AXBOROTNI HIMOYALASHNING STEGANOGRAFIK USULLARI. STEGANOGRAFIYA USULLARI TAHLILI.

Норматов Иброхимали Холмаматович
O‘zbekiston Milliy universiteti professori
E-mail: i_normatov@nuu.uz,
Tel: +998977210920
Mamagapurova Shaxodat Shavkat qizi
O‘zbekiston Milliy universiteti ilmiy tadqiqotchisi

Annotatsiya. Mazkur maqola kriptografiyaning muhim vazifalaridan biri – steganografiyaga bag’ishlanadi. Ruxsat etilmagan kirishdan axborotni ishonchli himoyalash muammosi eng avvaldan mavjud va hozirgi vaqtgacha hal qilinishi qiyin bo‘lgan masalalardan biridir. Ushbu ilmiy ishda maxfiy xabarlarni yashirish usullari, inson faoliyatidagi ahamiyati hamda usullarning bir biridan farqlari keltirib o‘tiladi. Shu bilan birga dessetatsiya mavzusida ko‘zda tutilgan, steganografiya usulini o‘z ichiga olgan va xabarlar maxfiyligini ta’minlab beradigan dasturiy ta’minot ishlab chiqildi. Axborot uzluksiz almashinib, uzatilayotgan bugungi o‘zaro bog’liq dunyoda uning maxfiyligi va yaxlitligini ta’minlash ustuvor vazifaga aylandi. Shu sababli bugungi kunda axborotning maxfiyligini saqlash juda muhim va maxfiylikni ta’minlab beruvchi dasturiy ta’minotlarga ehtiyoj juda yuqori. Ushbu maqola ham aynan shu muammoga qaratilgan.

Kalit so‘zlar: axborot, steganografiya, maxfiylik, kriptografiya, himoya, LACK, RSTEG.

Annotation. This work is dedicated to one of the important functions of cryptography - steganography. The problem of reliable protection of information from unauthorized access is one of the oldest and still difficult to solve problems. In this scientific work, the methods of hiding secret messages, their importance in human activity, and the differences between the methods are mentioned. At the same time, software has been developed that includes the steganography method and ensures the confidentiality of messages. In today's interconnected world, where information is constantly exchanged and transmitted, ensuring its confidentiality and integrity has become a priority. That's why the privacy of information is very important today, and the need for privacy-enhancing software is very high. This article is also focused on this problem.

Keywords: information, steganography, confidentiality, cryptography, protection, LACK, RSTEG

Аннотация. Данная работа посвящена одной из важных функций криптографии – стеганографии. Проблема надежной защиты информации от несанкционированного доступа является одной из древнейших и до сих пор

ISSN 3030-3907

трудноразрешимых. В данной научной работе рассматриваются методы сокрытия секретных сообщений, их значение в деятельности человека и различия между методами. В то же время разработано программное обеспечение, включающее метод стеганографии и обеспечивающее конфиденциальность сообщений. В современном взаимосвязанном мире, где информация постоянно обменивается и передается, обеспечение ее конфиденциальности и целостности стало приоритетом. Именно поэтому конфиденциальность информации сегодня очень важна, и потребность в программном обеспечении, повышающем ее конфиденциальность, очень высока. Данная статья также посвящена этой проблеме.

Ключевые слова: информация, стеганография, конфиденциальность, криптография, защита, LACK, RSTEG

Kirish

Axborot uzluksiz almashinib, uzatilayotgan bugungi o‘zaro bog’liq dunyoda uning maxfiyligi va yaxlitligini ta’minlash ustuvor vazifaga aylandi. Shunday qilib, axborot xavfsizligi muhim soha sifatida paydo bo‘ldi va maxfiy ma’lumotlarni ruxsatsiz kirish yoki ushlashdan himoya qilishning turli usullarini o‘z ichiga oladi. Katta e'tiborga sazovor bo‘lgan bunday usullardan biri steganografiyadir. Hozirgi kunda xabarlarni yashirish, uning mavjudligini himoyalash qiyin masala bo‘lib bormoqda. Aynan shu sababli mazkur maqola mavzusi hozirgi kundagi eng dolzarb masalalardan hisoblanadi [1-3].

