UDK 004.415

KOMPYUTER TARMOQLARIDA UZATILAYOTGAN AXBOROTNI KRIPTOGRAFIK HIMOYALASH USULI

Ganiyev A.A.[1], *Mavlonov O.N.*[2], *Shodmonov D.A.*[2], *Maxmudov J.I.*[2]
[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Toshkent, O‘zbekiston
[2] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali, Samarqand, O‘zbekiston
mavlonov8686@gmail.com

Annotatsiya. *Mazkur maqolada Steganografik himoyadagi mavjud kamchiliklarni bartaraf etishda kriptografik himoya mexanizmlari ko‘rib chiqilgan. Steganografiyaning maqsadi maxfiy xabarlarni raqamli kontentlarga hech kim bunday xabarlar mavjudligini aniqlashga imkon bermaydigan tarzda yashirishdan iborat bo‘lib, u maxfiy xabarning tuzilishini o‘zgartirmasdan, maxfiy xabarni ochiq xabar tarkibiga yashiradi. Shuning uchun o‘zgarishni aniqlash murakkab hisoblanadi. Steganografiya usulining bardoshligi ushbu usulning maxfiyligiga bog‘liq bo‘lib, stegotahlil usuli yashirish usulini aniqlashni maqsad qiladi. Steganografik himoyadagi mavjud kamchiliklarni bartaraf etishda kriptografik himoya mexanizmlaridan foydalanish mumkinligini inobatga olgan holda kriptografik-staganografik himoyalash usuli taklif etilgan, ushbu usul asosida ishlab chiqilgan himoya mexanizmi to‘laqonli himoyani ta’minlashi isbotlandi.*

Kalit so‘zlar: *Tarmoq steganografiyasi, Kripto-steganografik xavfsizlik usuli, RSA, AES.*

I. KIRISH

Tarmoq steganografiyasi katta hajmdagi ma’lumotlarni real vaqtda yashirib uzatish imkonini beradi. Ya’ni, steganografik usulga teskari usulni qo‘llash bilan ochiq kontent tarkibiga yashirib uzatilgan xabarni ajratib olish mumkin bo‘ladi.

Karthikeyan, Kosaraju va Guptalar tomonidan olib borilgan tadqiqot ishida maxfiy axborotni uzatish paytida uning xavfsizligini ta’minlash uchun kuchli shifrlash sxemasi va steganografik texnikaning kombinatsiyasi taklif qilingan [1]. Bu usulda maxfiy xabarni QR kodiga kodlashdan avval shifrlash uchun AES-128 shifrlash algoritmidan foydalanish taklif qilingan. Keyinchalik, UTF-8 formatidagi shifrlangan xabar ishlov berish uchun mos kelishini ta’minlash uchun asosiy Base64 formatiga aylantiriladi. Kodlangan tasvirni shifrlash orqali xavfsizlik darajasi oshiriladi. Keyin, shifrlangan QR kodi tegishli tashuvchiga berkitilib xavfsiz tarzda uzatiladi. Xabar oluvchi tomonidan qabul qilinganda, maxfiy ma’lumotlar dekodlash jarayoni orqali tashuvchidan ajratib olinadi.

Pillai, Mounika, Rao and Sriramlar tomonidan Matnli xabarlarni shifrlash uchun DES algoritmidan foydalangan holda tasvir steganografiyasi usuli taqdim etilgan [2]. Keyinchalik, K-means pikselli klasterlash usuli tasvirni bir nechta segmentlarga klasterlash va ma’lumotlarni har bir segmentga joylashtirish uchun ishlatilgan. Tasvirlarni segmentlash uchun bir nechta klaster algoritmlari ishlatilgan. Segmentlash piksellar ko‘rinishida taqdim etilgan katta ma’lumotlar to‘plamidan iborat. Bundan tashqari, har bir piksel uchta komponent qizil, yashil va ko‘k (RGB) ranglarga ega. Klasterlarni shakllantirgandan so‘ng, ular shifrlangan xabarni har bir klasterda yashirilishi kerak bo‘lgan K segmentga bo‘lish uchun LSB usulidan foydalanilgan.

