanoqrafik proqramlar vasitəsilə WhatsApp Web sosial şəbəkəsində gizli kanal yaratmaq mümkün deyil.

İkinci fəsildə bundan əlavə, Internet protokollarında informasiyanın steqanoqrafik gizlədilməsi üsulları araşdırılmış, praktiki olaraq IP, TCP, UDP, ICMP protokolları vasitəsilə gizli kanallar yaradılmışdır. Təcrübə zamanı Wireshark analizatorundan və paketlərin göndərilməsi üçün PlayCap proqramlarından, ICMP paketlərinin şəbəkədən keçməsi üçün əmrlər sətrində ping utilitindən istifadə olunmuşdur.

Üçüncü fəsil Internet üzərindən reallaşdırılan steqanoqrafik sistemlərin keyfiyyət göstəriciləri təhlili edilmişdir. Steqosistemlərin təhlükəsizliyi onların dayanıqlığı ilə təsvir edilir və qiymətləndirilir. Steqosistemlərin dayanıqlığının təhlili zamanı məlumatın ötürülməsi faktının pozucudan gizlədilməsi, gizli ötürülən məlumatın pozucu tərəfindən dağıdılması, təhrif edilməsi, pozulması kimi cəhdlərə dayanıqlı olması keyfiyyətləri, eləcə də gizli ötürülən informasiyanın təsdiqi və ya inkarı xüsusiyyətləri araşdırılır. Buu məqsədlə dissertasiya işində gizli məlumatların xarakteristikası əsasında konteynerlərin, gizli kanalların və yeridilmə alqoritminin seçilməsi, Internet kanallarında informasiyanın gizli ötürülməsi üçün istifadə

olunan steqokonteynerlərin davamlığının qiymətləndirilməsi məsələlərinə baxılmış, Internet üzərindən reallaşdırılan gizli kanalların buraxıcılıq qabiliyyətinin qiymətləndirilməsi həyata keçirilmişdir.

Gizli informasiya ötürmə kanalının buraxıcılıq qabiliyyəti dedikdə konteynerin bir elementinə maksimum miqdarda informasiyanın yerləşdirilməsi kimi başa düşülür.

Bir qayda olaraq, gizli kanallar kiçik buraxıcılıq qabiliyyətinə malik olduqda ciddi təhlükə yaranmır. Ona görə də, gizli kanallar üçün təhlükəsiz sayılan buraxıcılıq qabiliyyətinin aşağı həddi təyin edilir.

Buraxıcılıq qabiliyyətinin müəyyən edilməsi, gizlədilən informasiyanın xüsusiyyətlərindən asılı olaraq, gizli kanalın, konteynerin və yeridilmə alqoritminin seçilməsi üçün zəruridir.

İnformasiya nəzəriyyəsi üsulları ilə gizli kanalın C buraxıcılıq qabiliyyətini

$$C = \max_{n}\left\{\frac{I(X,Y)}{\tau}\right\}$$

ifadəsi əsasında hesablamaq olar. Burada τ- paketin orta ötürülmə müddəti, $I(X,Y) = H(Y) - H(Y/X)$ - uyğun olaraq, gizli kanalın giriş və çıxış xarakteristikalarını təsvir edən X və Y təsadüfi kəmiyyətlərinin qarşılıqlı informasiyasıdır.

Paketin orta ötürülmə müddətinin gizli kanalın n parametri əsasında

$$\tau = \frac{2l_{fiks} + n - 1}{2\beta}$$

şəklində müəyyən edilməsi nəzərə alınaraq, gizli kanalın C buraxıcılıq qabiliyyəti aşağıdakı kimi hesablanır:

$$C \approx \frac{2\left(log_2(2l_{fiks} - 1) - log_2\left(W\left(\frac{2l_{fiks} - 1}{e}\right)\right)\right)}{2l_{fiks} + \frac{2l_{fiks} - 1}{W\left(\frac{2l_{fiks} - 1}{e}\right)} - 1}\beta \quad (3)$$

Burada β- rabitə kanalının buraxıcılıq qabiliyyəti, $W(y)$ isə $y = xe^x$ – tənliyinin kökləri kimi təyin edilən Lambert funksiyasıdır, yəni $f(w) = we^w$ – funksiyasının tərs funksiyasıdır. (3) düsturunda

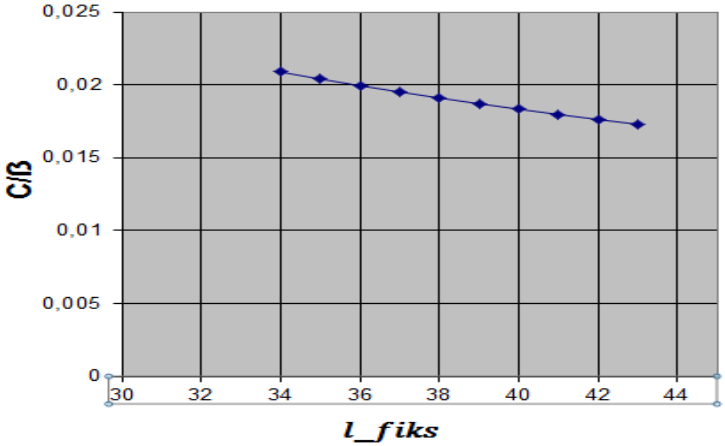
$$2l_{fiks} + \frac{2l_{fiks} - 1}{W\left(\frac{2l_{fiks} - 1}{e}\right)} - 1$$

ifadəsi minimum qiymət aldıqda gizli kanalın C buraxıcılıq qabiliyyəti maksimum olur. Bu isə o deməkdir ki, gizli kanalın n parametri aşağıdakı şəkildə seçilməlidir:

$$n \approx \frac{2l_{fiks} - 1}{W\left(\frac{2l_{fiks} - 1}{e}\right)} \quad (4)$$

Burada, l_{fiks} kəmiyyəti seçilərkən nəzərə almaq lazımdır ki, şəbəkə səviyyəli protokol IPv4 şəbəkə protokolundan istifadə edilirsə kanal səviyyəli texnologiya Ethernet olduqda şəbəkə və kanal səviyyəli başlıqların uzunluqları cəmi 34 baytdan, IPv6 protokolundan istifadə zamanı isə 54 baytdan kiçik olmur.

