O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA TELEKOMMUNIKATSIYALARNI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI SAMARQAND FILIALI

«Axborot xavfsizligi» kafedrasi

5330500 - « Kompyuter injiniringi » yo‘nalishi

"Himoyaga ruxsat"

"Axborot xavfsizligi" kafedrasi

Mudiri Bekmurodov U.B.

“_____”_____ 2018 yil.

“Axborotlarni rasm ma`lumotlarida berkitish dasturini ishlab chiqish ” mavzusida

BITIRUV MALAKAVIY ISHI

Bitiruvchi	_____	Toshtemirov J.M.
	(imzo)	(F.I.Sh)
Rahbar	_____	Mavlonov O.N.
	(imzo)	(F.I.Sh)
Taqrizchi	_____	Axatov A.R.
	(imzo)	(F.I.Sh)
HFX bo‘yicha	_____	Qurbanniyazov A.S
maslaxatchi	(imzo)	(F.I.Sh)

SAMARQAND - 2018

MUNDARIJA

KIRISH

O’zbekiston Respublikasi Prezidenti Sh.M.Mirziyoyevning 2017 yil 20 apreldagi «Oliy ta’lim tizimini yanada rivojlantirish chora-tadbirlari to’g’risida» PQ-2909 sonli qarori Respublikamizda oliy ta’lim tizimida ilmiy tadqiqotlarni yanada rivojlantirish, iqtidorli talaba-yoshlarni ilmiy faoliyat bilan shug’ullanishga jalb etishda yana bir muhim bosqich bo’lib qoladi.

Bugungi kunda axborot texnologiyalari sohasidagi o’zgarishlar ko’z ilg’amas darajada tez sodir bo’lmoqda, shunday ekan AKT sohasida faoliyat ko’rsatuvchi mutaxasislar hamda zamonaviy kompyuter vositalaridan foydalanuvchilar e’tiborini jalb etmoqda[1] .

Mamlakatimiz iqtisodiy siyosatida axborot muhim o’rin egallaydi. Banklar, korxonalar va boshqa iqtisodiy sektordagi tashkilotlar, ya’ni soliq tizimi, nodavlat fondlar, sug’urta agentliklari uchun axborotning o’zgarishi juda tez amalga oshadi hamda hajmi tez ortadi. Ular asosida turli tahlillar o’tkazilib, yechimlar qabul qilinadi, vazifalar belgilanadi, taktika va strategiya ishlab chiqiladi. Bu axborotlar bevosita fuqarolar, iqtisodiyotimiz taqdiri, qolaversa siyosatimiz asosini tashkil yetishini unutmasligimiz kerak.

.1993-yil 7-mayda qabul qilingan “Axborotlashtirish to‘g‘risida”gi qonun 2003-yil 11-dekabrda Oliy Majlisning sessiyasida kayta ko‘rib chiqilgan va u 23 moddadan iborat. Bu qonunga ko‘ra axborot resurslari va axborot tizimlarining texnika vositalarini sertifikatlashtirish, axborot tizimlarining tarmoqlararo bog‘lanishini amalga oshirish, axborot resurslari va axborot tizimlarini muxofaza qilish, xalqaro axborot tarmoqlaridagi ulanishni amalga oshirish, nizolarni xal etish, axborotlashtirish to‘g‘risidagi qonun xujjatlarini buzganlik uchun javobgarlik nazarda tutilgan [1].

Axborot xavfsizligi nazarda tutilgan qonunlardan yana biri bu “Elektron raqamli imzo to‘g‘risida”gi qonundir. Bu qonun 2003-yil 11-dekabrda Oliy Majlis sessiyasida qabul qilingan bo‘lib, u 22 moddani o‘z ichiga oladi.

1994 yil 6-mayida «Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma’lumotlar bazalarining huquqiy himoyasi to‘g‘risida»gi Qonun ishlab chiqilgan, bunda yaratilayotgan dasturiy vositalarning huquqiy tomonidan himoyalash chora-tadbirlari keltirilgan.

Bundan tashqari 1997 yil, 24-aprelda «Axborot olish kafolatlari va erkinligi to‘g‘risida»gi Qonun, 2006 yil, 4-aprelda «Avtomatlashtirilgan bank tizimida axborotni muhofaza qilish to‘g‘risida»gi Qonunlari qabul qilindi.

Axborotning kriptografik himoya usullari hozirda juda ishonchli vositalardan biri sanalib, xususan ma’lumotlarni yashirish usullari, stegonografiya usullariga bo‘lgan talab so‘ngi yillarda ortdi. Buning asosiy sababi, stegonografik usullarini amalga oshirish uchun kam resurs talab etishidir

Bitiruv malakaviy ishining maqsadi va vazifalari: Ushbu bitiruv malakaviy ishining maqsadi rasm ma’lumotlarda maxfiy axborotlarni yashirish usullarini tahlil etish bo‘lib, uni bajarishda quyidagi vazifalar qo‘yildi:

- Axborotni kriptografik himoyalash usullarini tadqiq etish;
- Axborotni stegonografik yashirish usullarini tadqiq etish;
- Stegonogrfik himoya sohasida mavjud xavfsizlik muammolarini aniqlash va ularni bartaraf etish usullarini tahlil etish;
- Rasm ma’lumotlarda axborotlarni yashirish usullarini tahlil etish;
- Rasm ma’lumotlarda axborotlarni yashirishning ishonchli usulini taklif etish.

Mazkur bitiruv malakaviy ish kirish, uchta asosiy bo‘lim, xulosa va foydalanilgan adabiyotlardan iboratdir.

Kirish qismida bitiruv malakaviy ishining dolzarbligi, ishning maqsadi keltirib o‘tilgan.

Nazariy qismda axborotning kriptografik va stegonografik usullari tahlil etildi.

Asosiy qismlarda esa rasm ma’lumotlarda axborotlarni yashirish usullari tahlil etildi va ular asosida ishonchli usul taklif etildi. Taklif etilgan usulning dasturiy ta’minoti ishlab chiqildi.

I BOB. AXBOROTNING KRIPTOGRAFIK VA STEGONOGRAFIK HIMOYA USULLARI

1.1. Axborotning kriptografik himoyasi

Axborotni qayta akslantirish yordamida himoyalash muammosi inson ongini uzoq vaqtlardan buyon bezovta qilib kelgan. Kriptografiya tarixi – inson tili tarixi bilan tengdosh. Hatto dastlabki xat yozish ham o‘z-o‘zicha kriptografik tizim hisoblangan, chunki qadimgi jamiyatda faqat alohida shaxslargina xat yozishni bilganlar. Qadimgi Yegipet va Qadimgi Hindistonning ilohiy kitoblari bunga misol bo‘la oladi [4].

Xat yozishning keng tarqalishi natijasida kriptografiya alohida fan sifatida vujudda keldi. Dastlabki kriptotizimlardan eramizning boshlaridayoq foydalanilgan. Sezar o‘z xatlarida tizimli shifrlardan foydalangan.

Kriptografiya – so‘zi grek tilidan olingan bo‘lib, “maxfiy yozish” degan ma’noni anglatadi. Umumiy qo‘lanilishiga ko‘ra mazkur tushuncha biror ma’lumotni maxfiy saqlash va himoyalash demakdir.

Bugungi kunda axborotlarning muhofazasini ta’minlashning turli usullari mavjud bo‘lib, masalan ma’lumotni ishonchli seyfda saqlash va ushbu ma’lumot bilan tanishishi mumkin bo‘lgan shaxslar sonini cheklab qo‘yish, qa’tiy qo‘riqlanadigan binolardan foydalanish mumkin. Axborotlarni bunday muhofazalash usularining qulaylik tomonlari bilan birga noqulayliklari ham bo‘lib, bu noqulayliklar axborotlar almashinuvi jarayonida namoyon bo‘ladi. Shuningdek, axborotlarni muhofazasini ta’minlash usullari qatoriga quyidagilarni ham keltirish mumkin:

- axborot uzatilayotgan aloqa tarmog‘ini muhofazalash;
- uzatilayotgan maxfiy ma’lumotni ochiq aloqa tarmog‘ida boshqa biror ochiq ma’lumot bilan niqoblab (aralashtirib) muhofazalash, ya’ni stegonografik usullardan foydalanish;
- asl ma’nosi maxfiy bo‘lgan oldindan kelishib olingan ochiq ma’lumotlarni o‘zaro abonentlar o‘rtasida almashish orqali;

- ochiq aloqa tarmog‘ida uzatilayotgan ma’lumotning kriptoanalitik tomonidan qo‘lga kiritilishini qiyinlashtirish, ya’ni ma’lumotni keng polosali aloqa tarmog‘ida maxsus usullarda, signallarni shovqin qo‘shib uzatish orqali.

Kriptografik tizimlar birinchi va ikkinchi jahon urushlarida jadal rivojlandi. Urush yillaridan so‘ng va hozirga qadar hisoblash vositalarining jadal rivojlanishi kriptografik usullar yaratishni tezlashtirdi va ularning mukammalligini oshirdi.

Bir tomondan, kompyuter tarmoqlaridan foydalanish kengaydi, jumladan, Internet global tarmog‘i. Bu tarmoqda begona shaxslardan himoyalanishi zarur bo‘lgan hukumat, harbiy, tijorat va shaxsiy xarakterga ega bo‘lgan axborotning katta hajmi harakatlanadi.

Boshqa tomondan, qudratli kompyuterlar, tarmoqli va neyronli hisoblash texnologiyalarining paydo bo‘lishi ochish mumkin emas deb hisoblangan kriptografik tizimlarning obro‘siga putur yetkazdi.

Shifrlarning kriptografik xossalarini tashkil etuvchi: kriptohujumlarga bardoshliligi, axborot-kommunikatsiya tarmoqlarida qo‘llanishi samaradorligi, elekton qurilmalarining yaratilishini qulayligi kabi masalalarni tahlil qilish bilan shug‘ullanuvchi fan turiga **kriptotahlil** deb yuritiladi. Ushbu termin fanga 1920 yilda buyuk matematik U. Fridman tomonidan kiritilgan.

Kriptografiya va kriptotahlil birlashtiruvchi(fan) bilim sohasiga **kritpologiya** deyiladi [4].

Shunday qilib, kriptografiya va kriptotahlil bir-birlari bilan uzviy ravishda bog‘liq bo‘lgan fan yo‘nalishlaridir, ya’ni har qanday himoyalanishni chuqur kriptotahlil qilmasdan amalga oshirish mumkin emas.

Kriptologiya – axborotni qayta akslantirib himoyalash muammosi bilan shug‘ullanadi (*kryptos* – maxfiy, sirli, *logos* - fan). Kriptologiya ikki yo‘nalishga bo‘linadi – *kriptografiya* va *kriptoanaliz*. Bu ikki yo‘nalishning maqsadlari qarama-qarshi [4].

Kriptografiya – axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi.

Kriptoanaliz – kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi.

Bu kitobda asosiy e’tibor kriptografik usullarga qaratilgan.

Zamonaviy kriptografiya quyidagi to‘rtta bo‘limlarni o‘z ichiga oladi [4]:

1. Simmetrik kriptotizimlar.
2. Ochiq kalitli kriptotizimlar.
3. Elektron imzo tizimlari.
4. Kalitlarni boshqarish.

Kriptografik usullardan foydalanishning asosiy yo‘nalishi – maxfiy axborotning aloqa kanalidan uzatish (masalan, elektron pochta), uzatiladigan xabarning uzunligini o‘rnatish, axborotni (hujjatlarni, ma’lumotlar bazasini) shifrlangan holda raqamli vositalarda saqlash.

Shunday qilib, kriptografiya axborotni shunday qayta ishlash imkonini beradiki, bunda uni qayta tiklash faqat kalitni bilgandagina mumkin.

Shifrlash va deshifrlashda qatnashadigan axborot sifatida biror alifbo asosida yozilgan matnlar qaraladi. Bu terminlar ostida quyidagilar tushuniladi [5].

Alifbo – axborot belgilarini kodlash uchun foydalaniladigan chekli to‘plam.

Matn – alifbo elementlarining tartiblangan to‘plami.

Zamonaviy ATlarida qo‘llaniladigan alifbolarga misol sifatida quyidagilarni keltirish mumkin:

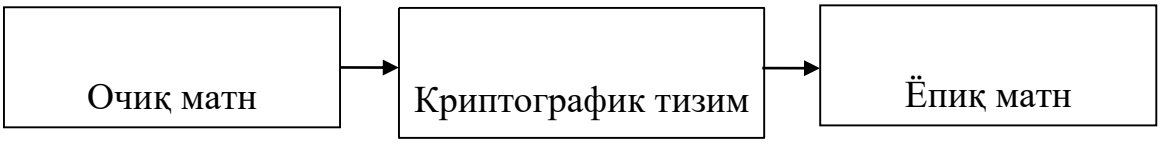
- Z_{33} alifbosi – rus alifbosining *32* harflari va bo‘sh joy belgisi;
- Z_{256} alifbosi – *ASCII* va *KOI-8* standart kodlariga kiruvchi belgilar;
- Binar alifbo - $Z_2=\{0, 1\}$
- Sakkizlik yoki o‘n oltilik alifbolar.

Shifrlash – akslantirish jarayoni: ***ochiq matn*** deb ham nomlanadigan matn ***shifrmatnga*** almashtiriladi.

Deshifrlash – shifrlashga teskari jarayon. Kalit asosida shifrmatn ochiq matnga akslantiriladi.

Kalit – matnni shifrlash va shifrini ochish uchun kerakli axborot.

Kriptografik tizim – ochiq matnni akslantirishning *T* oilasini o‘zida mujassamlashtiradi. Bu oila a’zolari *k* bilan indekslanadi yoki belgilanadi. *k* parametr kalit hisoblanadi. *K* kalitlar fazosi – bu kalitning mumkin bo‘lgan qiymatlari to‘plami. Odatda kalit alifbo harflari ketma-ketligidan iborat bo‘ladi (1.1 - rasm).



1.1 – rasm. Kriptotizim tuzulishi

Kriptotizimlar simmetrik va ochiq kalitli tizimlarga bo‘linadi.

Simmetrik kriptotizimlarda shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi.

Ochiq kalitli kriptotizimlarda bir-biriga matematik usullar bilan bog‘langan *ochiq* va *yopiq* kalitlardan foydalaniladi. Axborot ochiq kalit yordamida shifrlanadi, ochiq kalit barchaga oshkor qilingan bo‘ladi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi, yopiq kalit faqat qabul qiluvchigagina ma’lum.

Kalitlarni tarqatish va ***kalitlarni boshqarish*** terminlari axborotni akslantirish tizimlari jarayoniga tegishli. Bu iboralarning mohiyati foydalanuvchilar o‘rasida kalit yaratish va tarqatishdir.

Elektron raqamli imzo deb – xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo‘shilgan qo‘shimchaga aytiladi. Elektron xujjatdagi mazkur elektron xujjat axborotini elektron rakamli imzoning yopik kalitidan foydalangan xolda maxsus uzgartirish natijasida xosil kilingan xamda elektron rakamli imzoning ochik kaliti yordamida elektron xujjatdagi axborotda xatolik yukligini aniklash va elektron rakamli imzo yopik kalitining egasini identifikatsiya kilish imkoniyatini beradigan imzo.

Uzatilayotgan ochiq ma’lumot ko‘rinishini almashtirish muammosi aloqa tarmog‘ida foydalanuvchilari o‘rtasida yechilishi kerak bo‘lgan masalaning bir tomoni bo‘lsa, ikkinchi tomoni - ma’lumotlar almashuvi amalga oshirilganda

uzatilayotgan va qabul qilib olinayotgan ma’lumotlarning hamda foydalanuvchilarning haqiqiyligiga ishonch hosil qilish.

Bu keltirilgan muammoni yechish uchun quyidagilarni:

- foydalanuvchilar va ma’lumotlarning haqiqiyligini tasdiqlash, tekshirish;
- o‘zaro muomalaga kirishib ma’lumot almashinuvchi tomonlarning bir-birlariga zarar keltirish yoki aldash maqsadida qasddan qiladigan har-qanday hatti harakatlarini qayd qilishni va oldini olishni ta’minlash zarur.