Xabarni ruxsatsiz shaxslar uchun tushunarsiz qilishga qaratilgan kriptografiyadan farqli o‘laroq, steganografiya xabarning mavjudligini qabul qiluvchi bo‘lmaganlar uchun noma’lum qilishga qaratilgan.

Steganografiyaning asosiy maqsadi yashirin ma’lumotni samarali joylashtirish. Inson sezgilarining sezilmasligi va raqamli fayllarda mavjud bo‘lgan ortiqcha narsalardan foydalangan holda, steganografiya yopiq obyektlarining ko‘rinishi va funksionalligini saqlab, nozik ma’lumotlarni yashirin ravishda uzatish imkonini beradi.

Global kompyuter tarmoqlari va multimedia soxasidagi zamonaviy progress telekommunikatsiya kanallarida ma’lumotlarni uzatish xavfsizligini ta’minlash uchun mo‘ljallangan yangi usullarni yaratishga olib keldi. Bu usullar shifrlash qurilmalarining tabiiy noaniqligidan va analogli video yoki audiosignallarning ko‘pligidan foydalanib, xabarlarni kompyuter fayllari (konteynerlar)da yashirish imkonini beradi. Shu bilan birga kriptografiyadan farqli ravishda bu usullar axborotni uzatish faktining o‘zini ham yashiradi.

K.Shennon sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida steganografiyaning bazasi hisoblanadi. Zamonaviy kompyuter steganografiyasida ikkita asosiy fayl turlari mavjud: yashirish uchun mo‘ljallangan xabar-fayl, va

ISSN 3030-3907

konteynerfayl, u xabarni yashirish uchun ishlatilishi mumkin. Bunda konteynerlar ikki turda bo‘ladi:

konteyner-original (yoki «bo‘sh» konteyner) - bu konteyner yashirin axborotni saqlamaydi;

konteyner-natija (yoki «to‘ldirilgan» konteyner) — bu konteyner yashirin axborotni saqlaydi.

Kali sifatida xabarni konteynerga kiritib qo‘yish tartibini aniqlaydigan maxfiy element tushuniladi.

Kompyuter steganografiyasining asosiy holatlari quyidagilardan iborat:

- yashirish usullari faylning autentifikatsiyalanishligini va yaxlitligini ta’minlashi kerak;
- yovuz niyatli shaxslarga qo‘llaniluvchi steganografiya usullari to‘liq ma’lum deb faraz qilinadi;
- usullarning axborotga nisbatan xavfsizlikni ta’minlashi ochiq uzataladigan faylning asosiy xossalarini stenografik almashtirishlar bilan saqlashga va boshqa shaxslarga noma’lum bo‘lgan qandaydir axborot — kalitga asoslanadi;
- agar yovuz niyatli shaxslarga xabarni ochish vaqti ma’lum bo‘lib qolgan bo‘lsa, maxfiy xabarning o‘zini chiqarib olish jarayoni murakkab xisoblash masalasi sifatida tasavvur qilinishi lozim.
- konfidentsial axborotni ruxsat etilmagan kirishdan himoyalash;
- monitoring va tarmoq zaxiralarini boshqarish tizimlarini yengish;
- dasturiy ta’minotni niqoblash;
- intellektual egalikning ba’zi bir turlarida mualliflik huquqlarini himoyalash.[4, 5]