Yuxarıda göstərilənlər nəzərə alınaraq, OSI modelinin şəbəkə və kanal səviyyələrində başlıqların uzunluqları cəminin (l_{fiks}) müxtəlif qiymətlərində gizli kanalın nisbi buraxıcılıq qabiliyyəti (C/β) hesablanmış və nəticə şəkil 2-də qrafiki şəkildə əks olunmuşdur.



Şək. 2. Nisbi buraxıcılıq qabiliyyətinin (C/ß) OSI modelinin şəbəkə və kanal səviyyələrində başlıqların uzunluqları cəmindən (l_{fiks}) asılılığı qrafiki

Qrafikdən göründüyü kimi, l_{fiks} parametrinin 34-ə bərabər qiymətində nisbi buraxıcılıq qabiliyyəti maksimum qiymət alaraq, təqribən 0.021-ə bərabər olur. Qeyd edək ki, bu halda Ipv4 protokolundan istifadə halında gizli kanalın n parametri 138 qiymətini alır.

Beləliklə, $5Qbit/san$ buraxıcılıq qabiliyyətinə malik rabitə kanalında IPv4 protokollarından istifadə edildikdə $5Qbit \cdot 0{,}021 = 105Mbit/san$ və Ipv6 protokollarından istifadə edildikdə isə $5Qbit \cdot 0{,}014 = 70Mbit/san$ maksimim buraxıcılıq qabiliyyətinə malik gizli kanallar yaratmaq olar.

Dördüncü fəsil Internetdə informasiyanın gizli ötürmə kanallarının və steqanoqrafik üsullarının proqram həllərinə baxılmışdır. Mövcud steqanoqrafik proqram vasitələri konteynerlərdən istifadəsinə və alqoritmlərinə görə müqayisəli təhlili edilmişdir.

Qrafik fayllarda informasiyanın etibarlı gizlədilməsi üçün modifikasiya olunmuş LSB üsulu, mətnlərdə informasiyanın gizlədilməsinin simvollararası intervallar üsulu təklif edilmişdir

Mətnlərdə informasiya gizlədilməsinin etibarlığının artırılması məqsədilə simvolların psevdotəsadüfi seçilməsi üsulu irəli sürülmüşdür. Steqanoqrafik tətbiqlərin təhlili zamanı məlum olur ki, bu tətbiqlərin əksəriyyətinin realizasiyası zamanı ən az əhəmiyyətli bitlər (LSB – Least Significant Bit) üsulundan istifadə edilmişdir. Bu üsul insanların hissiyat orqanlarının məhdud xüsusiyyətlərinə əsaslanır. Belə ki, informasiyanın gizlədilməsi nəticəsində konteynerdə edilmiş kiçik rəng dəyişikliklərini insanların gözləri seçə bilmir. Bu üsulların çatışmazlığı steqokonteynerin rabitə kanalı ilə göndərilərkən rəqibin əlinə keçməsi və gizlədilən məlumatın aşkar edilməsi (açılması) ehtimalının olmasından ibarətdir.

Bu çatışmazlığın aradan qaldırılması məqsədilə LSB üsulunun modifikasiya olunmuş variantı təklif edilmişdir. Təklif olunan üsulda iki qrafik fayldan istifadə olunur, onlardan biri konteyner, digəri isə steqanoqrafik açar rolunda çıxış edir. Üsulun özəlliyi ondan ibarətdir ki, konteynerə yeridilən məlumatın özü yox, həmin məlumat haqqında informasiya olur. Yəni ikinci qrafik faylın - steqanoqrafik açarın piksellərinin RGB kanallarının sonuncu bitləri ilə gizlədilən

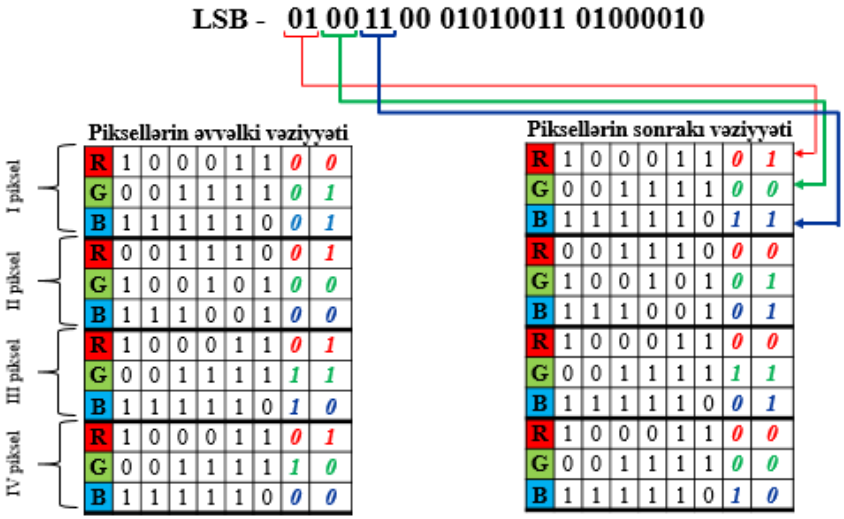
məlumatın bitləri 2 moduluna görə toplanır. Nəticə əsasında konteynerin müvafiq piksellərinin RGB kanallarının sonuncu bitləri dəyişdirilir. Açar fayl rabitə kanalı ilə ötürülmədiyindən gizlədilən informasiya rəqibin əlinə keçə bilməz, çünki modifikasiya olunmuş və gizlədilən informasiyanı özündə saxlamayan konteynerin əsasında onu açmaq mümkün deyil.