Mazkur muammolarni yechishda kriptografik usullar oldin bajarilgan har qanday hatti-harakatlarning inkor etilmasligini, yolg‘on ma’lumot uzatilganda esa uni aniqlash kabi imkoniyatlarni bera oladi. Demak, zamonaviy kritpografiya – axborotlarning aloqa tarmog‘ida almashinuvi jarayonlarida ularning [5]:

- maxfiyligini (konfidentsialligi ta’minlash);
- to‘liqligini (o‘zgartirilmagaligini aniqlash);
- autentifikatsiyasi (foydalanuvchilarning haqiqiyligini aniqlash);
- tomonlarning avtorlikni tan olmasligi kabi xolatlarning oldini olishni ta’minlash;
- kalitlarni yaratish, tarqatish va boshqarishni ta’minlash kabi masalalarni yechish bilan shug‘ullanuvchi bilim sohasi hisoblanadi.

HMAC tizimi MAS (message authentication code) ni hisoblashda kriptografik kalitdan foydalanilgan holdagi ko‘rinishidir. Ushbu tizimda ixtiyoriy xesh funktsiya algoritmlari foydalanilishi mumkin. Masalan, MD5, SHA1 va h.k. NMAS tizimlari unda foydalanilgan xesh funktsiyaga ko‘ra nomlanishi mumkin, masalan: NMAS-MD5 yoki NMAS- SHA1 [6].

NMAS tizimlarining kriptografik bardoshligi unda foydalanilgan xesh funktsiyaga, xesh funktsiyadan chiqadigan natija uzunligiga, kalit uzunligi va sifatiga bog‘liq.

Uning matematik ifodasi esa quyidagicha:

$$HMAC(K,m) = H((K \oplus opad) | H\big((K \oplus ipad) \big| m\big))$$

Bu yerda:

N – kriptografik xesh funktsiya;

K - maxfiy kalit, kalit uzunligi xesh funktsiya blok uzunligidan kichik bo‘lsa o‘ng tomondan “0” lar bilan to‘ldiriladi, uzun bo‘lsa kalitni xesh qiymati olinadi;

m autentifikatsiyalanuvchi ma’lumot;

| birlashtirish belgisi,

⊕ XOR amali;

opad tashqi qo‘shiluvchi qism (0x5s5s5s...5s5s ko‘rinishdagi uzunligi blok uzunligiga teng o‘zgarmas);

ipad ichki qo‘shiluvchi qism (0x363636...3636 ko‘rinishdagi uzunligi blok uzunligiga teng o‘zgarmas).

Bu keltirilgan masalalarning yechimlari ma’lumotlarni aloqa tarmog‘ida almashunuvi jarayonlari muhofazasini ta’minlab, kriptografiyaning asosiy masalalarini tashkil etadi.

Maxfiylikni ta’minlash - uzatilayotgan ma’lumot asl mazmuni (matni) bilan tanishish huquqi bo‘lmagan tomon yoki shaxslarning ushbu ma’lumotga ega bo‘lishiga qaratilgan hatti-harakatlari oldini olishni kafolatlash.

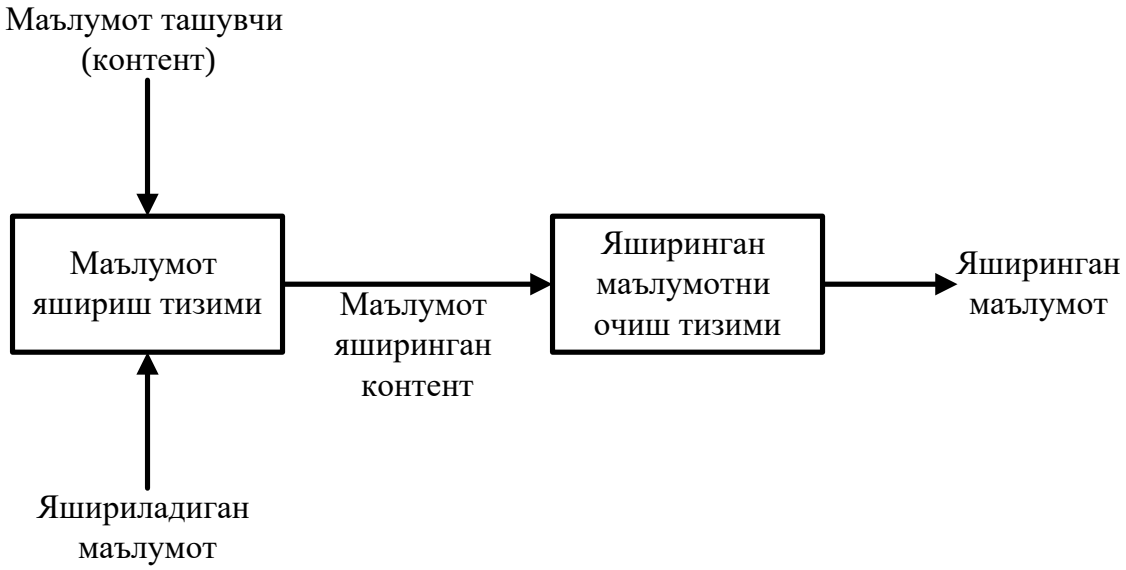
To‘lalikni ta’minlash- uzatilayotgan ma’lumotning (ruhsatsiz) o‘zgartirilishiga yo‘l qo‘ymaslikni kafolatlash.

Autentifikatsiyani ta’minlash - aloqa tarmog‘ida o‘zaro ma’lumot almashinuvi jarayonida tomonlarning haqiqiyligini (identifikatsiyasi) kafolatlash usullarni ishlab chiqish.

Tomonlarning avtorlikni tan olmasligi kabi xolatlarning oldini olishni ta’minlash - sub’ektlar tomonidan oldin amalga oshirilgan hatti-harakatlarini ma’lum vaqtdan so‘ng tan olmasliklari kabi holatlar oldini olishga qaratilgan chora tadbirlar.

1.2. Axborotning stegonografik himoyasi

Ma’lumotlarni yashirish (information hiding yoki data hiding) qadimdan foydalanilib kelingan va dolzarb bo‘lgan soha sanalgan. Ma’lumotlarni yashirish deganda kontent (rasmlar, qo‘shiqlar, videolar va hak.) ichida kerakli ma’lumotlarni yashirish tushuniladi. Bu yerda, yashirish tushunchasi, ma’lumotni sezilmaydigan ko‘rinishda keltirish yoki ma’lumot maxfiyligining mavjudligini saqlash uchun foydalaniladi. Qadimda turli ma’lumotlarni yashirish usullaridan foydalanilgan holda, ma’lum doiradagi odamlar orasida ma’lumotlar almashinilgan. Umumiy holda ma’lumotlari yashirish tuzulmasi quyidagicha [7]:



1.2-rasm. Ma’lumot yashirishning umumiy tuzilmasi

Yuqoridagi rasmda ko‘rsatilganidek, tuzilma ikki qismdan iborat: ma’lumotni yashirish (embedder) va yashiringan ma’lumotni ochish (Detector). Ma’lumotni yashirish tizimi ikkita kirishga, yashiriladigan ma’lumot va ushbu ma’lumotni tashuvchi ma’lumot (kontent) ega. Natijada esa, yagona ma’lumot yashiringan kontent hosil qilinadi. Yashiringan ma’lumotni ochish tizimi esa bitta kirishga ega bo‘lib, ma’lumot yashiringan kontentni qabul qiladi va undan yashiringan ma’lumotni ajratib oladi.

Odatda ma’lumotlarni yashirish sohasi ikkita katta qismga ajratiladi:

- Steganografiya;

- Watermarking (suv shaklidagi belgi).

Watermarking. Bu tushunchani aniqroq anglash uchun quyidagi misolni keltiramiz. Amerikaning 20 $ pulini olib, yoriqqa tutib, prezident Endryu Djekson rasmiga qaralsa, unda siz o‘ng tomonda ushbu rasmni bilinar-bilinmas (watermark) qilib aklanganini ko‘rishingiz mumkin. Ushbu watermark qog‘ozni tayorlash jarayonida unga qo‘shilgan va shuning uchun uni qalbakilashtirish murakkab [7].

1.3-rasm. Amerikaning 20 $ puli

Ushbu keltirilgan misolga tayanib, watermark quyidagi ikkita xususiyatga ega. Birinchisi, watermark odatiy ko‘rish jarayoni orqali ko‘rinishdan yashiringan, ya’ni maxsus ko‘rish jarayoni orqali uni ko‘rish mumkin (masalan, yoriqlikka tutish orqali). Ikkinchisi esa, watermark o‘zi yashiringan kontentga tegishli ma’lumotni saqlaydi (masalan, pulni qalbaki emasligini).

Bundan tashqari, watermarklarni fizik ob’ektlar va elektron ma’lumotlarga (musiqa, rasmlar va videolar) nisbatan ham qo‘llasa bo‘ladi.

1990 yillarning oxirlarida kelib, raqamli tizimlarda watermark tizimlariga bo‘lgan qiziqish kuchaydi. Dastlab asosiy kontent sifatida rasmlar, audio va video ma’lumotlari olingan bo‘lsa, keyinchalik, binar rasmlar, matn, chiziqlar, animatsion parametrlar, yuklanuvchi kodlar va hak. lardan ham foydalanila boshlandi.

Steganografiya. Ma’lumot yashirishning ushbu sohasida, yashiringan ma’lumot kontentga hech qanday aloqasi bo‘lmay, kontent faqatgina ma’lumotni yashirish uchun foydalaniladi. Masalan, faraz qilaylik Alisa maxfiy agent sanalib, u o‘z sherigiga maxfiy ma’lumotni yubormoqchi. Buning uchun u, yaqinda o‘tgan yozgi ta’til tafsilotlarini qog‘oz maktubda tasvirlaydi. Shundan so‘ng, u siyox rangini sutga almashtiradi. Shundan so‘ng, odatiy siyox rangi bilan yozilgan qatorlar orasiga, maxfiy ma’lumotni yozadi. Sut qurigandan so‘ng, qog‘ozdagi maxfiy ma’lumotlar oddiy inson ko‘zi uchun ko‘rinmas holda o‘tib qoladi. Ushbu maktubni, chiroqqa tutib qaralsa, maxfiy ma’lumotlarni ko‘rish imkoniyati mavjud bo‘ladi. Watermarkdan farqli ravishda maxfiy ma’lumotlar, kontentga tegishli emas. U shunchaki maxfiy ma’lumotni yashirish uchun foydalanilgan [7].

Steganografiyaga bo‘lgan talab, 2001 yil 11 sentyabr kunidagi voqeadan so‘ng keskin ortdi.

Watermarking tarixi. Qog‘oz xitoyda 1000 yil avval oldin ixtiro qilingan bo‘lib, dastlabki qog‘ozlardagi belgilar, qog‘ozni qaysi tashkilot tomonidan ishlab chiqilganini bildirgan.

18 asrga belib, yevropa va amerika qitalarida watermark turli hujjat va pullarni qalbakilashtirishga qarshi foydalanilgan.

Watermark atamasi 18 asr oxirisida nemis atamasi “wassermarke” kelib chiqqan bo‘lishi taxmin qilinadi. Watermark atamasi albatta noto‘g‘ri talqin etilgan, ya’ni, belgi yaratilishida albatta suvni ahamiyati muhim emas. U qog‘ozga suv shaklidagi belgi tushirilganligi sababli, kelib chiqqan.

Shundan so‘ng, bu sohada qator ishlar qilindi. Ma’lumotni yashirish xususida 1499 yilda anonim tarzda chop etilgan hikoyaga ko‘ra, “Hypnerotomachia Poliphili” kitobidagi har bir bo‘limlarning birinchi harflari olingan va “Poliam Frater Franciscus Columna Peramavit.” ketma-ketlik hosil qilingan va unda “Father Francesco Columna loves Polia.” ma’lumoti hosil qilingan [7].

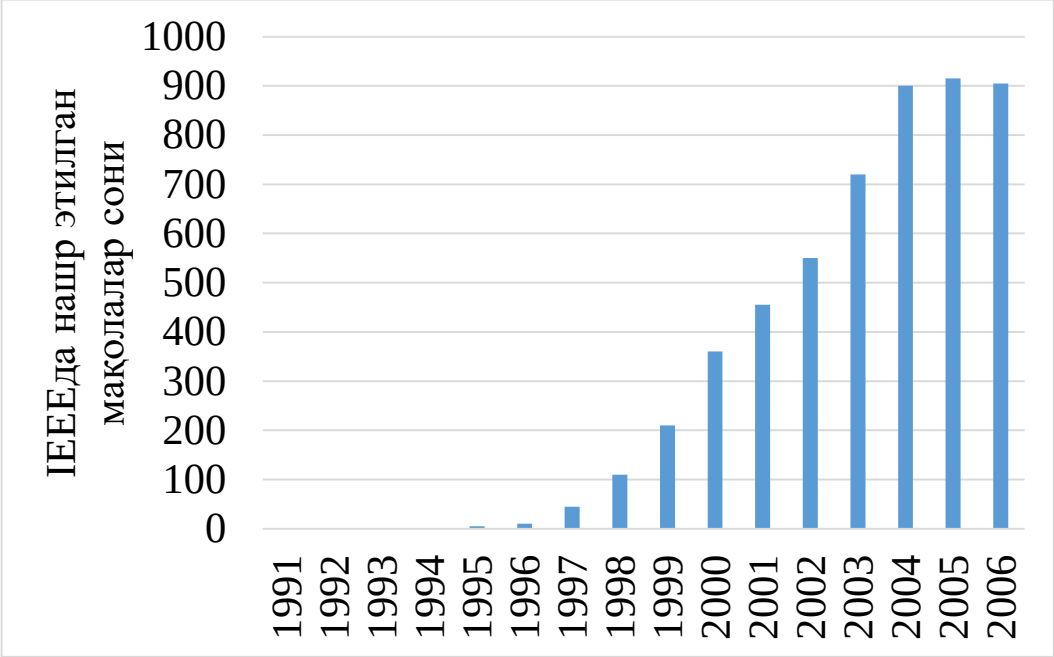
Shundan to‘rt yuz yil o‘tgandan so‘ng, dastlabki texnologiya yordamida hosil qilingan watermark tizimi yaratildi. 1954 yilda Emil Hembrooke (Muzak

Corporation) musiqa ortida ma’lumot yashirish amalga oshirildi. Bunda musiqa orasida doimiy takrorlanuvchi kichik uzunlikdagi bo‘shliqlar qoldirildi. Ushbu bo‘shliqlar uzunliklariga ko‘ra “nuqta” yoki “tire” ekanligi aniqlanadi. Bunda Morze koldash usulidan foydalanilgan.

Shundan so‘ng ko‘plab tashkilotlar tomonidan, watermarking texnologiyasi turli standartlar uchun ishlatila boshlandi. Copy Protection Technical Working Group (CPTWG) tashkiloti watermarking texnologiyasidan DVD larda videolarni himoyalashda foydalangan bo‘lsa, Secure Digital Music Initiative (SDMI) tashkiloti tomonidan musiqani himoyalash uchun foydalanildi. Yevropaning taniqli ikkita tashkiloti, VIVA va Talisman tomonidan watermarking texnologiyasi ommaviy axborot vositalari uchun ishlatila boshlandi [7].

Steganografiya tarixi. Steganografiya haqidagi dastlabki ma’lumotlar Gerodot hikoyalarida uchraydi (undagi qullar va ularning soshsiz boshlari haqidagi hikoya). Bundan tashqari uning “Demeratus” nomli hikoyasida, Spartani Gretsiya tomonidan rejalashtirilgan hujumdan ogohlantirgan Demeratus nomli shaxs, mumlangan daraxt po‘stlog‘iga ma’lumot yozib, ustini yana bir maratoba mumlagan va yangi mumlangan po‘stlog‘ sifatida yonida saqlab manzilga etkazgan.

Eney (qadimgi Troya sarkardalaridan biri) o‘z davrida ayollarning quloq ziraklari yoki shlyapalar yordamida ma’lumotlarni yasharish usullaridan foydalangan.