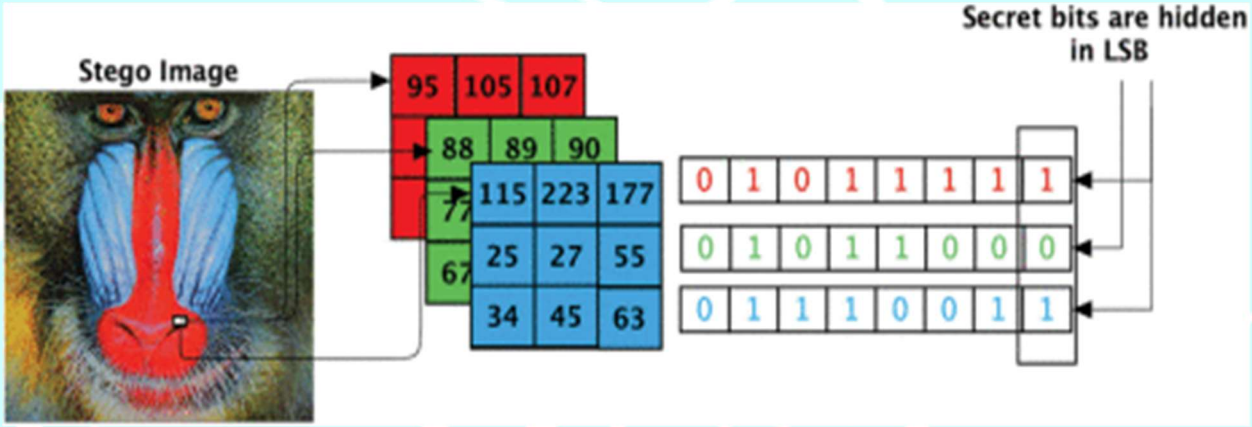
Tadqiqot maqsad va vazifalari:

- axborot xavfsizligida ma’lumotlarni himoyalashning steganografik usullari, metodlari va ularning bir-biridan farqlarini ko‘rsatish.
- axborotni stenografik va kriptografik himoyalash va ularni tahlil qilish;
- axborotni stenografik himoyalash usullari va yo‘nalishlarini o‘rganish;
- axborotni stenografik himoyalashga oid usullarni o‘rganish va qo‘llab ko‘rish.

Steganografiya keng tarqalgan bo‘lib, qo‘llaniladigan bir nechta yo‘nalishlar mavjud. Bularga quyidagilarni misol qilish mumkin:

Tasvir steganografiyasi: Bu raqamli tasvirlar ichida ma’lumotlarni yashirishni o‘z ichiga oladi. Yashirin ma’lumotlar rang qiymatlarini yoki tasvirdagi piksellarning eng kam ahamiyatli bitlarini (LSB) nozik o‘zgartirish orqali kiritiladi. Ushbu uslub LSBdagi kichik o‘zgarishlarni ko‘pincha inson ko‘zi sezib bo‘lmasligi, lekin maxsus algoritmlar yordamida aniqlanishi va olinishi mumkinligidan foydalanadi.

ISSN 3030-3907



1-rasm. Tasvirga maxfiy habarni yashirish.