Tutaq ki, konteyner qismində bir rastr tipli 24 bitlik RGB təsvirdən istifadə olunur. Belə təsvirdə hər bir nöqtə (piksel) üç baytla kodlaşdırılır. Burada birinci bayt qırmızı (Red), ikinci bayt yaşıl (Green), üçüncü bayt isə göy (Blue) rəngin intensivliyini, onların qiymətləri birlikdə həmin pikselin rəng çalarını müəyyən edir. Bu baytlarda kiçik (ən sağdakı) bitlər böyük (soldakı) bitlərə nisbətən təsvirin çalarına çox az təsir göstərir. Həmin baytlarda bir və ya iki kiçik bitin əvəz edilməsi insan gözü üçün hiss edilməyəcək dəyişikliyə gətirib çıxarır.

Əyani olması üçün rastr tipli 24 bitlik RGB təsvirində steqanoqrafik üsulun adı – "LSB" məlumatı gizlədilir. "LSB" məlumatının ikilik kodlarla təsviri "01001100 01010011 01000010" olar. Təsvirə 24 bitlik ardıcıllığı yerləşdirmək üçün hər baytda iki bit olmaqla dörd piksel lazımdır. Qeyd olunan bitlər ardıcıllığının piksellərdə yerləşdirilməsindən əvvəl və sonrakı təsvirləri şəkil 3-də göstərilmişdir.

Ən az əhəmiyyətli bitlər üsulu müəyyən çatışmazlığa malikdir. Belə ki, üsulun əks alqoritmi əsasında tətbiqlər də mövcuddur ki, bununla gizli məlumatı aşkarlamaq mümkündür. Qeyd olunan çatışmazlığın aradan qaldırılması məqalədə LSB üsulunun modifikasiya olunmuş variantı təklif edilmişdir.

Təklif olunan üsulda ölçüsü və qrafik parametrləri eyni olan iki PIC1 və PIC2 qrafik fayllarından (məsələn, 24 bitli rastr tipli RGB təsvirlərdən) istifadə olunur. PIC1 qrafik faylı steqanoqrafik açar rolunda çıxış edir və məxfi məlumatın konteynerdə gizlədilməsi və konteynerdən çıxarılması prosesində istifadə olunur. Bu fayl informasiyanı göndərən və alan tərəflər arasında əvvəlcədən təyin olunur. Tərəflər bu faylı qabaqcadan gizli kanalla bir-birinə ötürür və ya razılaşmaya əsasən hər hansı açıq mənbədən (məsələn, Internet saytdan) götürürlər.



Şək. 3. LSB üsulu əsasında gizlədilən bitlər ardıcıllığının yerləşdirilməsi

PIC2 qrafik faylı məxfi məlumatı göndərən şəxs tərəfindən konteyner qismində istifadə olunur. Qeyd etmək lazımdır ki, konteynerə ötürülən məlumat deyil, həmin məlumat haqqında informasiya daxil edilir. Konteynerin piksellərinin RGB kanallarının sonuncu bitləri ötürülən məlumata və PIC1 qrafik faylına uyğun olaraq dəyişdirilir. Dəyişdirilmiş PIC2 faylını alan şəxs qabaqcadan aldığı PIC1 faylından və konteynerdən istifadə etməklə gizli məlumatı bərpa edir. PIC1 faylı rabitə kanalı vasitəsilə ötürülmədiyindən rəqibin əlinə keçə bilməz. Rabitə kanalı ilə ötürülən modifikasiya olunmuş PIC2 konteynerinə məxfi məlumatın özü daxil edilmədiyindən, onu bu fayla əsasən bərpa etmək mümkün deyil.

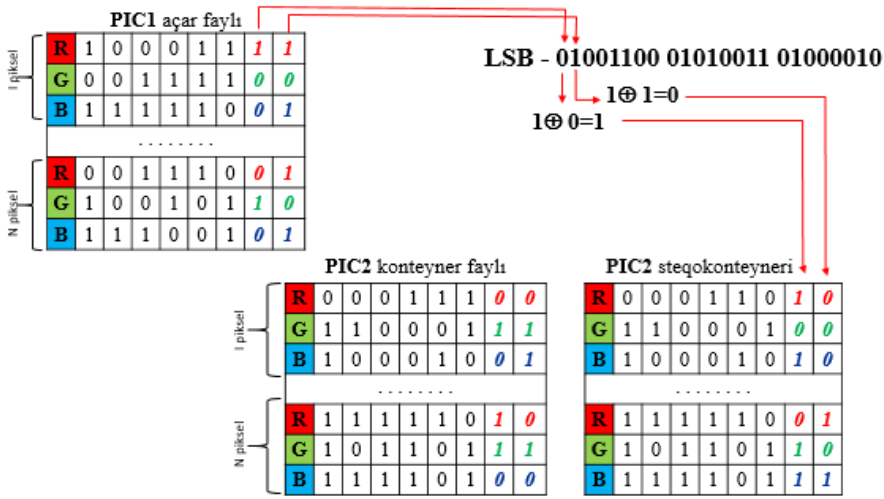
Ötürülən gizli məlumat konteynerə daxil edilməsi üçün əvvəlcə ikilik koda çevrilir. Bu zaman qorumanı gücləndirmək məqsədilə məlumatı əvvəlcədən şifrləmək olar.

Təklif olunan üsula əsasən konteyner təsvirin hər pikselinə 3 bit, yəni hər rəng kanalına 1 bit yerləşdirildiyinə görə konteynerdə gizlədilən informasiyanın maksimal həcmi $L \leq 3*I$ olar. Burada L – gizlədilən informasiyanın bitlərlə ölçüsü, yəni konteynerə daxil edilən

bitlərin sayı, I – konteynerin, yəni PIC2 təsvirinin piksellərinin miqdarıdır.

Qeyd edildiyi kimi konteynerin piksellərinin hər bir rəng kanalında yəni, hər baytında iki bit də gizlətmək mümkündür. Bu halda gizlədilən informasiyanın həcminə qoyulan məhdudiyyət $L \leq 6*I$ olar.

Məlumatın konteynerdə gizlədilməsi alqoritmini aşağıdakı kimi təsvir etmək olar. Gizlədilən məlumatın birinci (ikinci və üçüncü) biti götürülür və PIC1 təsvirinin birinci pikselinin birinci (ikinci və üçüncü) baytının axırıncı biti ilə 2 moduluna görə (⊕) toplanır. Alınan nəticə PIC2 təsvirinin birinci pikselinin birinci (ikinci və üçüncü) baytının axırıncı bitində uyğun olaraq yerləşdirilir (şək.4.).