1.4-rasm. Watermarking va Steganografiya bo‘yicha chop etilgan moqolalarning yillar kesimida ko‘rinishi

Tilga asoslangan steganografiya eng qadimgi usullardan biri sanalib, maxfiy ma’lumotlar matndagi har bir gapning birinchi harflari orqali ifodalangan. Ushbu usulning shakllantirilgan shakli, Cardan tomonidan o‘rganilib chiqildi. Bunga ko‘ra yashiringan ma’lumotni kontent ichidan topishda maxsus “maskalar”dan foydalaniladi. Maskalar haqidagi ma’lumot esa faqat ikki tomongagina ma’lum bo‘ladi. Ushbu usuldan birinchi jaxon urushida nemis va antinemis kuchlarida keng foydalanilgan [7].

Zamonaviy steganografiya texnologiyasi ko‘rinishlaridan biri Brassil va boshqalar tomonidan yaratildi. Unga ko‘ra, matndagi harflarni yoki so‘zlarni 1/300 inchga yuqoriga yoki pastga surilishini inson ko‘zi anglay olmaydi. Ammo, maxsus kserikopiya orqali uni aniqlash juda ham oson.

Stenografiya va watermarkingning muhimligi. Watermarking texnologiyasining jadal rivojlanishi asosan uning mualliflik huquqini ta’minlash (copyright protection)da foydalanilishi sabab bo‘ldi. Internet tarmog‘ining jadal rivojlanishi, u orqali ma’lumot almashinishining ortishi, rasm, musiqa va video ko‘rinishidagi ma’lumotlarni ko‘chirilishi va yuklanishi, o‘z navbatida mualliflik huquqini ta’minlash muammosini keltirib chiqardi [7].

Dastlabki ma’lumotlar analog shaklda yozilgan bo‘lib, unda bu muammo uncha sezilmagan. Sababi, anaolog ma’lumotdan qayta-qayta ko‘chirilishi natijasida ma’lumot sifati kamayib boradi. Ammo, raqamli shaklda ma’lumotlarni yozish imkoni natijasida, ko‘chirilgan va asl ma’lumot orasida sezilarli farq bo‘lmaydi. Bu esa, ma’lumotlarni qalbakilashtirish, mualliflik huquqini buzulishiga olib keldi.

Ma’lumot himoyasining dastlabki usullaridan biri bu – kriptografiya sanaladi. Kriptografiya raqamli ma’lumot himoyasini ta’minlashda keng foydalanilayotgan usuldir. Kriptografiyada, xabar jo‘natuvchi ma’lumotni maxfiy kalit bilan shifrlaydi va shifrlangan ma’lumotni internet tarmog‘i orqali yuboradi. Qabul qiluvchi, shifrlangan ma’lumotni maxfiy kalit bilan deshifrlaydi va ma’lumotga ega bo‘ladi. Ammo, kriptografiyada maxsulot sotuvchi o‘z maxsulotlarini deshirfrlangandan keyin monitoring qilish imkoniyatiga ega bo‘lmaydi. Masalan, sotuv oluvchi qonuniy ma’lumotni sotib oladi va kalit bilan uni deshifrlaydi. Shundan so‘ng, ochiq matnga ega bo‘ladi va uni noqonuniy tarzda sotish imkoniyatiga ega bo‘ladi. Boshqa so‘z bilan aytganda, kriptografiya ma’lumotlarni almashinish jarayonida xavfsizligini ta’minlay oladi.

Buning natijasida, ma’lumotni deshifrlangandan so‘ng ham uni himoyasini ta’minlash muammosi dolzarb bo‘lib qoldi. Watermarking texnologiyasida kontent ichida joylashtirilgan watermark odatiy foydalinganda, shifrlanganda, deshirfrlanganda, raqamli – analog almashtirishda, siqish jarayonlarida o‘chib ketmaydi.

Hozirda watermarking texnologiyasidan qurilmalar va dasturiy mahsulotlarni noqonuniy tarzda foydalanishlardan himoyalashda keng foydalanilmoqda.

Elektron ma’lumot almashinishi ortishi natijasida ularni noqonuniy tarzda qo‘lga kiritish, o‘rtada turib eshitish yoki ma’lumotni ushlab qolish kabi tahdidlar keng tarqaldi. Ushbu tahdidlarga qarshi kriptografiyadan keng foydalanilsada, kriptografiya texnologiyasida katta hisoblashlar va matematik amallarni bajarish talab etiladi.

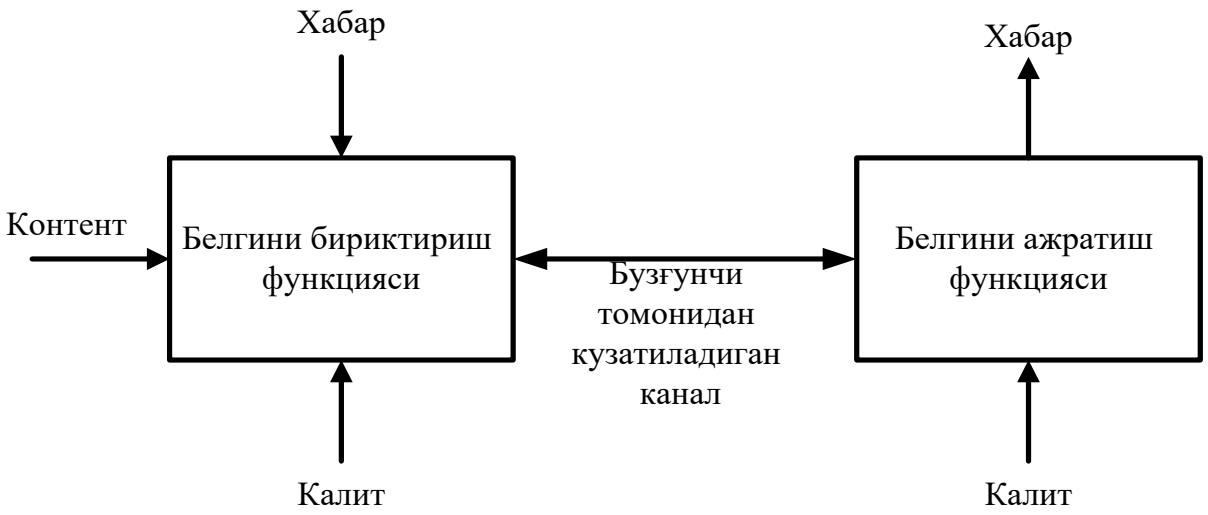
Steganografiyada esa ochiq ma’lumot orqasida maxfiy ma’lumotni yashirish sodda hisoblashni talab etadi. Bu esa bu texnologiyani istalgan joyda foydalanish imkonini beradi [7].

Steganografik algoritmlardan foydalangan holda maxfiy aloqani tashkil etish asosida bir nechta maqsad yashiringan bo‘lishi mumkin. Umumiy holda ma’lumot almashadigan tomonlar o‘z aloqalarini boshqalardan sir tutishda foydalanishadi. Bundan maqsad, siyosiy, terrorizm yoki boshqa sabablar bo‘lishi mumkin. Ushbu sohada ko‘plab, ilovalar ishlab chiqilgan bo‘lib, ularning ba’zilari nomalum sanaladi va turli tashkilotlar tomonidan foydalaniladi.

Stegonografiya ma’lumotlarni yashirish usullarini o‘rganib, bunda yashiringan ma’lumotni faqat yuboruvchi va qabul qiluvchi bilishi mumkin. Stegonografiya tizimlariga qo‘yiladigan asosiy talablardan biri bu – aniqlab bo‘lmaslikdir. Boshqa so‘z bilan aytganda buzg‘unchi kontentda ma’lumot yashiringanligini bilmasligi shart va zarur.

Watermarking va stegonografiya tizimlari ma’lumotlarni yashiruvchi ikki asosiy ko‘rinish sanalsada, ularning orasida muhim farq mavjud.

Stegonografik aloqa tizimlari. Stegonografiyaning dastlabki formal bo‘lmagan ko‘rinishdagi sxemasi, Simons tomonidan *mahbuslar muammosi* tarzida ifodalangan. Bunga asosan ikki maxbus bir-biri bilan ma’lumot almashashi kerak. Ammo ma’lumot almashinuvini qamoq boshlig‘i nazorat qiladi. Bunda ikki mahbus shundan usul orqali ma’lumotni yashirishi kerakki natijada qamoq boshlig‘i yashiringan ma’lumotni aniqlay olmasin. Ushbu sxema quyida keltirilgan [7].



1.5 – rasm. Stegonografik aloqa tizimlari

Ma'lumotni uzatish kanali. Stegonografiyada odatda aloqa fizik kanallar orqali amalga oshiriladi. Umumiy holda shovqin bo‘lishini hisobga olib, bu tizimlarda xatoliklarni tuzatish kodlaridan foydalaniladi. O‘rtada buzg‘unchi borligini hisobga olgan holda, ularni uz turga: aktiv, passiv va zararli turlarga ajratish mumkin [7].

Passiv turdagi buzg‘unchi o‘rtada uzatilayotgan ma'lumotni kuzatish imkoniga ega bo‘ladi. Agar yashiringan ma'lumot topilsa unda aloqa uziladi. Aks holda aloqaga teginilmaydi.

Aktiv turdagi buzg‘unchi o‘rtada uzatilayotgan ma'lumotni kuzatibgina qolmay, yashiringan ma'lumot topilmagan taqdirda kontentga o‘zratirish kiritadi va yashiringan ma'lumotni aniqlab bo‘lmas holatga keltiradi va qabul qiluvchiga yuboradi.

Zararli turdagi buzg‘unchi o‘rtada turib, har ikki tomonga yolg‘on ma'lumotlarni uzatadi. Bu odatda ochiq kalitli tizimlardan foydalanilgan holda o‘xshaydi. Ya'ni, aldamchi ma'lumotlarni yuborish orqali tomonlarni chalg‘itish va aldash amalga oshiriladi.

Stegonografiyaning quruvchi bloklari. Stegonografik algoritmlarning qurishning asosiy bloklari quyidagilar [7]:

- Yashiruvchi ma'lumotni, kontentni tanlash;

- Quyidagilarni o‘z ichiga olgan biriktirish va ajratish algoritmlari:
    - Belgilarni tayinlash funktsiyasi;
    - Biriktirish o‘zgartirishlari;
    - Tanlash qoidalari.
- Stego kalitlarni boshqarish.

Stegonografiya tizimlari Watermarking tizimlariga o‘xshamagan holda yashiruvchi ma’lumot, kontent haqida ma’lumotni o‘zida saqlamaydi. Natijada esa ma’lumotni tashuvchi kontentlarni ixtiyoriy tanlash imkoniyati vujudga keladi.

Belgilarni yashirish, qo‘yish funktsiyasi quyidagi uchta asosiy prinsipga asoslanadi:

- Ma’lumotni yashiruvchi kontent oldindan mavjud bo‘lib, yembedder kontentni o‘zgartirmaydi. Bu esa stegonografiyada ma’lumotni yashirish “qarash” orqali amalga oshiriladi.
- Ma’lumotni tashuvchi kontent maxfiy ma’lumot asosida yaratiladi va kontent hech qanday o‘zgartirilmaydi. Bu prinsip kontentni sintezlash deb ham ataladi.
- Kontent oldindan aniqlangan bo‘ladi va embedder kontentni o‘zgartiradi. Bu usul kontentni o‘zgartirish orqali stegonografiya usuli deb ham ataladi.

Qanday qilib kontentni o‘zgartirmasdan ma’lumotni yashirish mumkin? Masalan, Alisa 10-bitli ma’lumotni Bobga yubormoqchi. Buning uchun Alisa 1 000 ga yaqin qo‘shiqni oladi va ularning har biriga maxfiy kalitini biriktirib, xeshlaydi va natijani yubormoqchi bo‘lgan ma’lumoti bilan solishtiradi. Natija teng bo‘lsa, u holda shu qo‘shiq tanlanadi, aks holda keyingi qo‘shiq olinadi va hisoblash amalga oshiriladi. Bu usulning murakkabligi kerakli bo‘lgan kontentni topish darajasi bilan aniqlanadi.

Sintezlash usuliga ko‘ra, dastlab maxfiy ma’lumot olinib, keyin uni yashiruvchi kontent tanlanadi. Bunga misol sifatida ikkinchi jahon urushida foydalanilgan “Windswept” kodlarini olish mumkin. Bunga asosan, suhbatlashish uchun kerakli bo‘lgan birikmalar qatori ma’lum bir kod bilan belgilangan. Bu

kodlar orqali esa birikmani topish imkoni yaratiladi. Bu kodlar to‘plami maxsus kitob shaklida ishlab chiqilgan [7].

Kontentni o‘zgartirishga asoslangan stegonografiyada esa kontentni ma’lumotga qarab o‘zgartirish amalga oshiriladi. O‘zgartirishlar tanlash qoidalariga asosan tanlanadi.

Kontentga ma’lumotni yashirish kalitlar asosida amalga oshirilgan. Bu kalitlar turli maqsadlarda foydalanilgan.

Faraz qilaylik, K_s stego kalit kalitlar to‘plami K olingan. M yuborilishi kerak bo‘ldigan maxfiy ma’lumotlar. C esa yashiruvchi kontent. Bu holda embedderlash va aniqlash jarayonlari quyidagicha ifodalanadi:

$Embed: CxKxM \rightarrow C$

$Aniq: C \rightarrow M$

Xususiy holda esa, ajratilgan belgi $c \in C, K_s \in K \; va \; m \in M$ bo‘lgan holda $Ext\big(Emb(c, K_s, m)\big) = m$ ga stegokontent esa $s = Emb(c, K_s, m)$.

Bu yerda Ext – belgini ajratish funktsiyasi, Emb – belgini bikirtirish funktsiyasi.

Stegonografiyada kontent va ma’lumot sifatida quyidagi turdagi ma’lumotlardan foydalanish mumkin:

- video ko‘rinishdagi;
- matn ko‘rinishdagi;
- rasm ko‘rinishdagi;
- ovozli ma’lumotlardan.

Shunga ko‘ra stegonografik algoritmlar turlicha bo‘ladi. Stegonografiyada ma’lumotlarni yashirishda quyidagilar maxfiy saqlanishi mumkin va ular ma’lumotni yashiringanligini anglatadi.

- yashirish kalitini maxfiy saqlash. Bu holda algoritmning o‘zi barchaga ochiq bo‘ladi;
- algoritmni maxfiy holda saqlash. Bu holda algoritm faqat tegishli foydalanuvchilarga ma’lum bo‘ladi va qoganlar uchun noma’lum bo‘ladi.

Birinchi turdagi stegonografik algoritmlar amalda o‘rganiladi va tahlil qilinsa, ikkinchi turdagi algoritmlarni aniqlash amalda qiyin.

Zamonaviy kompyuter stenografiyasining asosiy holatlari quyidagilardan iborat:

- yashirish usullari faylning autentifikatsiyalanishligini va yaxlitligini ta’minlashi kerak;
- yovuz niyatli shaxslarga qo‘llaniluvchi steganografiya usullari to‘liq malum 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 chikarib olish jarayoni murakkab xisoblash masalasi sifatida tasavvur qilinishi lozim.

Internet kompyuter tarmog‘ining axborot manbalarini tahlili quyidagi xulosaga kelishga imkon berdi, ya’ni hozirgi vaqtda stenografik tizimlar quyidagi asosiy masalalarni yechishda faol ishlatilmoqda:

- 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.

1.3. Kriptografik va stegonografik himoya usullaridan foydalanilgan holda axborotni himoyalash

Odatda stegonografiyada quyidagi turdagi tahdid turi mavjud [7]:

Ruxsatsiz belgini biriktirish. Ko‘plab ruxsatsiz belgini biriktirish usulida ixtiyoriy olingan kontentga haqiqiy xabar belgisi qo‘yiladi. Bu hol odatda xabarni biriktirish jarayoni texnologiyasini o‘rganish natijasida kelib chiqadi.

Ruxsatsiz belgini aniqlash. Bu turdagi tahdidda belgini aniqlash ruxsatiga ega bo‘lmagan foydalanuvchi tomonidan belgini aniqlash amalga oshiriladi.

Qo‘yilgan belgini ruxsatsiz olib tashlash. Bu tahdid natijasida kontentdan belgi ruxsatsiz olib tashlanadi va belgi qo‘yilmagan holda keltiriladi.