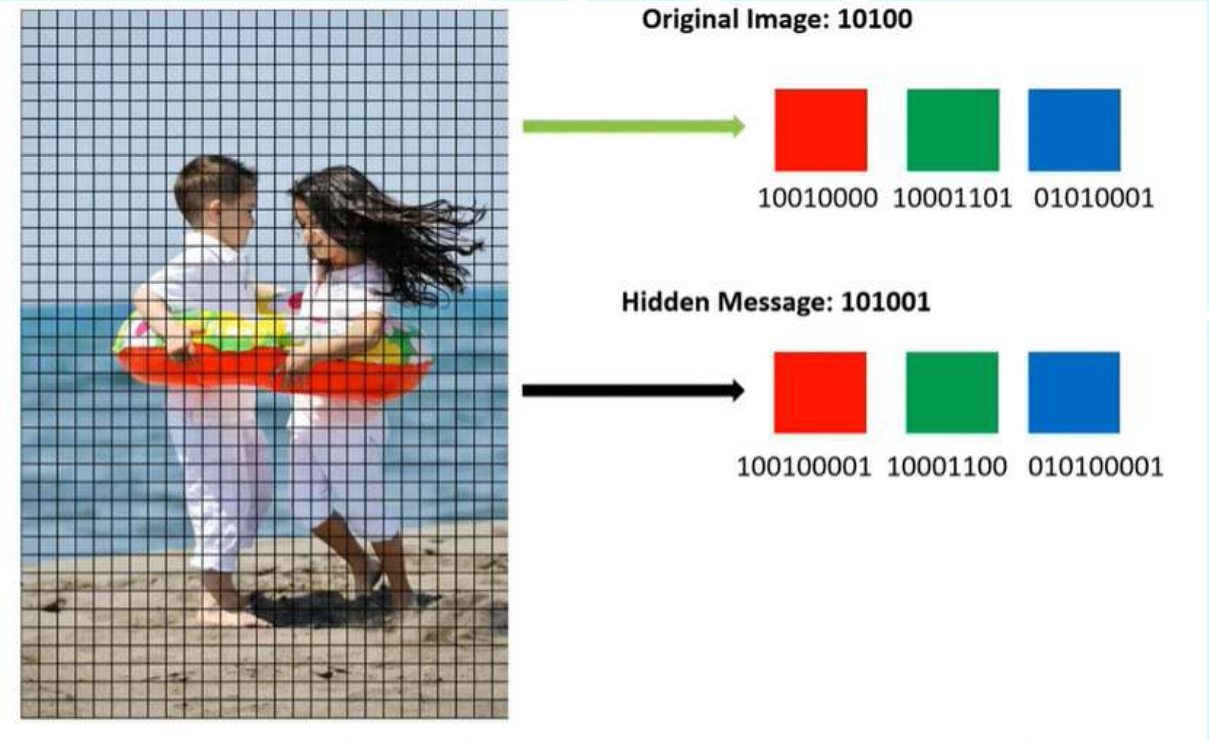
Audio steganografiya: Tasvir steganografiyasiga o‘xshash audio steganografiyasi audio fayllar ichidagi ma’lumotlarni yashiradi. Texnika ovoz namunalariga yashirin ma’lumotlarni qo‘shish yoki chastota spektri yoki faza kabi audioning ma’lum xususiyatlarini o‘zgartirish orqali audio to‘lqin shaklini manipulyatsiya qilishni o‘z ichiga oladi.

Video steganografiya: Video steganografiya video fayllar ichidagi ma’lumotlarni yashiradi. Bu harakat vektorlari yoki rang komponentlari kabi video oqimining muayyan ramkalarini yoki muayyan xususiyatlarini o‘zgartirish orqali amalga oshirilishi mumkin. Ushbu usul yashirin ma’lumotlarni joylashtirish uchun video ma’lumotlarning vaqtinchalik ortiqcha va murakkabligidan foydalanishi mumkin.

Rasm steganografiyasi: Bu steganografiyaning eng mashhur va keng qo‘llaniladigan shakllaridan biridir. Bu raqamli tasvirlar ichida ma’lumotlarni yashirishni o‘z ichiga oladi. Yashirin ma’lumot tasvir piksellarining eng kam ahamiyatli bitlariga joylashtirilishi yoki ma’lumotlarni kodlash uchun rang qiymatlarini biroz o‘zgartirish orqali kiritilishi mumkin.

Matn steganografiyasi: Matn steganografiyasi matn hujjatlaridagi ma’lumotlarni yashiradi. U ko‘rinmas belgilardan foydalanish, formatlash yoki intervalni o‘zgartirish yoki matn ichidagi ma’lumotlarni yashirish uchun maxsus kodlash sxemalarini qo‘llash kabi turli xil usullarni o‘z ichiga olishi mumkin.

ISSN 3030-3907



2-rasm. Maxfiy habarni yashirish uchun tasvirda pixellarni o‘zgartirish.

Audio steganografiya - bu audio fayllar ichida maxfiy ma’lumotlarni yashirish amaliyotidir. Tasvir steganografiyasiga o‘xshab, maqsad maxfiy ma’lumotlarni inson tinglovchilari uchun sezilmaydigan tarzda joylashtirishdir. Bunga erishish uchun turli xil texnikalardan foydalanish mumkin, jumladan:

Exo yashirish: Exo yashirish yashirin ma’lumotlarni yetkazish uchun eshitilmaydigan aks-sadolarni yoki audio signaldagi kechikishlarni kiritishni o‘z ichiga oladi. Steganografiyadan foydalaniladigan yana bir sohalardan biri — bu mualliflik huquqlarini himoyalash hisoblanadi. Kompyuterli grafik tasvirlarga maxsus belgi qo‘yiladi va u ko‘zga ko‘rinmay qoladi. Lekin, maxsus dasturiy ta’minot bilan aniqlanadi. Bunday dastur mahsuloti allaqachon ba’zi jurnallarning kompyuter versiyalarida ishlatilayapti. Steganografiyaning ushbu yo‘nalishi nafaqat tasvirlarni, balki audio va videoaxborotni ham qayta ishlashga mo‘ljallangan. Bundan tashqari uning intellektual egaligini himoyalashni ta’minlash vazifasi ham mavjud.