Şək. 4. LSB üsulunun modifikasiya olunmuş variantının təsviri

İnformasiyanın bütün bitləri PIC1 təsvirinin müvafiq piksellərinin rəng kanallarının axırıncı bitləri ilə 2 moduluna görə toplanır və nəticədən asılı olaraq PIC2 təsvirinin müvafiq piksellərinin rəng kanallarının axırıncı bitləri ilə dəyişdirilir. Nəticədə PIC2 qrafik faylı dəyişdirilmiş olur. Lakin göründüyü kimi bu fayl ötürülən məlumatı özündə saxlamır. Ona yalnız göndərilən məlumatın bitləri ilə PIC1 faylının rəng kanallarının sonuncu bitlərinin eyni və ya fərqli

olması barədə informasiya daxil edilir. PIC1 faylına malik olmayan şəxs gizlədilən informasiyanı aşkar edə bilməz.

Dəyişdirilmiş PIC2 faylı heç bir təhlükə olmadan açıq rabitə xətti vasitəsilə ünvana göndərilir. Əgər göndərilən fayl rəqibin əlinə keçərsə və həmin faylda məlumatın gizlədilməsi barədə şübhə yaranarsa, PIC1 faylı məlum olmadığından gizlədilmiş məlumatı steqokonteynerdən çıxarmaq mümkün olmayacaqdır.

PIC2 steqokonteynerini alan tərəf gizlədilən məlumatın çıxarılması üçün onun piksellərinin bütün kanallarının sonuncu bitlərini ardıcıl şəkildə uyğun olaraq PIC1 açar faylının piksellərinin sonuncu bitləri ilə 2 moduluna görə toplayır. Alınan nəticə gizli informasiyanın bitlərini əks etdirmiş olur.

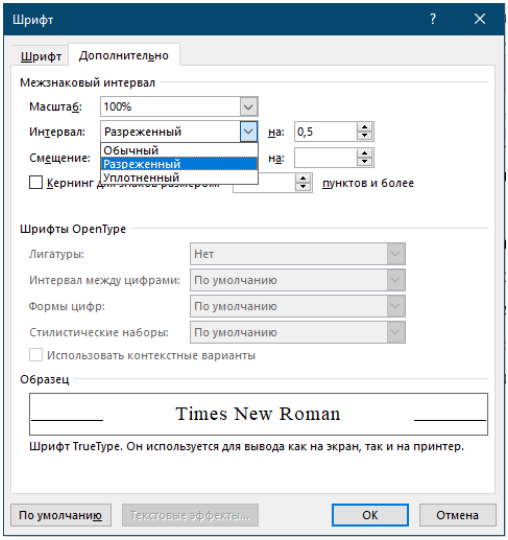
Təklif olunan iki qrafik fayllı LSB üsulunun modifikasiyası adi LSB üsulunun çatışmazlığını aradan qaldırır. Bu üsulda konteyner kimi istifadə olunan bir qrafik fayla gizlədilən məlumatın özü deyil, onun haqqında informasiya daxil edilir. Bu informasiya gizlədilən məlumatla steqanoqrafik açar rolunda çıxış edən hər hansı ikinci qrafik faylın əsasında tərtib edilir. Steqanoqrafik açar rabitə kanalı ilə ötürülmədiyindən gizlədinlən informasiyanın qorunması daha etibarlı təmin edilmiş olur.

Qeyd etmək lazımdır ki, konteyner qismində bmp, jpeg, gif və s. formatlı qrafik fayl istifadə oluna bilər. Burada yeganə tələb həm konteyner, həm də steqanoqrafik açarın eyni formatlı və eyni ölçülü olmasından ibarətdir.

Daha sonra dördüncü fəsildə Word sənədlərində informasiyanın gizlədilməsinin simvollararası intervallar üsulu təklif edilmişdir.

Məlumdur ki, bu gün praktikada istifadə olunan mətn tipli fayllar arasında MS Word redaktorunda hazırlanmış sənədlər əksəriyyət təşkil edir. Məhz belə sənədlərdə informasiyanın gizlədilməsi üçün daha çox imkanlar mövcuddur. Belə imkanlardan biri də, mətndə sözlərin simvolları arasındakı intervallardan istifadə olunmasıdır. Bunun üçün verilmiş gizli informasiya əvvəlcə ikilik koda (məsələn, ASCII standartına uyğun olaraq) çevrilir. Bundan sonra, MS Word redaktorunun *Шрифт* (Şrift) pəncərəsinin *Интервал* (İnterval) hissəsində olan *Интервал* (İnterval) açılan siya-

hısının *Разреженный* (Seyrək) və *Уплотненный* (Sıx) parametrlərinin qiymətlərini dəyişməklə həmin informasiya sənədlərin mətnlərində gizlədilir (şək.5.).



Şək. 5. İnformasiyanın gizlədilməsi üçün parametrin dəyişdirilməsi

Qeyd edilməlidir ki, Word redaktorunda hazırlanmış sənəddə sözlərin simvolları arasındakı intervallar üçün *Expanded* (Seyrək) və *Condensed* (Sıx) parametrlərinin qiyməti 0–0,3 pt intervalında təyin edildikdə, mətndə baş verən dəyişikliklər insan gözü ilə görünəcək həddi aşmır. Ona görə də simvollar arasındakı intervalı 0,3-ə qədər dəyişməklə ikilik formatda verilmiş informasiyanı kodlaşdırmaq və sənədə yerləşdirmək mümkündür.

Məlum olduğu kimi, Word redaktorunda bu parametrlər üçün başlanğıc qiymət 0, artırıb-azaltma addımı isə 0,05-dir. Beləliklə, sinvollararası intervalı 0-dan 0,25-dək 0,05 addımı ilə dəyişdikdə 10 kodlaşdırma variantı yaratmaq olar. Bu isə sənəddə daha çox informasiya gizlətmək imkanı verir (cədv. 1).