Tizimga tahdid. Ba’zi hollarda tahdid belgi qo‘yilgan kontentga qarshi emas, balki tizimga qarshi amalga oshiriladi. Bunda tizimdagi ba’zi bir zaifliklarga asoslnadi. Masalan, ko‘chirishni nazoratlash tizimlarida har bir qurilmalarda maxsus mikrochiplar bo‘lib, ular belgini aniqlash uchun foydalaniladi. Ushbu mikrochipni olib tashlash orqali, qurilmada noqonuniy tarzda nusxalash imkoniyatini hosil qilish mumkin. Bu Watermarking tizimiga qilingan tahdidga misol bo‘la oladi.

Tahdidchining imkoniyatlari. Tahdidchi turli imkoniyatlarga ega bo‘lishi mumkin. Masalan, qandaydir tizim uchun tahdidchi faqat belgi qo‘yilgan kontent haqida ma’lumotga ega bo‘lsa, boshqa bir tizimda umuman ma’lumotga ega bo‘lmasligi mumkin. Quyida buzg‘unchi imkoniyatlari va oqibatlari keltirib o‘tilgan:

Buzg‘unchi hech nimani bilmagan hol. Bu holda tahdidchi tizim qurilmalari va algoritmi haqida hech qanday ma’lumotga ega bo‘lmaydi. Bu holda tahdidchi barcha watermarking tizimlarida bo‘lishi mumkin bo‘lgan hollar va algoritmlarni o‘rganishdan boshlaydi. Masalan, tahdidchi kontentni belgi qo‘yilgan deb hisoblaydi va undan belgi olib tashlashga harakat qilsa, buning uchun umumiy usullar sanalgan, maskalash, turli geometrik, vaqtinchalik o‘zgarishlarni, turli

filterlash usullarini qo‘llab ko‘rishga harakat qiladi. Umumiy holda olinadigan xususiyatlar Stirmark tizimidan olinishi mumkin.

Tahdidchiga bittadan ortiq belgi qo‘yilgan kontentlar mavjud bo‘lgan hol. Ba’zi hollarda tahdidchiga bir nechta belgi qo‘yilgan kontentlar mavjud bo‘ladi. Bu holda u algoritmni bilmagan holda ham belgini olib tashlashga harakat qiladi. Bu holda keng foydalaniladigan usul bu *kolliziya tahdididir*.

Kolliziya tahdidining ikkita yo‘nalishi mavjud. Birinchisida tahdidchi bir xil belgi biriktirilgan bir nechta kontent oladi va ularni o‘rganish orqali algoritmni aniqlashga harakat qiladi. Masalan, sodda holda tahdidchi barcha bir xil belgi mavjud kontentlarning o‘rtacha qiymatini hisoblaydi. Agar bir xil belgi yasharingan bo‘lsa u holda olingan qiymat kontentlar qiymatiga yaqin bo‘ladi. Olingan o‘rtacha qiymatni kontentdan olib tashlash orqali belgini o‘chirish imkoniyati tug‘iladi. Bu usul ayniqsa audio watermarking tizimlarida katta samara beradi.

Kolliziya tahdidining ikkinchi usulida bir kontent nusxalarida turlicha belgilar qo‘yilgan bo‘lib, tahdidchi barcha belgi qo‘yilgan nusxalar orqali haqiqiy kontentni olishga harakat qiladi. Masalan, ba’zi kontent belgilari olib tashlanishi mumkin va hak.

Tahdidchi algoritmni bilgan hol. Odatda qatiy xavfsizlik talab etilgan tizimda tahdidchi tizim algoritmi haqida to‘liq ma’lumotga ega bo‘lmaydi. Ba’zi hollarda algoritmni to‘lik xavfsiz saqlashni imkoni yo‘q. Bundan tashqari algoritmni maxfiy saqlash natijasida, uning xavfsizligini to‘liq ta’minlab bo‘lmaydi.

Shuning uchun amalda algoritm maxfiy tutilmaydi. Faqat unga tegishli bo‘lgan maxfiy kalitlar sir tutiladi. Tahdidchi algoritm haqida to‘liq ma’lumotga ega bo‘lish orqali biriktirilgan ma’lumotni aniqlashi mumkin. Algoritm ma’lum bo‘lgan holda ham tahdidchi tomonidan buza olmaslilik algoritmning bardoshliligi yuqori ekanligini anglatadi.

Tahdidchiga detektor ma’lum bo‘lgan hol. Yuqorida tahdidchiga algoritm ma’lum bo‘lgan hol yoki ba’zi qism ma’lumotlar ma’lum bo‘lgan hollar ko‘rib

o‘tildi. Bundan tashqari tahdidchi detektor qurilmasiga ega bo‘lgan hol ham mavjud bo‘lib, bi qarashda bu tahdidchi faqat belgini aniqlash imkoniyatiga ega bo‘ladi degan xulosani beradi.

Tahdidchi detektor qurilmasiga egalik qilgan holda, kontentda ma’lum o‘zgarishlarni amalga oshirib, kontentdan aniqlanish regionini aniqlashi va buning natijasida algoritmni aniqlash imkoniga ega bo‘lishi mumkin.

Watermarking va kriptografiyaning analogligi. Watermarking va kriptografiya tizimlari bir-biriga o‘xshash bo‘lib, bu o‘xshashlikni quyidagi tengliklar orqali ham ko‘rish mumkin.

Kriptografiyada ma’lumotlar shifrlash va deshifrlash (simmetrik shifrlash algoritmlari uchun):

Shifrlash: $c = E_K(m)$; Bu yerda m – ochiq matn, s – shifr matn va E_K shifrlash funktsiyasi.

Deshifrlash: $m = D_K(c)$; Bu yerda m – ochiq matn, s – shifr matn va D_K deshifrlash funktsiyasi.

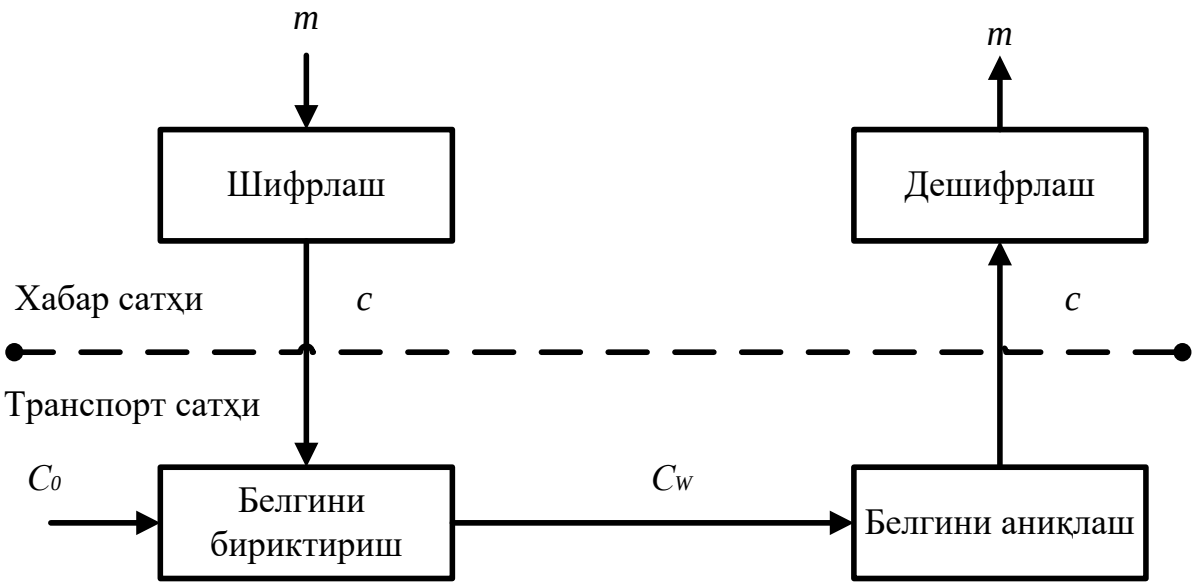
Watermarking tizimlari ham shunga o‘xshash bo‘lib, belgilarni biriktirish va ajratib olish bosqichlaridan iborat:

Belgilarni biriktirish: $c_w = \varepsilon_K(c_0, m)$, Bu yerda: ε_K – biriktirish funktsiyasi, c_0 – haqiqiy kontent va m – belgi.

Belgilarni aniqlash : $m = D_K(c_w)$, Bu yerda: $D_K -$ belgilarni aniqlash funktsiyasi.

Stegonografiyada mavjud yuqoridagi tahdidlar quyidagicha yechilishi mumkin:

Ruxsat etilmagan aniqlashdan himoyalash. Watermarking tizimlarida kriptografiya algoritmlaridan foydalanish orqali watermarking tizimlarida mavjud ko‘plab tahdidlarni bartaraf etish mumkin. Quyidagi rasmda ruxsat etilmagan aniqlash tahdidini kriptografiy usullardan foydalanish orqali bartaraf etish ko‘rsatilgan:



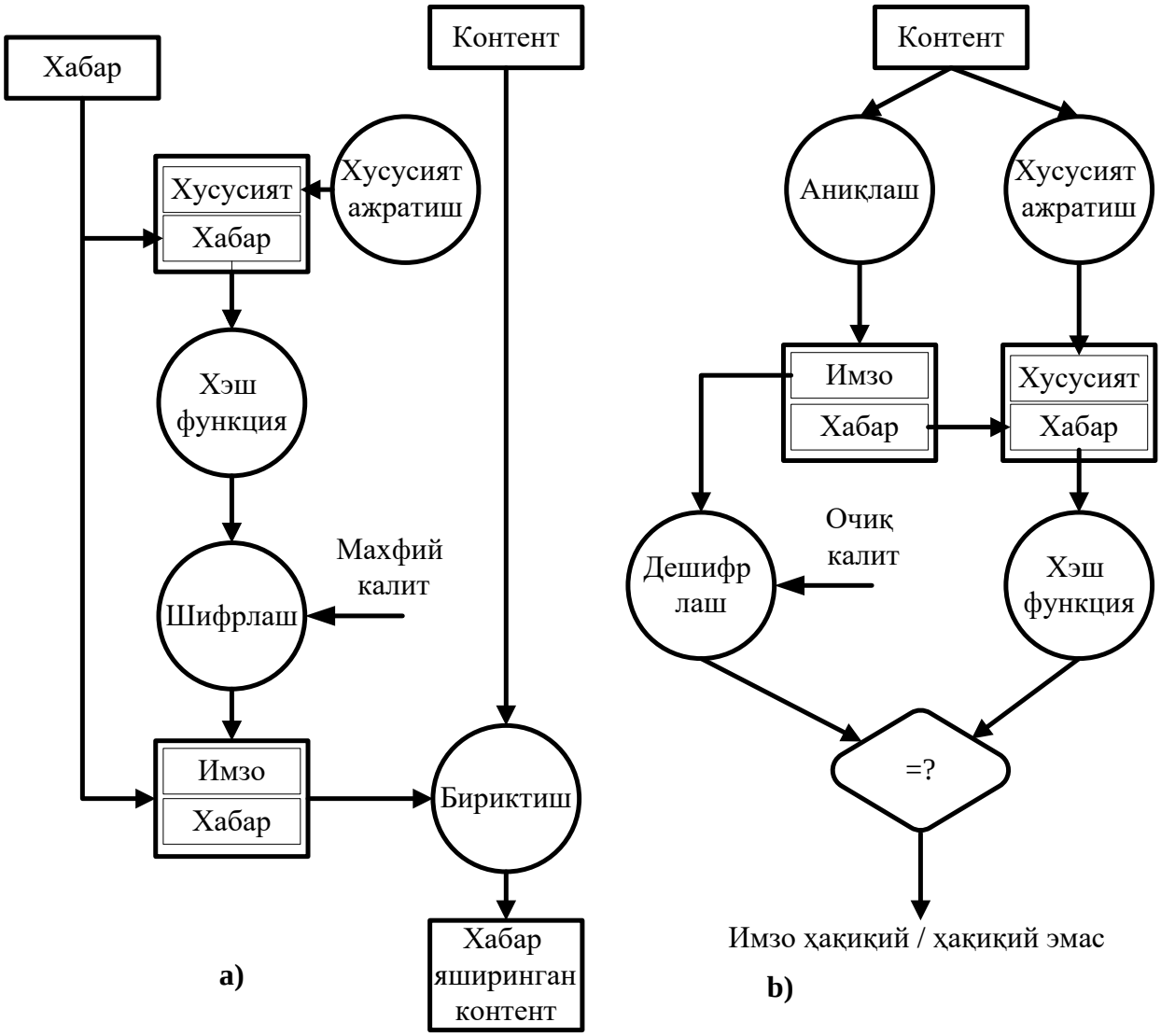
1.6 – rasm. Ruxsat etilmagan o‘qishdan himoyalash

Belgilarni ruxsat etilmagan qo‘yishdan himoyalash. Bu usulda ham kriptografik himoya usullaridan foydalaniladi. Kriptografiyada autentifikatsiyalash jarayonini amalga oshirish uchun ochiq kalitli shifrlash va elektron raqamli imzo algoritmlaridan keng foydalaniladi.

Ochiq kalitli shifrlash algoritmlarida ikkita kalitdan foydalaniladi. Birinchisi ma’lumotni shifrlashda va ikkinchisi deshifrlashda foydalaniladi. Ma’lumotni shifrlash kalitlari barchaga ma’lum bo‘ladi. Deshifrlash kaliti esa faqat kalit egasiga ma’lum bo‘ladi.

Elektron raqamli imzo algoritmlari yuborilgan xabarni aynan bir foydalanuvchiga tegishligini anglatadi. Bu tizimlar ham ikkita kalitdan foydalanadi. Birinchi kalit imzo chekish uchun (faqat bitta foydalanuvchiga tegishli bo‘ladi), ikkinchi kalit esa imzoni tekshirish uchun foydalaniladi (barchaga ma’lum bo‘ladi).

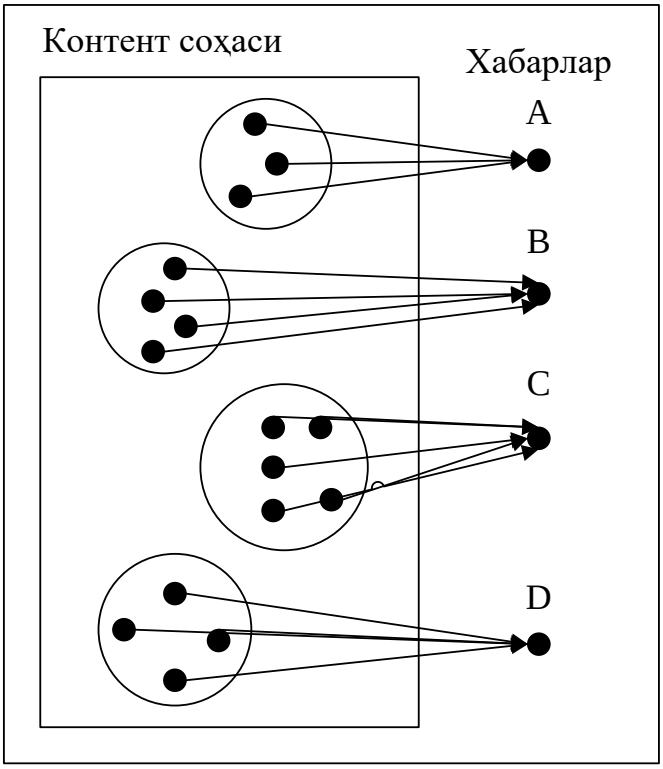
Quyida elektron raqamli imzodan foydalangan holda belgilarni ruxsat etilmagan qo‘yishdan himoyalash usuli keltirilgan.