LSB (Least Significant Bit) usuli. Eng oddiy va samarali usul. Rasmning har bir pikselining eng kichik bitlari (LSB) ma’lumot bitlari bilan almashtiriladi. Masalan, piksel (10110100) → (10110101) ga o‘zgaradi, ammo inson ko‘zi buni seza olmaydi. Formulaviy ko‘rinish:

$Si=(Ci-(Cimod\ 2))+MiS_i = (C_i - (C_i \mod 2)) + M_iSi=(Ci−(Cimod2))+Mi;$

bu yerda **S** — stegopiksel, **C** — original piksel, **M** — yashirilgan bit.[2]

Steganografiya tarmoqlari. LACK va RSTEG usullari tahlili. Steganografiya raqamli kutubxonalar va bulutli omborlardagi materiallarni raqamli belgilash uchun ishlatilishi mumkin. Steganografik biriktirma hatto ma’lum

ISSN 3030-3907

darajada elektron imzo o‘rnini bosishi mumkin, chunki u uzatilgan ma’lumotning yaxlitligini isbotlash imkonini beradi. Boshqa tomondan, steganografiya yordamida tajovuzkor tarmoqda o‘rnatilgan barcha filtrlarni chetlab o‘tib, maxfiy ma’lumotlarni ochiq aloqa kanallari orqali uzatishi mumkin. Shuning uchun bugungi kunda steganografiya va stegoanaliz usullari ayniqsa diqqat bilan o‘rganishni talab etadi. Tarmoq steganografiyasi katta hajmdagi ma’lumotlarni real vaqtda yashirib uzatish imkonini beradi. Tarmoq steganografiyasi paketini modifikatsiyalash, paketlarni uzatilayotganda strukturasini modifikatsiyalash va gibrid(aralash) usullarga bo‘linadi.[3]

Tarmoq steganografiyasining paketlar modifikatsiyalash usullarining asosiy g’oyasi steganogramma qo‘shish uchun sarlavha maydonlarini o‘zgartirishga asoslanadi. Buni amalga oshirishda maydonlardagi ba’zi ortiqcha foydalanilmaydigan jaylardan, ya’ni paketlarni uzatishda ahamiyatga ega bo‘lmagan maydonlardan foydalaniladi. Eng ko‘p ishlatiladigan sarlavha maydonlari IP va TCP protokollari tarkibida mavjud.