Cədv.1. Bitlər ardıcıllığının kodlaşdırılması üçün simvollararası intervallar

Kodlaşdırılan bitlər	Simvollararası intervallar	
	Seyrək (Expanded)	Sıx (Condensed)
000	0,05	-
001	-	0,05
010	0,1	-
011	-	0,1
100	0,15	-
101	-	0,15
110	0,2	-
111	-	0,2
0	0,25	-
1	-	0,25

Qeyd edilməlidir ki, təklif olunan üsulda konfidensial informasiyanın mətndə gizlədilməsi üçün tələb olunan konteynerin həcmi mətn steqanoqrafiyasının digər mövcud üsullarında istifadə edilən konteynerlərdən əhəmiyyətli dərəcədə kiçik ola bilər. Belə ki, sözlərarası probelin istifadəsi alqoritmində hər sözdə bir bit, sətirsonu probellər üsulunda bir sətirdə 1-3 bit gizlədildiyi halda, təklif olunan üsulda hər simvolda 3 bit gizlətmək mümkündür. Başqa sözlə, 300 simvoldan ibarət informasiyanı gizlətmək üçün birinci üsulda 2400 sözdən, ikinci üsulda təxminən 18000 sözdən, təklif olunan üsulda isə 100 sözdən ibarət mətn tələb olunur.

Təklif olunan üsulun iş prinsipini daha əyani nümayiş etdirmək üçün aşağıdakı nümunəyə baxaq. Tutaq ki, MS Word sənədində "*Seminar sabah keçiriləcək*" informasiyasının gizlədilməsi tələb olunur. Bunun üçün informasiya əvvəlcə ASCII standartına uyğun olaraq ikilik koda çevrilir:

11010001 11100101 11101100 11101000 11101101 11100000
11110000 11110001 11100000 11100001 11100000 11111001
11101010 11100101 11110111 11101000 11110000 11101000
11101011 11111111 11100110 11111111 11101010

Göründüyü kimi, 23 hərfdən ibarət olan informasiya ikilik koda çevrildikdən sonra 184 ikilik simvoldan ibarət ardıcıllıq alınır. Alınmış ardıcıllıq hər biri 3 bit olmaqla qruplara bölünür və cəmi 62 qrup alınır. Ən azı 62 sözdən ibarət sənəd-konteyner seçilir (şək.6).

Fiziki proseslərdə bir neçə enerji forması mövcuddur. Onları bir neçə qrup daxilində birləşdirmək mümkündür. Enerji forması onun daxil olduğu qrupdan asılı olmayaraq sistemin halını göstərən xarakterik kəmiyyətdir. Burada enerjinin saxlanması qanunu hökm sürür, yəni qapalı sistemin ümumi enerjisi həmişə sabitdir. Yalnız sistemə kənardan təsir etdikdə (əlavə enerji verdikdə) onun ümumi enerjisi dəyişir. Mexaniki sistemin enerjisini kibernetik və potensial enerjinin cəmi kimi təsvir etmək olar.

Şək.6. Orjinal konteyner

Fiziki proseslərdə bir neçə enerji forması mövcuddur. Onları bir neçə qrup daxilində birləşdirmək mümkündür. Enerji forması onun daxil olduğu qrupdan asılı olmayaraq sistemin halını göstərən xarakterik kəmiyyətdir. Burada enerjinin saxlanması qanunu hökm sürür, yəni qapalı sistemin ümumi enerjisi həmişə sabitdir. Yalnız sistemə kənardan təsir etdikdə (əlavə enerji verdikdə) onun ümumi enerjisi dəyişir. Mexaniki sistemin enerjisini kibernetik və potensial enerjinin cəmi kimi təsvir etmək olar.

Şək.7. İnformasiya daxil edilmiş konteyner

Verilən informasiyanın gizlədilməsi üçün sənəd-konteynerin sözlərində simvollar arasındakı intervallar müvafiq bit qruplarının qiymətlərinə uyğun təyin edilir (şək.7).

Mətnlərdə informasiyanın gizlədilməsinin simvollararası interval üsulunun steqoanalizə davamlılığının daha da yüksəldilməsi üçün gizli informasiyanın konteynerə yazılma prosesini ardıcıl deyil, xaotik şəkildə yerləşdirilməsi məqsədəuyğundur. Bu proses psevdotəsadüfi ədədlər (PTƏ) ardıcıllığından istifadə etməklə yerinə yetirilə bilər, yəni, cədvəl 1-ə əsasən bitlərlə qruplara ayrılmış gizlədilən informasiyanın yerləşdirilməsi üçün konteyner mətninin simvollarının xaotik seçilməsini müəyyən ediir. Psevdotəsadüfi

ədədlər ardıcıllığının generasiya edilməsi üsulları çoxluq təşkil edir, lakin müxtəlif alqoritmlərə əsaslanan üsulların səmərəliliyi, əsasən onların tətbiq edildiyi sahələrdən asılı olur. İnformasiyanın qorunması kimi daha ciddi məsələlərdə bir neçə üsulun birgə istifadəsi məqsədəuyğun hesab edilir.

Apardığımız bu tədqiqat işində gizlədilən informasiyanı mətn tipli konteynerdə təsadüfi ardıcıllıqla yerləşdirilməsi üçün xətti konqruyent üsul və Feygenbaumun kvadratik funksiyasının birgə tətbiqi ilə alınan psevdotəsadüfi ədədlər ardıcıllığından istifadə edilmişdir.