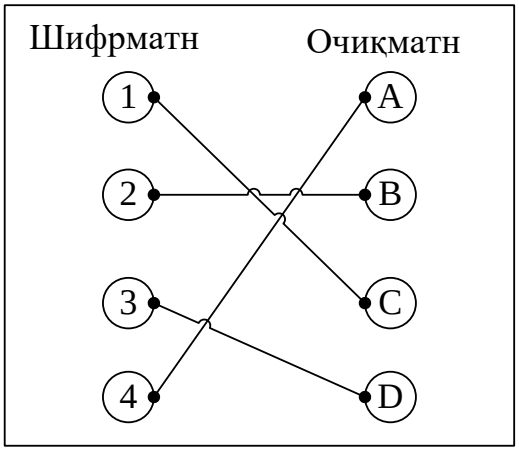
1.7 – rasm. a) belgini biriktirish b) belgini aniqlab olish

Ruxsat etilmagan olib tashlashdan himoyalash. Kriptografik himoya usullaridan foydalangan holda ruxsat etilmagan qo‘yish va aniqlashdan soddalik bilan foydalanish mumkin. Ammo, ruxsat etilmagan olib tashlash kriptografik muammo sanalmaydi.

Ruxsat etilmagan olib tashlash tahdidiga qarshi *keng polosalarda* modulyatsiyalash usulidan foydalaniladi. Bu usulda modulyatsiyalanganda ma’lumotlar turli chastotalarda ifodalanadi. Quyida keng polosalarda modulyatsiyalash va kriptografik himoya usuli orasidagi bog‘lanish keltirilgan.



Белгини бириктириш



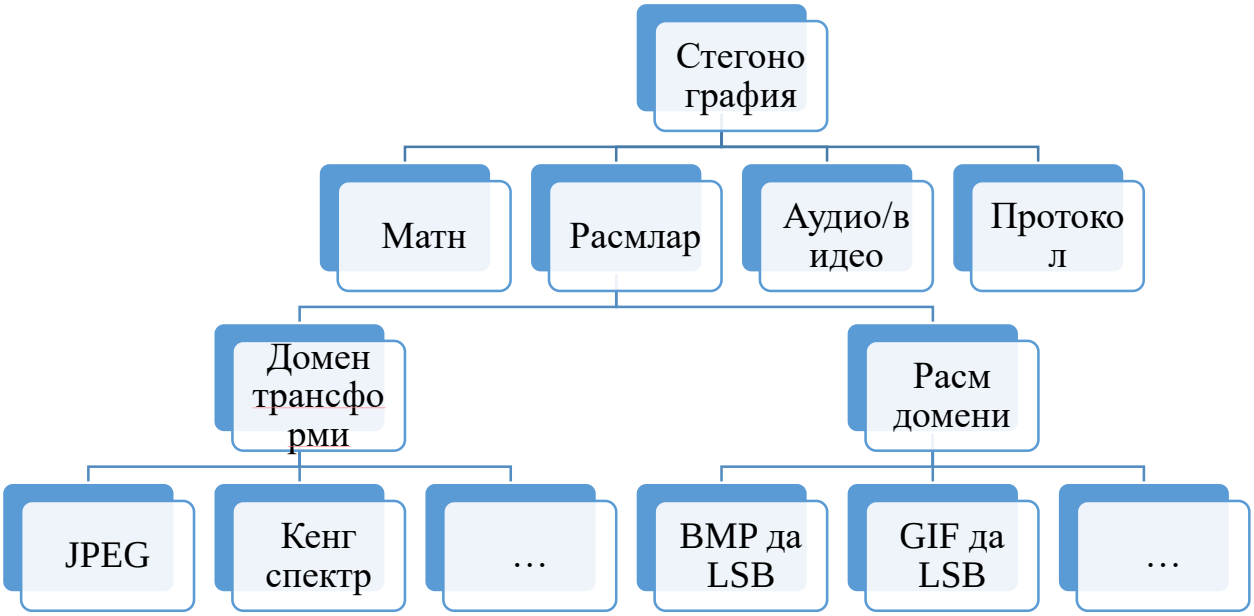
Шифрлаш

1.8 – rasm. Keng palasalarda modulyatsiyalash va shifrlash usullari

2. Asosiy qism. Rasm ma’lumotlarda axborotni stegonografik algoritmlar yordamida himoyalash

2.1. Rasm ma’lumotlar stegonografiyasi

Rasm ma’lumotlar stegonografiyada yeng ko‘p tarqalgan ma’lumot tashuvchi kontent hisoblanadi. Rasm ma’lumotlarning raqamli ishlov berishda ularning formatlaridan foydalanilgan holda yondoshiladi. Rasm ma’lumotlarning ko‘p turlari mavjud bo‘lib, ular tuzilishlari bilan bir – biridan farq qiladi. Hozirda amalda .JPEG, .GIF, .BPM, .PNG, .TIFF kabi keng tarqalgan turlari mavjud. Har bir rasm formatlari turli xususiyatlarga ega bo‘lganligi sababli, raqamli stegonografiyada ulardan foydalanishda unga etibor berish kerak. Masalan, .JPEG formati ma’lumotlarni siqishda yo‘qotish usullaridan foydalanilganligi sababli, undan stegonografiyada foydalanilganda (rasm ustida ishlov berib, uni yana rasm sifatida .JPEG formatida saqlaganda) ma’lumotlarni yo‘qolish xavfi mavjud bo‘ladi [10].



2.1 – rasm. Rasm stegonografiyasi kategoriyalari

Yoqotilishsiz siqishga asoslangan rasm formatlariga esa .GIF va .BMP (8 - bitli) formatlarini olish mumkin. Yuqorida aytib o‘tilganidek, stegonografiyada rasm ma’lumotlardan foydalanilganda ularni yo‘qotish bilan yo‘qotishsiz siqish hususiyatiga etibor berish kerak.

LSB usuli. Ushbu usulga ko‘ra kontentdagi piksellar bitlarining muhim sanalmagan o‘rinlaridagi qiymatini (LSB (least significant bit)) ma’lumot piksellari bitlariga almashtiriladi. Ushbu usul quyidagilarga asoslanadi [8]:

- Rasm ma’lum o‘lchamga ega bo‘lganligi sababli (masalan, NxM), ixtiyoriy (i,j) o‘rindagi pikselini binar holda ifodalash imkoniyati mavjud;
- Bu ifodalanish natijasida rasm bitlarini muhim sanalgan (most significant bit,MSB) va muhim sanalmagan (least significant bit, LSB) bitlarga ajratish imkoniyati tug‘iladi.

Umumiy holda ushbu algoritmning umumiy mohiyati kontentning muhim bo‘lmagan pozitsiyalarini aniqlash va uni maxfiy ma’lumotning (watermarking belgisi) muhim sanalgan pozitsiyalaridagi bitlari bilan almashtirishga asoslangan.

Ushbu algoritmdan foydalanishda kontent va maxfiy ma’lumot sifatidagi rasmlar *grayscale* modelida bo‘lishi mumkin. *grayscale* rang modelida barcha piksellar 0-255 gacha bo‘lgan sonlar bilan ifodalanadi. Bu modelda berilgan pikseldagi bitlarni muhim va muhim bo‘lmagan bitga ajratish quyidagicha amalga oshiriladi: 201(11001001) pikseli uchun ular quyidagicha (2.2 – rasm) [9].

	MSB						LSB
Bit indeksi	8	7	6	5	4	3	2	1
Qiymati	1	1	0	0	1	0	0	1

2.2 – rasm. Bitlarning joylashuvlari

Agar rasm RGB rang modelida bo‘lsa, unda uning tashkil etuvchi har bir qismi bir baytdan ifodalanadi.

Ushbu usulga asosan rasmning har bir pikselining 8 – bitiga (LSB) ga yashirinuvchi ma’lumotning bir biti qo‘yiladi. Agar rasm RGB rang modelida bo‘lsa, unda bir pikselda uch bit ma’lumotni yashirish mumkin [10].

Masalan, RGB rang modelidagi 3 – piksel quyidagicha bo‘lsa:

```
1 – pixel (00101101 00011100 11011100)
```

2 – pixel (10100110 11000100 00001100)
3 – pixel (11010010 10101101 01100011)

Yashirinuvchi ma’lumot 200 ga (11001000 ikkilikda) teng. Ma’lumot yashiringan pikselning ko‘rinishi quyidagiga teng bo‘ladi:

1 – pixel (00101101 00011101 11011100)
2 – pixel (10100110 11000101 00001100)
3 – pixel (11010010 10101100 01100011)

O‘zgartirilgan piksellardan qayta rasm hosil qilinganda (yo‘qotilishsiz siqish bilan) inson ko‘zi ilg‘amas tarzdagi o‘zgirish sodir bo‘ladi. Bu usuldan foydalanilganda BMP rasm formatidan foydalanish tavsiya etiladi. Ammo, BMP formatidagi rasmning hajmi katta bo‘lishi talab etiladi. Shuning uchun ushbu usulning boshqa rasm formati uchun ishlab chiqishga urinishlar ortmoqda.

LSB va palitraga asoslangan rasmlar. Palitraga asoslangan rasmlar, masalan, GIF formati, Internet tarmog‘ida foydalaniladigan yana bir keng tarqalgan rasm turi hisoblanadi. GIF formatidagi rasmlarda ham bit uzunligi 8 ga teng va shuning uchun maksimal ranglar soni 256 ta bo‘ladi. Ushbu rasm turi indekslangan rasm sanalib, rasmlarda mavjud ranglar palitrada saqlanadi. Ba’zida maxsus jadvallar tarzida ifodalanadilar. Har bir piksel yagona bayt orqali ifodalanadi va piksel ma’lumot indeks sifatida ranglar palitrasida saqlanadi. Bu ranglar palitrasi odatda yeng keng tarqalgan ranglardan yeng kam tarqalgan ranglar tomonga qarab tartiblangan bo‘ladi [10].

GIF rasmlar ham LSB stegonografiyasida foydalaniladi va katta etiborni talab etadi. GIF rasmlardagi ushbu muammo, piksel LSB bitining birgina o‘zgarishi, palitradagi indekslar o‘zgarishi natijasida butin rasmga ta’sir etishi mumkin. Buning oldini olishning bir usuli bu palitradagi ranglarni tartiblashdir. Ya’ni, palitrani shunday tartiblash kerakki, ketma – ket kelgan ranglar orasidagi farq juda kichik bo‘lsin. Ushbu muammoni hal qilishning ishonchi usuli bu – *grayscale* rasmlardan foydalanishdir. Bunda ma’lumot yashiringan rasmlarda juda

kichik o‘zgarishlar sodir bo‘ladi va natijada tahdidchi ushbu o‘zgarishni payqay olmaydi.

JPEG siqish. Rasmni JPEG formatga siqishdan oldin, RGB ranglar YUV ko‘rinishida o‘tkaziladi. Bunda Y tashkil etuvchi yorug‘lik miqdorini, U va V ranglarni ifodalaydi. Tajribilar shuni ko‘rsatadiki, inson ko‘zi ranglar o‘zgarishi farqidan ko‘ra, yorug‘lik o‘zgarishi farqini yaxshiroq ajratadi. Ushbu fakt JPEG siqishda foydalanilgan, ya’ni rasm faylining o‘lchamini kamaytirish uchun ranglar ma’lumotlari kamaytiriladi. Ranglar tashkil etuvchisi (U va V) gorizontal va vertikal yo‘nalishni ifodalagin sababli, rasm fayli o‘lchami 2 martadan kamayadi [10].

Keyingi bosqich, rasmni tronsformi bo‘lib, JPEG uchun Discrete Cosine Transform (DCT) foydalaniladi. Bundan tashqari Discrete Fourier Transform (DFT) o‘zgartirishlari ham foydalaniladi. Bu metematik o‘zgartirishlar rasmni piksellarini o‘zgartirish orqali amalga oshiriladi. DCT o‘zgartirishlarida rasm ko‘rinishidagi signallar chastota shaklida ifodalanadi. Bunda rasmning 8x8 piksel qismlari bir blok sifatida olinadi va o‘zgartirish natijasi har bir blok uchun 64 DCT koiffitsientga teng bo‘ladi. Bir DCT koiffitsientni o‘zgarishi 64 ta rasm pikseliga ta’sir etadi.

Shundan so‘ng, sanash (kvantizatsiya) jarayoni amalga oshiriladi. Bu yerda inson ko‘zining boshqa bir xususiyatidan foydaniladi. Ya’ni, inson ko‘zi katta sohadagi yoritilganlikdagi kichkina farqni yaxshi farqlay oladi. Ammo, yuqori chastotadagi yoritilganlikdagi farqlarni ajratish darajasi yaxshi emas. Ya’ni, yuqori chastotalar kuchini kamaytirish orqali rasmni o‘zgarmasligini ta’minlash mumkin. JPEG buni blokdagi barcha qiymatlarni kvantlash koiffitsenti orqal bo‘lish bilan amalga oshiradi. Bu natijalar butun qiymatlarga yaxlitlanadi va koiffitsentlarni Xaffan kodlash usulidan foydalanib o‘lchamlari kamaytiriladi.

JPEG stegonografiyasi. Odatda stegonografiyada JPEG fayllardan yo‘qotish orqali siqishi sababli foydalanilmaydi. Stegonografiyaning muhim bir xususiyatlaridan biri shuki xabarni kontentning muhim sanalmagan bitlari o‘rniga qo‘yishdir. JPEG formatdan foydalanilganda aynan shu muhim sanalmagan bitlar

o‘zgarishi natijasida, xabar buzulishi mumkin. Shunga qaramasdan siqish algoritmlarining xususiyatlaridan foydalanib, JPEG uchun ham stegonografik algoritm ishlab chiqish mumkin [10].

JPEG formatining asosiy xususiyatidan biri bu - siqish natijasidagi o‘zgarishni inson ko‘zi orqali aniqlash imkoni yo‘qligidir. DCT foydalanib siqishda, koifitsientlardani o‘zgarishga katta ahamiyat qaratilmaydi. Ushbu xususiyat algoritmni yo‘qolish bilan siqishini ta’minlab qolmasdan, balki ma’lumotlarni yashirish uchun foydalanilishi mumkin.

JPEG forati odatda yo‘qotilish bilan siqish usuli sifatida qaralsada, unda yo‘qotilish bilan va yo‘qotilishsiz amalga oshirish bosqichlari mavjud. DCT va kvantizatsiya jarayonlari yo‘qotilishli bosqichlar sanalsa, Xaffam usulida kodlash esa yo‘qotilishsiz bosqichdir. Stegonografiya ushbu bosqichlarning o‘rtasida joylashishi lozim. Ya’ni, LSB usulida ma’lumotlarni yashirish Xaffman kodlashidan oldin amalga oshiriladi. Bu usul orqali ma’lumotni yashirganda, uni aniqlash jarayoni juda qiyin bo‘ladi va inson ko‘zi orqali aniqlash mumkin bo‘lmaydi.

Bundan tashqari rasm stegonografiyasida yuqoridagi ikkita usulning kombinatsion tarzda foydalanishga asoslangan usullar ham mavjud.

Patchwork. Yuqoridagi usullarning kombinatsyasi asosida ishlab siqilgan usullardan biridir. Patchwork statistik texnologiya sanalib, rasmda xabarni biriktirish uchun qoldiq xabarni kodlashdan foydalaniladi. Algoritm yashirinuvchi xabarga qoldiq xabar qo‘shadi va uni rasm bo‘ylab yoyadi. Psevdotasodifiy sonlar generatori rasmdan ikkita tasodifik qismni, A va B qismlarni topishda foydalaniladi. A qismdagi barcha piksellar yoritiladi va B tomon qorong‘ulashtiriladi. Boshqa so‘z bilan aytilganda, birinchi qism biror qiymatda yoritilsa, ikkinchi qism aynan shu qiymatda qorong‘ulashtiriladi. Bu qarama-qarshilik orqali bir bit ma’lumotni kodlash mumkin bo‘lib, rasmning qolgan qismi o‘zgarmas qoladi [10].

Bu usulning kamchiligi esa faqat bir bitni yashirishidir. Birdan ko‘p bitlarni yashirish uchun, rasmlarni ko‘plab qism rasmlarda ajratish va ularning har birida

bir bitdan ma’lumotlarni yashiriladi. Bu usulning afzalligi esa, maxfiy xabarni butun kontent (rasm) bo‘ylab teng yoyilishidir. Shuning uchun, rasmning bir qismdagi o‘zgarish boshqa qismlariga ta’sir etmaydi.