VoIP protokoli imkoniyatlaridan foydalanib xabarni yashirin uzatish usullaridan yana biri LACK (Lost Audio Packets Steganography) hisoblanadi. IP-telefoniya orqali aloqa ikki qismdan signal (xizmat) va suhbatdan iborat bo‘ladi. Ikkala qismda ham ma’lumotlar har ikki yo‘nalishda ham uzatiladi. Signal uzatish uchun SIP (Session Initiation Protocol) va suhbatni amalga oshirish uchun RTP (Real-time Transport Protocol) protokollaridan foydalaniladi. Bu shuni anglatadiki, qo‘ng‘iroqning signalizatsiya bosqichida foydalanuvchi agentlar SIP xabarlarini almashadilar. Odatda, SIP xabarlari SIP serverlari orqali o‘tadi va foydalanuvchilarga bir-birini qidirish va topish imkonini beradi. Ulanish o‘rnatilgandan so‘ng, suhbat bosqichi boshlanadi va bu yerda RTP audio oqimi qo‘ng‘iroq qiluvchilar o‘rtasida har ikki yo‘nalishda ovozli xabar almashishni ta’minlaydi. Ovozli xabarlaga maxfiy ma’lumotlarni samarali yashirish usullaridan biri LACK hisoblanadi. LACK usulining ishlash prinsipiga ko‘ra transmitter ovozli oqim paketlaridan birini tanlaydi va uning foydali yukini maxfiy xabarning bitlari bilan almashtiriladi. Keyin tanlangan paket ataylab kechiktiriladi. Har safar haddan tashqari kechiktirilgan paket steganografik protsedura bilan tanish bo‘lmagan qabul qiluvchiga yetib borganida, u yo‘q qilinadi. Biroq, agar qabul qiluvchi yashirin ulanish haqida bilsa, u qabul qilingan RTP paketlarini o‘chirish o‘rniga ularni qabul qiladi va yashirib uzatilgan ma’lumotga ega bo‘ladi. Qasddan yo‘qotishlarni keltirib chiqarganda aloqa sifati yomonlashadi. Bu esa oddiy foydalanuvchilarda ham, tinglovchi kuzatuvchilarda ham shubha uyg‘otishi mumkin. LACK usulining stegoanalizining taqdim etilgan natijalariga asoslanib, ushbu usul o‘rtacha aniqlash murakkabligiga ega degan xulosaga kelish mumkin.

ISSN 3030-3907

Bu usuldan foydalanish juda murakkab va ba’zi operatsion tizimlarda amalga oshirilmasligi mumkin

LACK usuli haqida keltirilgan ma’lumotlardan ko‘rish mumkinki, uzatlayotgan ovozli paketga maxfiy ma’lumotni yuklash va uni oddiy foydalanuvchiga bildirmaslik maqsadida ataylab kechiktiriladi. Bunda uzatilayotgan paketga to‘liq maxfiy ma’lumotni yuklash imkoniyati LACK usulining maxfiy ma’lumotlarni tarmoqda uzatilishining samaradorligini ta’minlaydi. Sababi uzatilayotgan paketga to‘liq maxfiy ma’lumotni yashirib uzatish imkoniyati mavjud. Paketlarni qayta uzatish mexanizmiga asoslangan steganografik usullardan yana biri RSTEG (Retransmission Steganography) hisoblanadi.

RSTEG usulida dastlab ma’lumot yuboruvchi paketni jo‘natadi, lekin qabul qiluvchi tasdiq(ACK) paketi bilan javob bermaydi. Natijada paketlarni qayta jo‘natish mexanizmi ishga tushadi. Qayta jo‘natish paytida paket ichiga steganogramma joylashtirib uzatiladi. Qabul qiluvchi ichida steganogramma mavjud paketni qabul qiladi, lekin yana tasdiq(ACK) paketini yuboruvchiga jo‘natmaydi. Yana paketlarni qayta jo‘natish mexanizmi ishga tushganda asl paket qo‘shimchalarsiz uzatiladi va qabul qiluvchi ma’lumotni olgandan so‘ng tasdiq(ACK) paketini yuboruvchiga jo‘natadi. Natijada tasdiq(ACK) paketini yuborilmasdan qayta uzatilganda ma’lumotlar steganografik yashirib uzatiladi. RSTEG usulining unumdorligi paket yuki hajmi va segmentlar hosil bo‘lish chastotasiga bog’liq hisoblanadi. Steganografiyaning haqiqiy usullaridan hech biri mukammal emas. Qanday usul bo‘lishidan qat’i nazar, yashirin ma’lumotni aniqlash mumkin. Ma’lumotlar oqimiga qancha yashirin ma’lumot kiritilsa, uni stegoanaliz qilish usullari bilan aniqlash ehtimoli shunchalik yuqori bo‘ladi. Bundan tashqari, yashirin ma’lumotlarni yuborish uchun qancha paketlar ishlatilsa, aniqlash chastotasi ortadi. Yashirin aloqa kanalini aniqlashni sezilarli darajada osonlashtiradigan vositalar relayli paketlar hisoblanadi.