Xətti konqruyent üsulun alqoritmi 1948-ci ildə D.X.Lemer tərəfindən təklif edilmişdir və o, müntəzəm paylanmış təsadüfi ədədlərin generasiyası üçün yaradılan alqoritmlərdən biridir. Alqoritmin əsasını

$$x_{n+1} = (ax_n + c)\ mod\ m, n \geq 0 \quad (5)$$

ifadəsi təşkil edir. Burada, x_0 – başlanğıc qiymət $(x_0 \geq 0)$, a – vuruq $(a \geq 0)$, c – sabit ədəd $(c \geq 0)$, m isə moduldur $(m > x_0, m > a, m > c)$. Alqoritmin reallaşdırılması nəticəsində alınan sıra, x_0 başlanğıc qiymətinin seçilməsindən asılıdır və bunun fərqli qiymətləri üçün təsadüfi ədədlərin müxtəlif ardıcıllığı əldə edilir. x_0, a, c və m kəmiyyətlərinin müəyyən qiymətlərində alınan ədədlər ardıcıllığında dövri olaraq təkrarlanmalar baş verir, yəni bu kəmiyyətlər ixtiyari seçilə bilməz. Xətti ardıcıllığın dövrü yalnız o vaxt m-ə bərabər olur ki, o, aşağıdakı şərtləri ödəmiş olsun:

1) c və m qarşılıqlı sadə ədədlərdir;

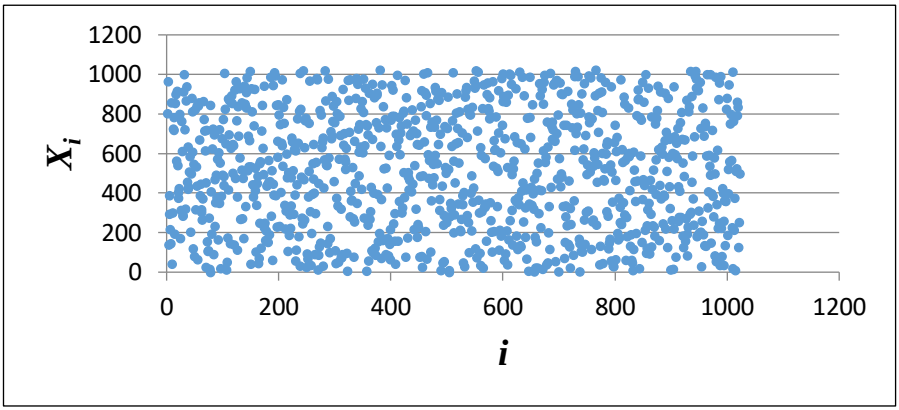
2) m-in hər bir sadə p böləni üçün $b = a - 1$ ədədi p-nin mislinə bərabərdir;

3) m 4-ün mislinə bərabər olduğu halda, b ədədi 4-ün mislinə bərabərdir.

a sabitinin yuxarıdakı şərtləri ödəməklə seçilməsi kifayət qədər yaxşı nəticənin əldə olunmasını təmin edir, təbii ki, burada a və m ədədlərinə qoyulan $m>a$ şərtinin də ödənilməsi nəzərə alınmalıdır. c sabiti, a-nın qiymətinin müəyyən edilməsində ciddi rol oynamır və burada əsas tələb c-nin tək ədəd olmasıdır. Nümunə üçün, baxılan tələblər əsasında $m = 1024, a = 397$ və $c = 11$ götürsək,

$$x_{i+1} = (397x_i + 11)\ mod\ 1024 \quad (6)$$

ifadəsi əsasında 1024-dək təsadüfi ədədlər ardıcıllığını generasiya edə bilərik. Başlanğıcı $X_0 = 497$ olan psevdotəsadüfi ədədlər ardıcıllığının vizual görüntüsü şəkil 8-də əks olunmuşdur və göründüyü kimi ədədlər müntəzəm paylanmaya malikdir.



Şək.8. Xətti konqruyent üsulla alınan psevdotəsadüfi ədədlər ardıcıllığı

Lakin qeyd etmək lazımdır ki, əksər PTƏG-lər kimi bu üsulda da ardıcıl gələn elementlər arasında müəyyən asılılıq vardır və bu asılılıqdan bir neçə ardıcıl ədəd məlum olduqda, digərlərinin hesablanması üçün istifadə edilə bilər. Bunu nəzərə alaraq, ədədlər ardıcıllığının müəyyən nöqtələrində əlaqəni zəiflətməklə ardıcıllığın məlum elementlərinə görə digərlərinin hesablanması prosesini əhəmiyyətli dərəcədə mürəkkəbləşdirmək mümkündür. Bu məqsədlə, apardığımız tədqiqat işində Feygenbaumun kvadratik funksiyasından istifadə edilməsi təklif olunur.

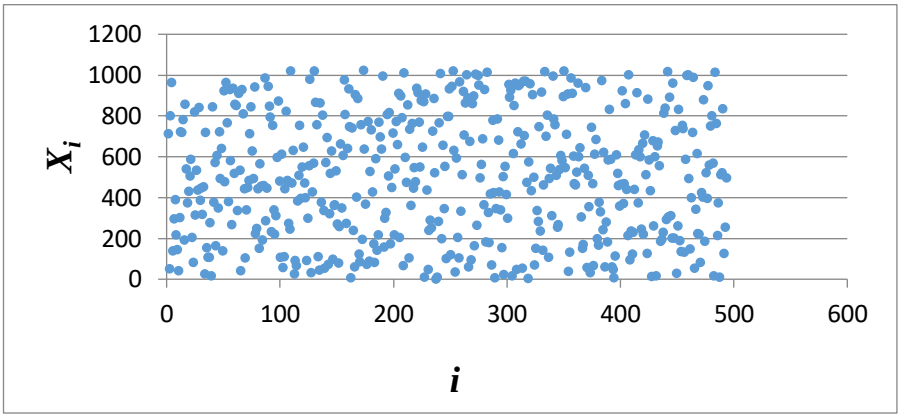
Feygenbaumun kvadratik funksiyası deterministik xaos proseslərini əks etdirən funksiyalardan biri olub aşağıdakı iterasiyalı düsturla ifadə edilir:

$$y_{n+1} = r y_n (1 - y_n) \qquad (7).$$

(7) kvadratik funksiyası r parametrinin 3,57-dən 4-dək olan qiymətlərində y_i-nin 0-la 1 arasında xaotik qaydada dəyişən ədədlər ardıcıllığını generasiya etməyə imkan verir. Məhz bu xaotiklik xüsusiyyətindən istifadə etməklə, (6) ifadəsi əsasında alınmış ədədlər

ardıcıllığının seçmə yolu ilə bir qisminin çıxarılması ilə yeni ardıcıllıq yaradılır. Alınan yeni ardıcıllıqda ədədlər arasında əlaqəlilik kifayət qədər zəifləmiş olur ki, bu da ardıcıllığın məlum elementlərinə görə digərlərinin hesablanması işini çətinləşdirir.