Keng spektrlar. Keng spektrlar texnologiyasida yashirinuvchi ma’lumot kontent (rasm) buylab tarqatiladi. Bu tizim Marvel tomonidan taklif etilgan bo‘lib, keng spektrlar aloqasi, xatoliklarni nazoratlash kodlari va rasm jarayonlari kombinatsiyasidan iborat [10].

Keng spektrlar aloqasi keng polosali chastotalarda kichik polosali chastotalarni yoyish bilan xarakterlanadi. Buning natijasida keng polasalardan kerakli polosadagi chastotani aniqlash imkoni yo‘qoladi. Bu usulda asoslangan rasm stegonografiyasida esa, xabar shovqinlar ichiga kiritiladi va keyin kontent (rasm) bilan biriktiraladi. Natijada maxfiy xabar yashiringan kontent hosil bo‘ladi. Xabar shovqin ma’lumot ichiga kiritganligi sababli, uni aniqlash qiyinlashadi. Xabarni aniqlashda haqiqiy kontent (haqiqiy rasm, xabar biriktirmadan oldingi holati) zarur bo‘lib, u bo‘lmaganda xabarni aniqlash imkoni mavjud emas.

Quyidagi jadvalda rasm stegonografiyasidagi algoritmlarning tahlili keltirilgan [9, 10].

2.1- jadval

	BMP da LSB	**GIF da LSB**	**JPEG siqish**	**Patchwork**	**Keng spektrlar**
Ko‘rinmaslik	Yuqori	O‘rtacha	Yuqori	Yuqori	Yuqori
Qo‘shimcha qo‘shiladigan ma’lumot hajmi	Yuqori	O‘rtacha	O‘rtacha	Past	O‘rtacha
Statistik tahdidga bardoshlilik	Past	Past	O‘rtacha	Yuqori	Yuqori
Rasmni buzishga asoslangan tahdidga	Past	Past	O‘rtacha	Yuqori	O‘rtacha

bardoshlilik					
Fayl formatiga bog‘liqlilik	Past	Past	Past	Yuqori	Yuqori
Shubhalanmaslik darajasi	Past	Past	Yuqori	Yuqori	Yuqori

2.2. Rasm ma’lumotlarni stegonografik algoritmlar orqali yashirish usulining dasturiy ta’minoti

Ushbu bo‘limda LSB usuliga asoslangan stegonografik algoritmlarning dasturiy vositasi ishlab chiqilgan. Bunda xabar matn va rasm ko‘rinishlarda olingan va xavfsizlik parol asosida ta’minlanadi.

Matn ma’lumotlarni LSB usulida yashirish. Ushbu usulga ko‘ra rasm konetntining LSB o‘rnidagi bitlariga, axborotning bitlari biriktiriladi. Rasmning axborotni yashirish hajmi quyidagicha hisoblanadi. Masalan, rasmning o‘lchami 300x400 piksel va u RGB rang modelida. Demak unda jami 300*400=120 000 bit mavjud va jami 120 000 * 3 = 360 000 ta LSB mavjud. Agar har bir belgini 8 bit shaklida ifodalansa, unda kontent 360 000 / 8 = 45 000 ta belgini o‘zida yashira oladi [11].

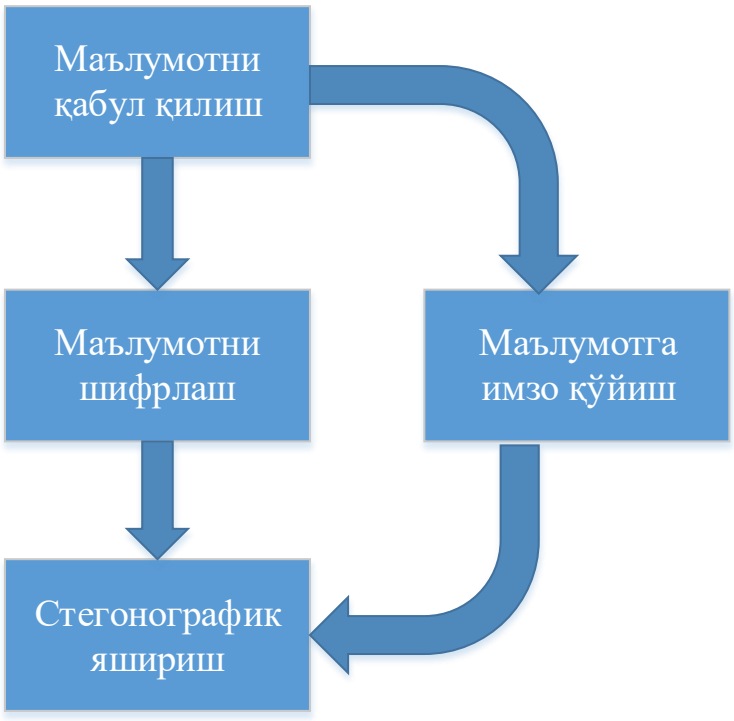
Rasm ichida axborotni yashirish quyidagicha amalga oshiriladi:

- Rasmdagi piksellari soniga teng tsikl yaratilib, har bir piksel uchun RGB ning tashkil etuvchilari alohida butun sonlar ko‘rinishida olinadi;
- Har bir piksel uchun R, G va B tashkil etuvchilarning LSB bitlari nolga tenglashtiriladi, ya’ni axborotni yashirish uchun;
- Yashiriniladigan axborot belgisi butun son shaklida, 8 bit hajmda ifodalanilib (agar yashiriniladigan axborotni maxfiyligini ta’minlash ham talib etilsa, u holda axborot shifrlash usullari asosida dastab shifrlanadi va shifrlangan ma’lumotlar rasm ichiga yashiriniladi), mos holda R1, G1, B1, R2, G2, B2, R3, G3 piksellarning LSB qiymatlari bilan almashtiriladi;

- Ushbu jarayon axborotning oxirgi bitigacha amalga oshiriladi va o‘zgartirilgan kontent rasm yo‘qotilishsiz usulda rasm shaklida saqlanadi (BMP, PNG formatda). *Izoh:* yashirish kerak bo‘lgan axborotning hajmi rasmning hajmiga nisbatan kichik bo‘lishi kerak. Ya’ni, axborotni tugaganligini ko‘rsatish uchun biror ko‘rsatkich zarur. Bu ko‘rsatkich oddiy 8 ta uzunlikdagi nollar ketma – ketligidir. Bu ko‘rsatkich yashirinilgan axborotni aniqlash uchun foydalaniladi.

Rasmdan yashirinilgan axborotni aniqlash uchun rasm piksellarining LSB bitlari olinadi (toki 8 ta uzunlikdagi ketma – ket nolgacha). Olingan bitlar 8 tadan qilib ajratiladi, baytga aylantiriladi va mos belgi olinadi. Belgilar birlashtirilib, yashirinilgan axborot olinadi.

Rasm ma’lumotlarda axborotlarni yashirishda stegonografik algoritmlar yordamida yashirganda ularni aniqlash imkoniyati mavjud bo‘ladi. Bu zaiflikni oldini olish uchun odatda stegonografik algoritmlar kriptografik algoritmlar bilan kompleks holda foydalaniladi. Bu kompleks usul ma’lumotni maxfiyligini ta’minlash va butunligini tekshirish imkonini beradi. Ushbu g‘oyaga asoslanib taklif etilgan usul ko‘rinishi quyidagicha:

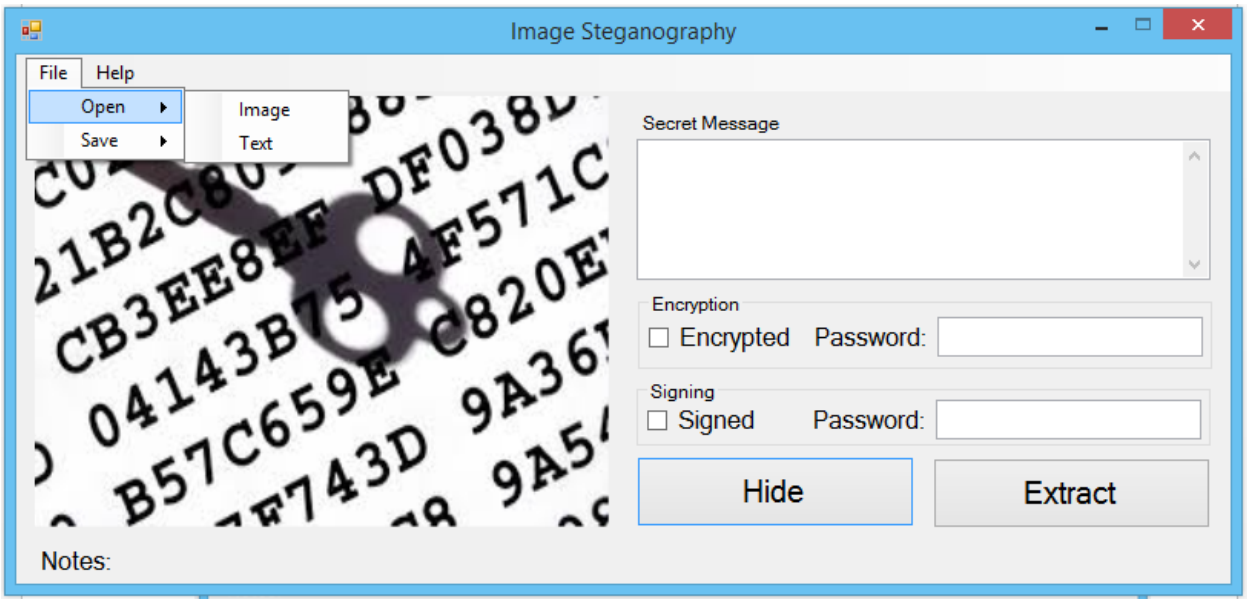


2.2- Rasm. Taklif etilgan usul

Taklif etilgan usul asosida dasturiy ta’minot ishlab chiqilgan bo‘lib, unda quyidagi algoritmlardan foydalanilgan:

- ma’lumotlarni shifrlashda AES shifrlash algoritmidan;
- ma’lumotni butunligini ta’minlashda SHA1 xesh funktsiyasi asosida HMAC tizimidan foydalanilgan.

Dasturdan foydalanish tartibi. Ushbu dasturiy vosita C# dasturlash tilida yaratilgan bo‘lib, dasturning umumiy ko‘rinishi quyidagicha:



2.3– rasm. Dasturning umumiy ko‘rinishi

Dasturning asosiy oynasi yuqoridagi rasmda keltirilgan. Undan foydalanish tartibi quyidagicha:

Maxfiy ma’lumotni yashirish jarayoni:

- Dastlab kontent rasm tanlanadi. Buning uchun File-Open-Image bandi orqali kerakli rasm tanlanadi. Shundan so‘ng tanlangan rasm maxsus maydonda hosil bo‘ladi.
- Shundan so‘ng yashirishili kerak bo‘lgan maxfiy ma’lumotlar kiritladi. Buning uchun oldindan saqlangan matn bo‘lsa File-Open-Text bandi orqali yoki Secret Message maydoniga kerakli matnni kiritish bilan amalga oshiriladi.

- Keyingi bosqichda yashirinishi kerak bo‘lgan axborotni maxfiyligi yoki butunligini ta’minlash kerak bo‘lganda foydalaniladi. Buning uchun kerakli maydonda maxfiy kalitni kiritishning o‘zi yetarli.
- So‘ngi bosqichda barcha bosqichlarni amalga oshirilgandan so‘ng yashirish “Hide” tugmasi bosiladi.
- Barcha ishlar bajarilgandan so‘ng maxfiy ma’lumot kiritilgan rasm qaytadan saqlanadi. Buning uchun File-Save-Image bandi tanlanadi.

Yashiringan maxfiy ma’lumotni aniqlash:

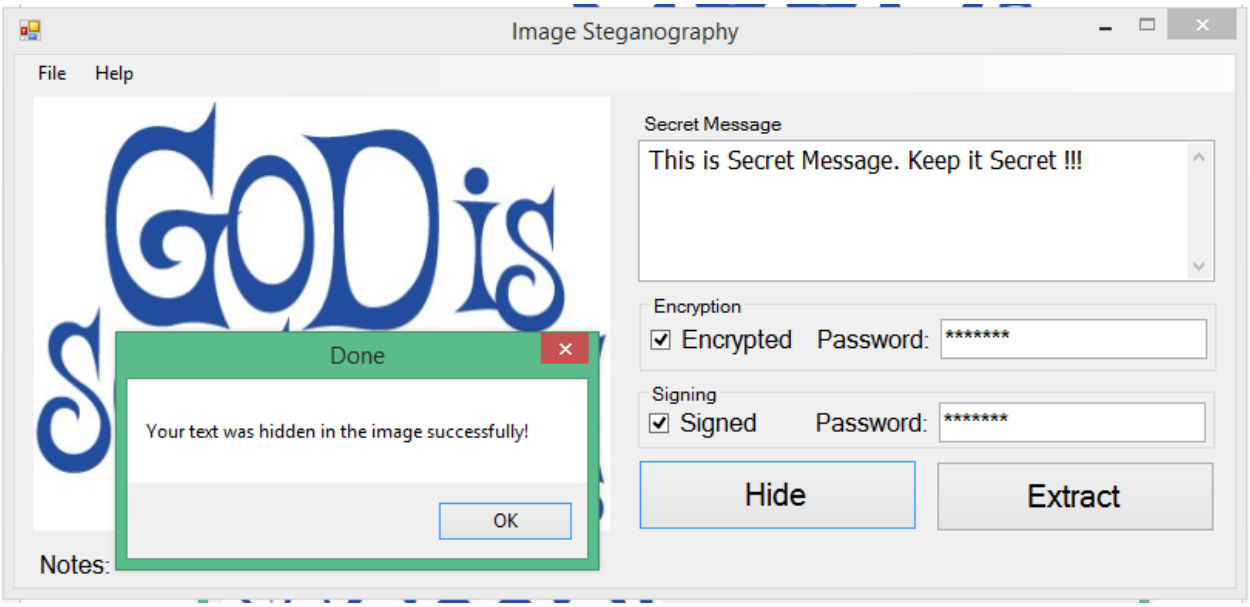
- Dastlab maxfiy ma’lumot yashiringan rasm tanlanadi. Buning uchun File-Open-Image bandi orqali kerakli rasm tanlanadi.
- Shundan so‘ng agar ma’lumot shifrlangan bo‘lsa, shifrlash kaliti yoki imzolangan bo‘lsa, imzoni shakllantirish kaliti kiritiladi.
- Shundan so‘ng “Extract” tugmasi bosiladi. Natija maxfiy ma’lumotlar maydonida namayon bo‘ladi.
- Imzoni tekshirishdagi natijalar xabar shaklida namayon bo‘ladi.

Dasturni ishlatib natija olishda quyidagi rasm kontent sifatida olindi:

2.4– rasm. Kontent rasm

Maxfiy ma’lumot sifatida esa “This is Secret Message. Keep it Secret !!!” xabari olindi. Ushbu ma’lumotni maxfiyligi va butunligini ta’minlash talab etilgan hol uchun quyidagicha bo‘ladi.