RSTEG gibrid usul hisoblanadi. Shuning uchun uning steganografik o‘tkazuvchanligi taxminan paketlarni o‘zgartirish usullarining o‘tkazuvchanligiga teng va shu bilan birga paketlarni qayta tartiblash usullaridan yuqori. Aniqlash va o‘tkazishning murakkabligi to‘g‘ridan-to‘g‘ri usulni amalga oshirish uchun ishlatiladigan mexanizmga bog‘liq. RTO(Recovery Time Objective) asosidagi RSTEG usuli aniqlanishning yuqori murakkabligi va past o‘tkazish qobiliyati bilan tavsiflanadi. Xuddi shu usulga asoslangan SACK (Selective acknowledgment RSTEG uchun maksimal o‘tkazish qobiliyatiga ega, ammo uni aniqlash oson. RSTEG usuli TCP/IP protoklida ishlatish uchun juda mos keladi va o‘rtacha darajadagi uzatish bilan bu usul kuzatuvchida shubha uyg‘otmaydi. Ammo bu usulni amalga oshirish juda qiyin, ayniqsa uning oddiy foydalanuvchilarning

ISSN 3030-3907

paketlarini ushlash va tuzatishga asoslangan algoritmlari. O‘tkazilayotgan paketlar chastotasining keskin oshishi yoki uzatishda g‘ayrioddiy kechikishlarning paydo bo‘lishi tufayli steganogrammalar tashqi kuzatuvchida shubha tug‘dirishi mumkin.[4]

Xulosa. Stegoanaliz qilingan yashirin axborot oshkor bo‘lishi mumkin. Ushbu holatda maxfiy habar oshkor bo‘lmasligi uchun steganografik usullar bilan kriptografik algoritmlarni birga qo‘llash yashirin uzatilgan xabarlarni oshkor bo‘lishini qiyinlashtiradi.Tahlil natijalari shuni ko‘rsatdiki, tarmoq steganografiyasining gibrid usullaridan bo‘lgan RSTEG va LACK usullarining axborotni yashirib uzatish qobiliyati yuqori lekin aniqlashning aniqlik darajasi yuqori emas. Steganografik biriktirma hatto ma’lum darajada elektron imzo o‘rnini bosishi mumkin, chunki u uzatilgan ma’lumotning yaxlitligini isbotlash imkonini beradi. Boshqa tomondan, steganografiya yordamida tajovuzkor tarmoqda o‘rnatilgan barcha filtrlarni chetlab o‘tib, maxfiy ma’lumotlarni ochiq aloqa kanallari orqali uzatishi mumkin. Shuning uchun bugungi kunda steganografiya va stegoanaliz usullari ayniqsa diqqat bilan o‘rganishni talab etadi. Tarmoq steganografiyasi katta hajmdagi ma’lumotlarni real vaqtda yashirib uzatish imkonini beradi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. И.Х.Норматов, Н.С.Джумагулов, Е.Н.Жолбарыс Методы разработки, хранения и обучения моделей на основе текстовой информации в образовании// Journal Development of science Sentyabr 2025/9 Issue 9. Volume 2, C. 85-95, ISSN 3030-3907.
2. Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari universiteti professorlari S.K. Ganiyev, A.A. Ganiyev, Z.T. Xudoyqulov “Kiberxavfsizlik asoslari” o‘quv qo‘llanma// Aloqachi - 2020 yil, 303 bet
3. Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь, Вилкина К. А., студент гр.253504, Клебеко Е. Ю., студент гр.253504 Носкович П. Н., студент гр.253504 “ Стеганографические Методы Защиты Информации”
4. Абазина Е. С., Ерунов А. А. “ Цифровая стеганография: состояние и перспективы” Системы управления, связи и безопасности №2. 2016URL: http://sccs.intelgr.com/archive/2016-02/07-Abazina.pdf, С.182-201.
5. Sh. Mamagapurova “Steganography techniques and types of stenography”, (master’s degree of National University of Uzbekistan named after Mirzo Ulug’bek) “Sun’iy intellekt nazariyasi va amaliyoti: tajribalar, muammolar va istiqbollar respublika ilmiy-amaliy konferensiyasi” maqolalar to‘plami (1-qism) Toshkent “Iqtisodiyot” 2024, 162-168 betlar