Xətti konqruyent üsulu və Feygenbaumun kvadratik funksiyası ($r = 3{,}9612345678,\ y_0 = 0{,}5678987654$) əsasında generasiya olunmuş psevdotəsadüfi ədədlər ardıcıllığının vizual görüntüsü şəkil 9-da əks olunmuşdur. Şəkil 8 ilə müqaisədə aydın olur ki, ədədlər müntəzəm paylanmaya malik olmayan psevdotəsadüfi ardıcıllıqdan ibarətdir.



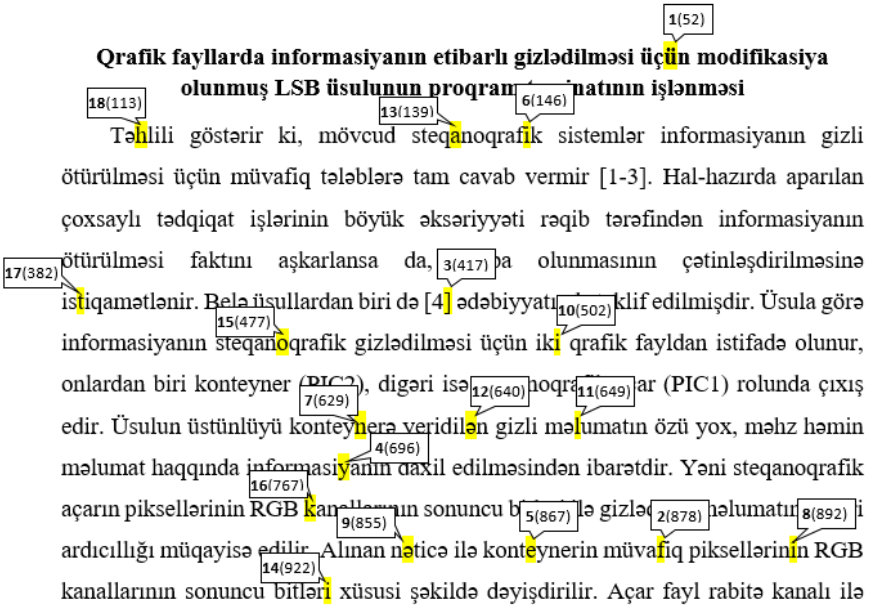
Şək.9. Xətti konqruyent üsul və Feygenbaumun kvadratik funksiyası əsasında alınan psevdotəsadüfi ədədlər ardıcıllığı

Yeni ardıcıllığın alınması prosesi aşağıdakı addımlarla həyata keçirilir:

a) (6) ifadəsi əsasında n sayda psevdotəsaddüfi ədədlərdən ibarət A ardıcıllığı generasiya edilir;
b) Generasiya edilmiş ədədlər ardıcıllığı hər biri 10 ədəddən ibarət olmaqla $n/10$ sayda q_i $(i = 1..n/10)$ qruplarına bölünür;
c) (7) ifadəsi əsasında $n/100$ sayda elementdən ibarət B ardıcıllığı generasiya edilir (burada onluq kəsr şəklində olan hər bir elementin kəsr hissəsinin uzunluğu 10 rəqəmdən kiçik olmamalıdır);

d) B ardıcıllığının 1-ci elementinin vergüldən sonrakı 1-ci rəqəminə uyğun sayda A elementinin 1-ci qrupunun ilk elementləri götürülərək yeni C ardıcıllığının ilk elementləri kimi qəbul edilir.
e) Bu proses A ardıcıllığı bitənədək davam edir və alınan nəticələr ardıcıl olaraq C ardıcıllığına əlavə edilir.

Nəticədə alınan C ardıcıllığı xətti konqruyent üsulu və Feygenbaumun kvadratik funksiyasının birgə istifadəsindən alınan psevdotəsadüfi ədədlər ardıcıllığıdır. Konteynerinin simvollarının ardıcıllığı bu psevdatəsadüfi ədədlər ardıcıllığına uyğun olaraq seçilir və gizlədilən informasiya seçilmiş ardıcıllıqla simvolların aralıq intervallarında yerləşdirilir (Şək.10).



Şək.10. Konteynerdə psevdotəsadüfi ardıcıllıq əsasında simvolların seçilməsi

Gizlədilən informasiyanın steqokonteynerdən çıxarılması prosesi informasiyanın konteynerə yeridilməsinin əks prosesidir, yəni qəbul edən tərəf gizli informasiyanı steqokonteynerdən çıxarması üçün bu prosesi əks ardıcıllıqla yerinə yetirməlidir. Göndərən və qəbul

edən tərəflər arasında əvvəlcədən razılaşdırılmış cədvəl 1 ilə yanaşı mətndə simvolların mövqeyini və ardıcıllığını təyin etmək üçün psevdotəsadüfi ardıcıllıqlar cədvəli də göndərilir. Qəbul edən tərəf psevdotəsadüfi ardıcıllıqlar cədvəli əsasında steqokonteynerdə simvolların mövqeyi və ardıcıllığını təyin edərək həmin simvolların aralıq intervalından cədvəl 1-ə uyğun gizli informasiyanı çıxarır.

Təklif edilən xətti konqruyent üsulu və Feygenbaumun kvadratik funksiyasının birgə istifadəsindən alınan psevdotəsadüfi ədədlər ardıcıllığı əsasında mətn konteynerlərinin simvollararası məsafəsində yerləşdirilən informasiyanın gizlilik səviyyəsi kifayət qədər artırılmış hesab edilir. İnformasiyanın gizlədilməsi məqsədilə konteynerlərdə simvolların xaotik seçilməsi üçün istifadə olunan psevdotəsadüfi ədadlər ardıcıllığının hesablanmasının mürəkkəbləşdirilməsi ardıcıl gələn elementlər arasında müəyyən asılılığın qarşısının alınması məqsədini daşıyır.