2.5– rasm. Dasturdan foydalanish jarayoni

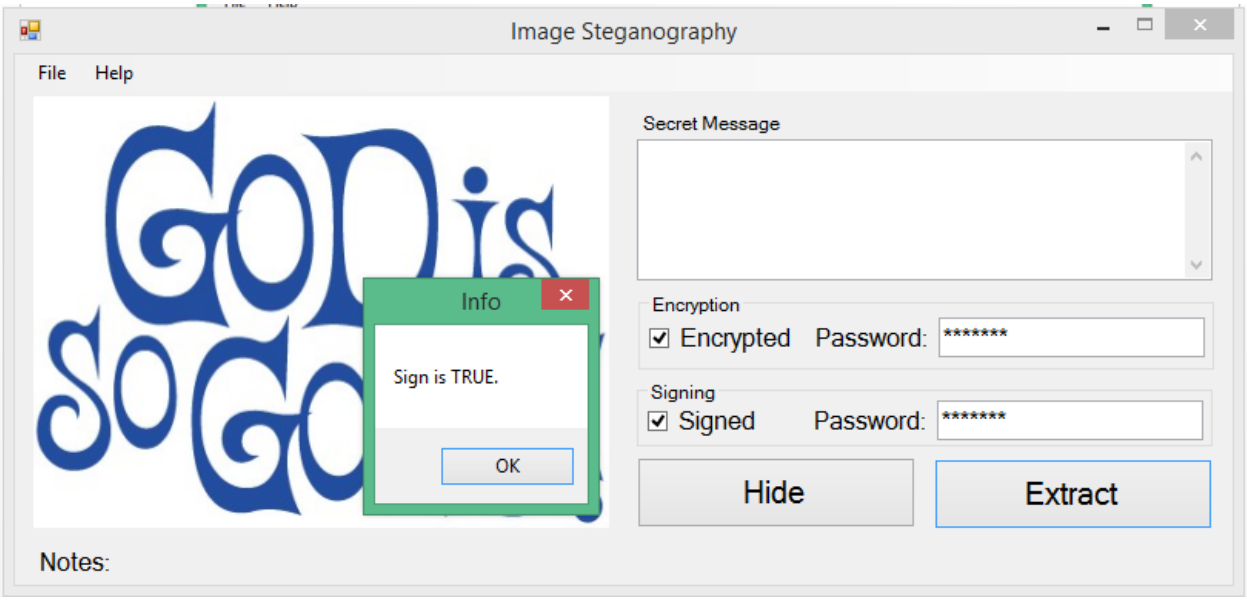


2.6– rasm. Muofaqqiyatli yakunlangan jarayon

2.7– rasm. Maxfiy ma’lumot yashiringan kontent

Ushbu rasmdan maxfiy ma’lumotni ajratib olish quyidagicha amalga oshiriladi.

2.8– rasm. Maxfiy ma’lumotni aniqlash jarayoni



2.9- rasm. Xabar butunligini to‘liqligi isboti

2.10– rasm. Maxfiy ma’lumotni aniqlash

Ushbu dasturiy vositadan foydalanganda katta hajmdagi ma’lumotni yashirish uchun katta o‘lchamdagi rasm talab etiladi. Ma’lumot yashiringan rasmni saqlashda esa yo‘qotilishsiz siqishga asoslangan rasm formatlaridan foydalanish tavsiya etiladi.

2.3. Rasm ma’lumotlarda axborot yashiringanligini tahlillash usullari

Stegonotahlil sohasi stegonografiya sohasiga qarama-qarshi hisoblanib, unda stegonografiya usullarining bardoshligi tahlil qilinadi.

Stegonotahlil senariysi umumiy holda ikkita qonuniy foydalanuvchi orasida uzatilgan yashirinilgan maxfiy ma’lumotni aniqlashdan iboratdir.

Aniqlash. Aniqlash jarayoni kontentga maxfiy belgi yashirinilganmi yoki yo‘qligini aniqlash bo‘lib, aniqlash jarayoni natijasida kontentning shunchaki kontentligi yoki stegokontentligi (belgi yashirinilganligi) aniqlanadi.

Stegonotahlilni olib boruvchi buzg‘unchi stegonotahlilchi deb yuritiladi va uning asosiy vazifasi unga ma’lum bo‘lgan axborotlarga asoslangan holda kontentda belgi mavjud yoki mavjud emasligini aniqlash. Stegonotahlilchiga gohida hech qanday ma’lumot ma’lum bo‘lmasligi, faqat maxfiy aloqadan foydalanilishini bilish mumkin. Ba’zida, stegonotahlilchiga foydalanuvchilar tomonidan foydalanilgan stegonografik algoritm ma’lum bo‘ladi. Birinchi holatda stegonotahlilchi belgilarni topishda, umumiy usullardan foydalanadi va bu ko‘rinishdagi stegonotahlil usuli *ko‘rkorona stegonotahlil* usuli deb ataladi. Ikkinchi holatda esa, stegonotahlilchi aniq bir algoritmni tahlil qiladi va bu ko‘rinishdagi stegonotahlil usuli *maqsadli stegonotahlil* usuli deb ataladi.

Maqsadli stegonotahlil usuli. Yuqorida aytib o‘tilganidek, maqsadli stegonotahlil usulida tahlilchiga algoritm ma’lum bo‘lib, bu ko‘proq va aniqroq ma’lumot olishga asos bo‘ladi.

Ba’zida berilgan algoritmlar to‘liq holda tahlilchiga ma’lum bo‘lsa, ba’zida esa unda ishtirok etgan biror parametr (kalit) maxfiy tutiladi. Bu holda tahlilchiga algoritm ma’lum, ammo unda foydalanilgan kalit ma’lum emas.

Ko‘rko‘rona tahlil. Bu usulda olingan natija birmuncha noaniq bo‘lib, bu xarakter tahlilchiga algoritmni ma’lum emasligi bilan belgilanadi. Bu holda tahlilchiga belgi qo‘yilgan kontentlar ma’lum bo‘lib, ularni tahlillashda u ko‘plab stegonotahlil usullarini qo‘llab ko‘radi. Shuning uchun bu tahlil usuli odatda *universial bo‘lmagan* usul deb ham ataladi.

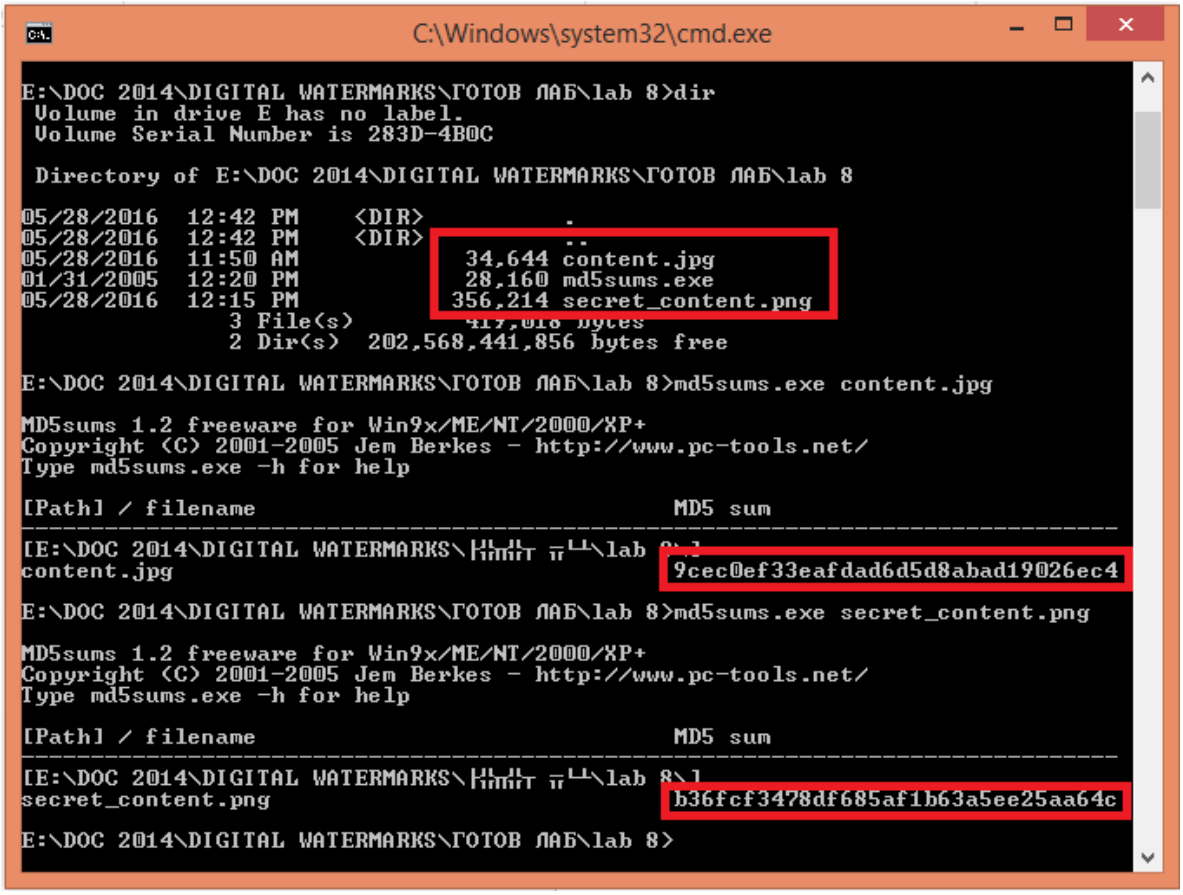
Tizimga tahdid. Ba’zi stegonografik algoritmlarning maqsadli va ko‘rko‘rona tahlil qilish orqali biror natijaga erishish juda qiyin. Bu holda odatda stegonografik algoritm foydalanilgan tizim tahlil qilinadi, boshqa so‘z bilan aytganda tizimda tahdid amalga oshiriladi. Masalan, 2006 yilda taqdim etilgan DVD qurilmalarida, bardoshli sanalgan kriptografik shifrlash algoritmidan foydalanilgan. Bu algoritmning amaliy tomondan tahlil qilish murakkab masala. Ammo bu turdagi pleyerlar 1 oydan so‘ng buziladi, ya’ni tahlilchilar tomonidan sindiriladi. Bunda tahlilchilar DVD pleyer qurilmalaridagi maxfiy kalitni xotiradan o‘qishdagi xatolikka asoslanadilar.

Haqiqiy kontentni stegonotahlilga ta’siri. Haqiqiy kontent yashiringan belgini xavfsizligiga ta’sir ko‘rsatadi va natijada stegonotahlilchiga ham ijobiy yoki salbiy ta’sir qilishi mumkin. Masalan, GIF formati kichik sondagi ranglardan tashkil topganligi natijasida unda yashirinilgan belgining oshkor bo‘lishi ko‘proq. Bundan tashqari kontentning ko‘rinishi yashiringan ma’lumotni yashirinilganlik darajasiga ta’sir ko‘rsatadi. Masalan, haqiqiy kontentga belgi bir tekis taqsimlangan bo‘lsa, kontentdagi o‘zgarishlar ochiq rangdagi qismda ko‘proq bo‘ladi. To‘qroq qismlarda esa o‘zgarishlar kamroq kuzatiladi.

Kontent rasm va belgi yashirinilgan kontent rasm farqni hisoblash. Belgi yashiringan va yashirinmagan rasmlar orasidagi farqni inson ko‘zi orqali aniqlash imkoni yuq. Buni aniqlashning quyidagi usullari mavjud:

- Hajm farqlariga ko‘ra;
- Ularning xesh qiymatlari farqiga ko‘ra.

Quyida maxfiy ma’lumot biriktirilgan va haqiqiy kontent orasidagi farqni ularning o‘lchami va MD5 xesh funktsiyasidagi qiymatlari orqali aniqlash keltirilgan.



2.10 – rasm. Ikki bir xil rasmlar orasidagi farqni aniqlash

2.4. HAYOT FAOLIYATI XAVFSIZLIGI

2.4. Meteriologik sharoit tavsifnomasi

Kompyuter xonalarida ish joyi to‘g‘ri tashkil etilishi ish unumdorligini oshirish, charchashni oldini olish, ish joyidagi jixozlarni va uskunalarni to‘g‘ri joylashtirishni omillar, ranglarni to‘g‘ri tanlay bilishdir. Uskunalar shunday joylashishi kerakki ishchilar ortiqcha xarakatsiz, o‘zini zo‘riqtirmasdan osongina foydalanishi kerak.

Ish joyida mehnat sharoitini yaxshilash ishlariga bir qancha omillarni hisobga olgan holda tashkil qilinadi. Bularga tashkiliy, texnikaviy, sanitariya – gigiena, tabiiy-iqlim omillari kiradi.

Tashkiliy omillar –ishning tashkil etish shakli intizom, mehnat jarayoni ustidan qilinadigan nazoratning holati, mehnat muhofazasi, ishchi xodimlarning kasbiy tayyorgarlik darajasi, texnik omillar jarayonlarini mexanizatsiyalash va avtomatlashtirish darajasi, boshqaruvda elektron hisoblash texnikalarida kompyuterlarni qo‘llash, himoyalash vositalarining sozligi va yetarliligi kiradi.

Sanitariya-gigiena omillari ish joyining sanitariya holatiga javob berish-bermasligi, erganomik omil mashina va uskunalarni inson bilan o‘zaro harakatda bo‘lganda mashina elementlarining mos kelishi. Bunda texnikani tezlik parametrlariga tegishli, ishchi organlaridan kelayotgan ma’lumotlar xajmi, ish joyining tashkil etilish darajasi, boshqarish organlarining qulay joylashganligi operator o‘rindig‘ining konstruksiyasi kiradi.

Psihofiziologik omillar - mehnatning og‘irligi va qizg‘inligi, jamoadagi psixologik vaziyat, ishchilarning bir-biri bilan o‘zaro munosabati, jismoniy zo‘riqish, asabiy-psixik zo‘riqishlar mehnat sharoitining inson organizmiga ta’sirini o‘rgangan holda quyidagilarni amalga oshirish kerak:

-ishda bajarilayotgan jarayonlar tez va tez talablar chegarasida va harakatlantiruvchi maydonning eng qulay doirasida amalga oshirish;

-ishlab chiqarish binolarida havo muhitini tekshirish;

-ishlab chiqarishdagi metrologik omillarini aniqlash;

-mahalliy va umumiy titrashni aniqlash;

-ishlab chiqarishdagi shovqin darajasini aniqlash;

-ish joyininig yoritilganligini aniqlash;

-nurlanganlikni tekshirish;

-havo almashuvini tekshirish.

Kompyuter xonalarida ishlaganda mehnat sharoitlarini yaratishdagi eng ko‘p qo‘yiladigan xatolarga quyidagilar kiradi:

1. Ish joylarni etarlicha katta emasligi.
2. Xona harorati va namligi talab qilinadigan me’yorlarga mos kelmasligi.
3. Xona va ish joylarni yetarlicha yoritilmaganligi.
4. Monitordan chiqayotgan past chastotali elktromagnitni maydonida nurlanishning ko‘p darajada ajralishi.
5. Ish vaqtini va dam olish vaqtlarini to‘g‘ri taqsimlanganligi.

Kompyuter operatorlari, dasturchilar va boshqa hisoblash texnikasi ishchilari shovqin, elektr toki, statik elektr kabi fizik, xafli va zararli fizik omillar ta’sirida bo‘ladi. Ko‘pgina hisoblash texnikasi bilan ishlovchi hodimlar aqliy zo‘riqish, ko‘rish va eshitish analizatorlarini zo‘riqishi, emotsional zo‘riqish kabi psixofizik omillar ta’sirida bo‘ladilar. Toliqish paydo bo‘lishi ish paytida markaziy asab tizimida paydo bo‘ladigan o‘zgarishlarga bog‘liq. Masalan kuchli shovqin rang ajratishni qiyinlashtiradi, ko‘rish o‘tkirligi, yorug‘likka moslashishni pasaytiradi, axborot qabul qilishni qiyinlashtiradi va 5-12 foizga ish unumini pasaytiradi. 90 DB shovqinni uzoq vaqt davomidagi ta’siri ish unumdorligini 30-60 foizga pasaytiradi. Hisoblash texnikasi bilan ishlovchi ishchilar tibbiy tekshiruvdan o‘tkazilganda ish unumdorligi pasayishdan tashqari shovqin eshitish qobiliyatini

xam pasaytiradi. Kombinatsiyalashgan zararli omillar ta’sirida ko‘p vaqt qolish kasbiy kasallanishga olib kelishi mumkin.

Elektr qurilmalari ya’ni kompyuterning barcha qurilmalari inson uchun xafli hisoblanadi. Chunki kompyuterda ishlayotganda inson tok kuchlanishi ta’sirida bo‘lgan qismlarga tegib ketishi mumkin.

Elektr qurilmalarning spetsifik xavfi - bu elektr o‘tkazuvchilar, izolyasiyasi shkastlanishi natijasida tok ta’siriga tushib qolgan kompyuter korpusi Elektr tokining ta’siri faqat tok inson tanasidan o‘tganda seziladi. Elektr shikastlanishidan himoyalanishda elektr qurilmalari to‘g‘ri joylashtirilishi, elektr o‘tkazuvchi sim va kabellarni to‘g‘ri ulanishi muxim o‘rin egallaydi.