ƏSAS NƏTİCƏLƏR

1. Xidməti informasiyanın etibarlı ötürülməsini təmin edən steqanoqrafik sistemin və gizli kanalın modelləri təklif olunmuşdur.
2. Xidməti informasiyanın ötürülməsi məqsədilə Internetin sosial şəbəkləri üzərindən gizli kanalların yaradılması imkanları təhlil edilmiş, Whatsapp və elektron poçt xidmətləri vasitəsilə gizli kanallarının reallaşdırılması texnologiyaları təklif olunmuşdur.
3. Gizlədilən məlumatların xarakteristikasından asılı olaraq, konteynerlərin, gizli kanalların və yeridilmə alqoritmlərinin seçilməsi üsulları işlənmişdir.
4. Internetdə paketin uzunluğunun dəyişdirilməsinə əsaslanan gizli kanalın buraxıcılıq qabiliyyətinin hesablanması üçün nəzəri-informasiya üsulları əsasında müvafiq analitik ifadə alınmışdır.
5. Steqanoqrafik sistemlərin dayanıqlığının və steqokonteynerlərin davamlığının təhlili və qiymətləndirilməsi məsələsinə baxılmış, müvafiq tövsiyə və təkliflər işlənmişdir.
6. Xidməti informasiyanın qrafik fayllarda daha etibarlı gizlədilməsini təmin etmək üçün modifikasiya olunmuş LSB üsulu və onun reallaşdırılması alqoritmi işlənmişdir.
7. Mətn tipli konteynerlərdə informasiyanın gizlədilməsi üçün daha effektiv üsul təklif edilmiş, yeni simvollararası intervallar üsulu işlənib hazırlanmış, müvafiq proqram təminatı reallaşdırılmışdır.
8. Mətnlərdə informasiyanın gizlədilməsi üçün simvollararası intervallar üsulunun etibarlığının yüksəldilməsi məqsədilə xətti konqruyent üsulu və Feygenbaumun kvadratik funksiyasının birgə istifadəsindən alınan psevdotəsadüfi ədədlər ardıcıllığı əsasında simvolların təsadüfi seçilməsi alqoritmi təklif edilmişdir.

Dissertasiya işinin əsas nəticələri aşağıdakı elmi əsərlərdə dərc edilmişdir:

1. Qasımov V.Ə., Məmmədov S.Z., Mustafayeva E.Ə. Korporativ kompüter şəbəkələrində informasiya təhlükəsizliyinin təmin olunmasında elektron imza texnologiyasının tətbiqi haqqında // BDU-nun xəbərləri. Fizika-riyazıyyat elmləri seriyası. №2, 2007, səh.102-108
2. Qasımov V.Ə., Mustafayeva E.Ə. Word sənədlərində informasiyanın gizlədilməsinin simvollararası intervallar üsulu // Azərbaycan Milli Elmlər Akademiyasının xəbərləri. Fiziki-texnika və riyaziyyat elmləri seriyası. İnformatikanın və idarəetmənin problemləri. 2014, №6, səh.124-129
3. Qasımov V.Ə., Mustafayeva E.Ə. Internetdə informasiyanın gizli ötürülmə kanallarının yaradılması üsulları. // "Milli təhlükəsizlik və hərb elmləri" elmi-praktik jurnalı. Azərbaycan Respublikası Silahlı Qüvvələrinin Hərbi Akademiyası. Bakı. 2016. №3. səh.122-128.
4. Gasimov V.A., Mustafayeva E.A., Hüseynova G. Implementing covert channels to transfer hidden information over WhatsAPP on mobile phones // International Journal of Engineering and Applied Sciences (IJEAS) ISSN: 2394-3661, Volume-6, Issue-2, February 2019.
5. Gasimov V.A., Amashov Y.A., Aliyeva F.P., Mustafayeva E.A., Mutin D.I. Bolnokin V.E. Development of the information security system effective structure for the distributed computer networks. // IOP Conf. Series: Materials Science and Engineering. Vol. 537, IOP Publishing. 2019 (***Web of Sciences***)
6. Мустафаева Е. Принципы выбора контейнеров для стеганографических систем. // International Journal of 3D Printing Technologies and Digital Industry, Volume: 4 - Issue: 3, pages : 264-269, 04.11.2020 (***Ulakbim, TrDizin***)
7. Мустафаева Е.А. Исследование зависимости стеганографических систем от характеристик скрываемой

информации. // Проблеми інформатизації та управління, Том 3 № 67 (2021),с. 46-53 (***Ukrayna AAK***)

8. Gasimov V.A., Mammadov J.I., Mustaphayeva E.A. Intersymbol interval method for hiding secret information based on pseudo-random number sequences. Проблеми інформатизації та управління, Том 1 № 69 (2022), с. 18-23 (***Ukrayna AAK***)

Dissertasiya işinin müdafiəsi 26.10.22 il tarixində saat 16-da Azərbaycan Milli Elmlər Akademiyasının İdarəetmə Sistemləri İnstitutunun nəzdində fəaliyyət göstərən ED 1.20 Dissertasiya Şurasının iclasında keçiriləcək.

Ünvan: Az 1141, Bakı şəhəri, Bəxtiyar Vahabzadə küçəsi, 68. Azərbaycan Milli Elmlər Akademiyasının İdarəetmə Sistemləri İnstitutu.

Dissertasiya ilə Azərbaycan Milli Elmlər Akademiyasının İdarəetmə Sistemləri İnstitutunun kitabxanasında tanış olmaq mümkündür.

Dissertasiya və avtoreferatın elektron versiyaları Azərbaycan Milli Elmlər Akademiyasının İdarəetmə Sistemləri İnstitutunun rəsmi Internet saytında yerləşdirilmişdir.

Avtoreferat "23" sentyabr 2022-ci il tarixində zəruri ünvanlara göndərilmişdir.

Çapa imzalanıb:

Kağızın formatı: A5

Həcmi: 40721

Tiraj: 70