Ish joylarida statik elektrning razryadli toki ko‘proq kompyuterning biror bir elementiga tegib ketish natijasida xosil bo‘ladi. Bunday razryadlar insonga xavf tug‘dirmaydi, yoqimsiz ta’sirdan tashqari kompyuterni ishdan chiqishiga olib keladi. Simlar izolyatsiyasi shikastlanganda tok ta’sirini kamaytirish uchun ish xonalarining pollari bir qavatli polivinil xloridli antistatik linolium bilan qoplanishi lozim. Himoyalashni boshqa usuli ionlashtirilgan gaz bilan zaryadlarni neytrallash.

Kompyuter xonalarining kattaligi u erda ishlovchi xodimlar va kompyuterlar soniga mos kelishi zarur. Ish joylarini tashkillashtirishga, yana xarorat, yorug‘lik, havo tozaligi, shovqindan himoyalanganlik parametrlari hisobga olinadi.

Sanitar me’yorlariga ko‘ra bir ishchi uchun ish joyining xajmi 15 m^3 , ish maydoni esa 4,5 m^2 dan kam bulmasligi kerak. Xonaning balandligi poldan shiftgacha 3-3,5 m bo‘lishi kerak.

Kompyuter xonalarida odatda yon tomonlama tabiiy yoritilganlik qo‘llaniladi. Tabiiy yoritilganlikda shimol yoki shimoliy-sharqqa qaratilgan yorug‘lik darchalaridan foydalanish kerak, bunda tabiiy yoritilganlik koiffitsenti 1,2-1,5 % kam bo‘lmasligi shart. Kompyuterlarni podvallarda joylashtirishga ruxsat etilmaydi.

Kompyuter xonalari va ish joylarida tabiiy yoritilganlik qo‘llanishi zarur. Boshqa xollarda esa sun’iy yoritilganlikni qo‘llash mumkin. Ish xujjatlari joylashgan stol usti yoritilganligi 300-500 lk bo‘lishi kerak.Yorug‘lik manbaini shunday joylashtirish kerakki, bunda yorug‘lik ko‘zni qamashtirmasligi kerak, ko‘rish maydonidagi yorug‘lik manbaining yorqinligi 200 kd /m^2 oshmasligi kerak.

Kompyuter joyini shunday joylashtirish kerakki, bunda tabiiy yorug‘lik iloji boricha yondan tushishi lozim. Kompyuter stolining balandligi iloji boricha 680-800 mm bo‘lishi kerak. Ish stoli oyoqlar uchun balandligi 600 mm, eni 500 mm dan kam bo‘lmagan, chuqurligi tizza darajasida 450 mm dan kam bo‘lmasligi, uzatilgan oyoq darajasida 650 mm dan kam bo‘lmasligi kerak.

Ekran monitori ko‘zdan eng uzog‘i bilan 600-700 mm bo‘lishi kerak, lekin xarf va shriftlarning o‘lchamiga qarab 500 mm dan yaqin bo‘lmasligi kerak.

Xonalarni rangli jihozlanishi ishni sanitar-gigiyena sharoitlarini yaxshilashga qaratiladi, ish unumini oshishiga hizmat qiladi.

Kompyuter xonalarini rangini texnik jihozlar rangi bilan bir xil rangda bo‘yash maqsadga muvofik. Xonalar va jihozlar ranglari yumshoq bo‘lishi va yaltiroq bo‘lmasligi lozim.

Yong‘in xavfsizligi

Elektr qurilmalari, kompyuterlardan foydalanishda turli xildagi yonishlar xavfi doim mavjuddir. Zamonaviy kompyuterlarda elektron sxemalarning elementlarini joylashish zichligi juda yuqoridir, ulash simlari, kommunakatsion kabellar bir-biriga juda yaqin joylashgan. Ulardan tok oqqanda, kata miqdorda issiqlik ajraladi, ba’zi bo‘limlarda harorat 80-100^o C gacha ko‘tarilishi mumkin. Bu ularning izolyatsiya qobig‘ining erishiga, o‘tkazgich qismlarining ochilib qolishiga, oqibatda qisqa tutashuv bo‘lib, uchqun chiqishi va yonib ketishiga olib kelishi mumkin.

Ortiqcha issiqlikni yo‘qotish uchun havoni kondensionerlash va ventilyasiya tizimi xizmat qiladi. Lekin bu tizmlar mashina zallari va boshqa xonalar uchun qo‘shimcha yong‘in xavfini yuzaga keltiradi, chunki bir tarafdan, yong‘in sodir

bo‘lganda, ularni xonalarga tezda tarqalishiga yordam beradi.

Elektr qurilmalariga tok alohida yong‘in xavfi bo‘lgan kabel simlari orqali uzatiladi, yonuvchi izolyatsiya materialining mavjudligi, elektr uchquni va yaqinlashish qiyinligi kabel liniyalaridan yong‘in chiqishi va rivojlanishi ehtimoli yanada kattaligidan dalolat beradi. Shuning uchun kabel simlari yonmaydigan materiallardan tayyorlangan, olib-qo‘yiluvchi texnalogik pol ostidan o‘tishi kerak. Hisoblash markazlaridagi xonalarda yong‘in jo‘mraklari yo‘lkalarga zina maydonchalariga, kirish joylariga o‘rnatiladi. Olov o‘chirgichlari 40-50 sm^2 ga bitttadan o‘rnatiladi. Yong‘in signalizatorlari va avtomatik yong‘in o‘chirish qurilmalari o‘rnatiladi.

Yng‘inlar sanoat korxonalari , xalq xo‘jaligining hamma tarmoqlari, qishloq xo‘jaligi va turar joylarda yuz berishi mumkin bo‘lgan ,yetkazadigan zarari jixatidan tabiiy ofatlarga tenglashishi mumkin bo‘lgan xodisa hisoblanadi . Yong‘inlar katta moddiy zarar keltirishi bilan birga, og‘ir baxtsiz xodisalar, zaxarlanish, kuyish natijasida kishilar xayotini olib ketgan xollar ko‘plab uchraydi.

Shuning uchun ham yong‘inga qarshi kurash barcha fuqarolarning umumiy burchi hisoblanadi va bu ishlar davlat miqyosida amalga oshiriladi.

Umuman yong‘in chiqmasligini ta’minlash, yong‘in chiqqan taqdirda ham uning rivojlanib, tarqalib ketishining oldini olish, moddiy boyliklarni, inson salomatligi va uning xayotini saqlab qolishga qaratilgan chora tadbirlar bo‘lib, bu masalalar mehnatni muhofaza qilishning tarkibiy qismi hisoblanadi.

Bizning vazifamiz yongin haqida asosiy tushunchalar berish bilan birga, unga qarshi samarali kurash olib borish, yong‘inni o‘chirishda qo‘llaniladigan birlamchi vositalar, xar-xil tadbirlar bilan o‘quvchilarni tanishtirishga qaratilgan.

Yong‘inning sabablari: isitish pechlarini qurish yoki ishlatish qoidalarini buzish, ishlab chiqarish yoki uyda olovni ehtiyotsizlik bilan ishlatish, kerosin bilan ishlayotganda yoritish yoki qizdirish asboblaridan noto‘g‘ri foydalanish yoki noto‘g‘ri o‘rnatish, yashin yoki statik elektr razryadlarini ishlatish. Mashinalar va ishlab chiqarish jixozlarining nosozligi xamda ularni ishlatish qoidalariga rioya qilmaslik sabab bo‘ladi. Yong‘inni oldini olish uchun tadbirlar: tashkiliy, texnikaviy tadbirlar qo‘llash kerak bo‘ladi.

Xulosa

Ushbu bitiruv malakaviy ishi rasm ma’lumotlarda maxfiy axborotni yashirish usullari tadqiqiga bag‘ishlangan bo‘lib, ishni bajarish davomida quyidagi natijalar olindi:

- axborotning kriptografik himoya usullari tadqiq qilindi;
- axborotning yashirish usullari, raqamli watermarking va stegonografiya himoya usuli tadqiq etildi;
- stegonografik himoya usullarida mavjud xavfsizlik muammolari va ularni barataraf etishda foydalaniladigan usullar tahlil etildi;
- rasm ma’lumotlarda maxfiy axborotni yashirish usullari tahlil qilindi;
- rasm ma’lumotlarda yashiringan axborotni maxfiyligi va butunligini ta’minlaydigan usul taklif etildi va uning dasturiy vositasi ishlab chiqildi;
- rasm ma’lumotlarda axborotni yashirganda qo‘llaniladigan tahlillash usullari tahlil etildi.

Ushbu bitiruv malakaviy ishida taklif etilgan usulda stegonografik va kriptografik usullarning kombinatsiyasidan foydalanilgan bo‘lib, uni nafaqat rasm ma’lumotlarda balki boshqa formatdagi ma’lumotlarda amxborotni saqlashda foydalanish mumkin.

Foydalanilgan adabiyotlar ro‘yxati

1. “Axborotlashtirish” to‘g‘risida O‘zbekiston Respublikasining qonuni. Toshkent sh., 2003 yil 11 dekabr, 560-II-son.
2. “O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari” to‘g‘risida O‘zbekiston Respublikasi prezidentining qarori. Toshkent sh., 2007 yil 3 aprel, PQ-614-son.
3. “Axborotlashtirish sohasida normativ-huquqiy bazani takomillashtirish” to‘g‘risida O‘zbekiston Respublikasi Vazirlar Mahkamasining qarori. Toshkent sh., 2005 yil 22 noyabr, 256-son.
4. Akbarov D. Ye. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi” – Toshkent, 2008 – 394 bet.
5. Ganiev S.K., Karimov M.M., Toshev K.A. Axborot xavfsizligi. 2008.
6. Shnayer B. Prikladnaya kriptografiya. Protokolы, algoritmы, isxodnыe tekstы na yazыke Si. – M.: izdatelstvo TRIUMF, 2003 -816 str.
7. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker. Digital Watermarking and Steganography. 2008 y.
8. Vijay Kumar Sharma, Vishal Shrivastava. A steganography algorithm for hiding image in image by improved lsb substitution by minimize detection. Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1
9. Anwar H. Ibrahim, Waleed M. Ibrahim. Text Hidden in Picture Using Steganography: Algorithms and Implications for Phase Embedding and Extraction Time. International Journal of Information Technology & Computer Science (IJITCS) (ISSN No : 2091-1610) Volume 7 : No : 3 : Issue on January / February, 2013.
10. T. Morkel, J.H.P. Eloff, M.S. Olivier. An overview of image steganography. Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.

11. Champakamala B.S., Padmini K., Radhika D. Least Significant Bit algorithm for image steganography. International journal of advance computer technology | volume 3, number 4.
12. Ekologiya i bezopasnost jiznedeyatelnosti: Uchebnoe posobie dlya studentov VUZov/ red. L. A. Muraviy, 2002.
13. Belov S.V. Bezopasnost jiznedeyatelnosti M.: Vыsshaya shkola. 2003.
14. YormatovG‘.Yo., Isamuxamedov Yo.U. Mehnatni muxofaza qilish. Darslik. O‘zbekistan nashriyoti. Toshkent 2002.
15. http://bjd.ispu.ru/

```
using System;
using System.Drawing;
using System.Windows.Forms;
using System.Drawing.Imaging;
using System.IO;
using System.Text;

namespace Steganography
{
    public partial class Steganography : Form
    {
        private Bitmap bmp = null;
        private string extractedText = string.Empty;
        private string signedData = string.Empty;

        public Steganography()
        {
            InitializeComponent();
        }

        private    void    hideButton_Click(object    sender,
EventArgs e)
        {
            bmp = (Bitmap)imagePictureBox.Image;

            string text = dataTextBox.Text;

            if (text.Equals(""))
            {
                MessageBox.Show("The  text  you  want  to  hide
can't be empty", "Warning");

                return;
            }

            if (encryptCheckBox.Checked)
            {
                if (passwordTextBox.Text.Length < 6)
                {
                    MessageBox.Show("Please  enter  a  password
with at least 6 characters", "Warning");

                    return;
                }
                else
                {
                    text    =    Crypto.EncryptStringAES(text,
passwordTextBox.Text);
                }
            }
```

```
            if (isSigned.Checked)
            {
                if (passwordHMAC.Text.Length < 6)
                {
                    MessageBox.Show("Please enter a password
with at least 6 characters", "Warning");

                    return;
                }
                else
                {
                    byte[]                key                =
Encoding.ASCII.GetBytes(passwordHMAC.Text);
                    signedData = Crypto.Encode(text, key);
                    text += "^" + signedData;
                }
            }
            bmp = SteganographyHelper.embedText(text, bmp);

            MessageBox.Show("Your text was hidden in the
image successfully!", "Done");

            notesLabel.Text = "Notes: don't forget to save
your new image.";
            notesLabel.ForeColor = Color.OrangeRed;
        }

        private void extractButton_Click(object sender,
EventArgs e)
        {
            bmp = (Bitmap)imagePictureBox.Image;

            string              extractedText              =
SteganographyHelper.extractText(bmp);
            if (isSigned.Checked)
            {
                if(extractedText.Contains("^"))
                {
                int index_SPEC = extractedText.IndexOf("^");
                string message = extractedText.Substring(0,
index_SPEC);
                string                  sign               =
extractedText.Substring(index_SPEC+1);
                byte[]                  key                =
Encoding.ASCII.GetBytes(passwordHMAC.Text);
                string new_sign=Crypto.Encode(message,key);
                    if (sign.Equals(new_sign))
                    {
                        MessageBox.Show("Sign    is    TRUE.",
"Info");
                    }
                    else {
```

```
                        MessageBox.Show("Sign    is    FALSE.",
"Info");
                    }
                    extractedText = message;
                } else {
                MessageBox.Show("Message   has   not   sign.",
"Info");
                }
            }

            if (encryptCheckBox.Checked)
            {
                try
                {
                    extractedText                                =
Crypto.DecryptStringAES(extractedText, passwordTextBox.Text);
                }
                catch
                {
                    MessageBox.Show("Wrong          password",
"Error");

                    return;
                }
            }

            dataTextBox.Text = extractedText;
        }

        private   void   imageToolStripMenuItem1_Click(object
sender, EventArgs e)
        {
            OpenFileDialog       open_dialog       =       new
OpenFileDialog();
            open_dialog.Filter = "Image Files (*.jpeg; *.png;
*.bmp)|*.jpg; *.png; *.bmp";

            if (open_dialog.ShowDialog() == DialogResult.OK)
            {
                imagePictureBox.Image                            =
Image.FromFile(open_dialog.FileName);
            }
        }

        private    void    imageToolStripMenuItem_Click(object
sender, EventArgs e)
        {
            SaveFileDialog       save_dialog       =       new
SaveFileDialog();
            save_dialog.Filter   =   "Png   Image|*.png|Bitmap
Image|*.bmp";

            if (save_dialog.ShowDialog() == DialogResult.OK)
```

```
            {
                switch (save_dialog.FilterIndex)
                {
                    case 0:
                        {
                            bmp.Save(save_dialog.FileName,
ImageFormat.Png);
                        }break;
                    case 1:
                        {
                            bmp.Save(save_dialog.FileName,
ImageFormat.Bmp);
                        } break;
                }

                notesLabel.Text = "Notes:";
                notesLabel.ForeColor = Color.Black;
            }
        }

        private    void    textToolStripMenuItem_Click(object
sender, EventArgs e)
        {
            SaveFileDialog       save_dialog       =       new
SaveFileDialog();
            save_dialog.Filter = "Text Files|*.txt";

            if (save_dialog.ShowDialog() == DialogResult.OK)
            {
                File.WriteAllText(save_dialog.FileName,
dataTextBox.Text);
            }
        }

        private    void    textToolStripMenuItem1_Click(object
sender, EventArgs e)
        {
            OpenFileDialog       open_dialog       =       new
OpenFileDialog();
            open_dialog.Filter = "Text Files|*.txt";

            if (open_dialog.ShowDialog() == DialogResult.OK)
            {
                dataTextBox.Text                                =
File.ReadAllText(open_dialog.FileName);
            }
        }

        private    void    aboutToolStripMenuItem_Click(object
sender, EventArgs e)
        {
            MessageBox.Show("Image    Stegonography    1.0.0",
"About");
```

```
                }
            }
        }
```