Yuqorida keltirilgan steganografiya va kriptografiyani birlashtirishga asoslangan usullarning aksariyatida ma’lumotlarni shifrlash uchun simmetrik algoritmlar taklif qilingan. Ma’lumki, simmetrik shifrlash algoritmlarida kalitni qabul qiluvchiga xavfsiz yetkazib berish muammosi mavjud. Ushbu muammoni yechish uchun asimmetrik algoritmlardan foydalanish maqsadga muvofiq.

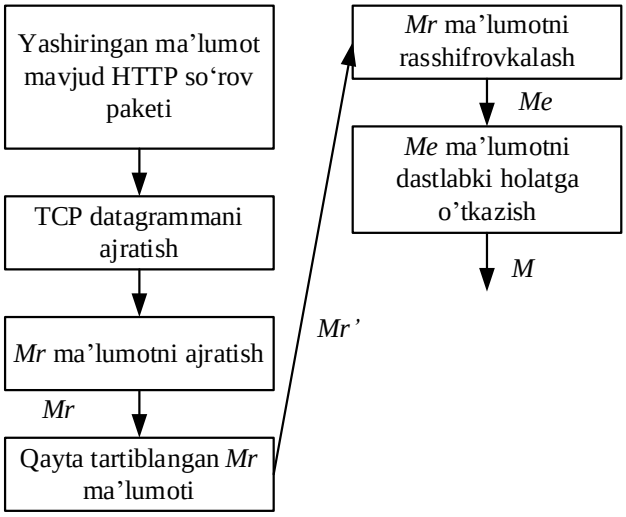
Ushbu muammoni bartaraf etish uchun biz taklif qilgan usul, kriptografiyaning simmetrik shifrlash algoritmlari asosan ma’lumotlarni shifrlashda, asimmetrik algoritmlar esa kalitlarni almashtirishda qo‘llaniladi. Shuning uchun kriptobardoshliligi yuqori simmetrik AES va asimmetrik RSA shifrlash algoritmlarini qo‘llash tarmoqda uzatilayotgan axborotning xavfsizligini oshiradi.

II. ASOSIY QISM

HTTP paketiga yashirilgan ma’lumotni qabul qiluvchi tomonidan ochish uchun yuqoridagi

jarayonlarning teskarisini amalga oshirish kerak. Ma’lumot yashiringan paketlar tarmoq kartasi orqali qabul qiluvchiga keladi. Tarmoq kartasi orqali ko‘plab paketlar o‘tganligi sababli, HTTP paketini yashirin ma’lumotlar bilan imkon qadar tezroq to‘ldirish uchun filtrlash modelini o‘rnatilishi kerak. Yashirin ma’lumotlar GET so‘rov paketidan quyida keltirilgam bosqichlarda ajratib olinadi. Yashirilgan ma’lumotni ajratib olish bosqichlari 1-rasmda ko‘rsatilgan algoritm asosida amalga oshiriladi:

1. GET so‘rov paketini qabul qilish tugagandan so‘ng, ushbu paketning TCP datagrammasi ajratib olinadi;
2. Qabul qilingan paketdan “X” va (\r\n) oralig‘idagi maxfiy ma’lumot M_r ajratib olinadi.
3. Ma’lumot M_r qayta tartiblanib, M_e ma’lumot hosil qilinadi.
4. Simmetrik kalit k yordamida M_e deshifrlanadi va M_c siqilgan ma’lumot hosil qilinadi.
5. M_c siqilgan ma’lumotni ajratish orqali M maxfiy ma’lumot olinadi.



1-rasm. Yashirilgan axborotni ajratib olish jarayoni.

Shaffoflik. Yashirin ma’lumotlar mijoz va web-server o‘rnatgan aloqa havolalariga qo‘yiladi. Server HTTP so‘rov paketiga yashirilgan ma’lumotni joylashtiradi, bu oddiy aloqaga ta’sir qilmaydi. Ya’ni, mijoz HTTP paketiga maxfiy ma’lumotlarni yashirib web-serverga o‘tkazilishini bilmaydi.

Maxfiy ma’lumotlarning shaffofligi buzg‘unchi uchun qulay. Maxfiy ma’lumotlar mijozdan serverga HTTP paketiga kiritiladi va umumiy kanal orqali uzatiladi, bu esa buzg‘unchining e’tiborini chetlab o‘tishga imkon beradi.

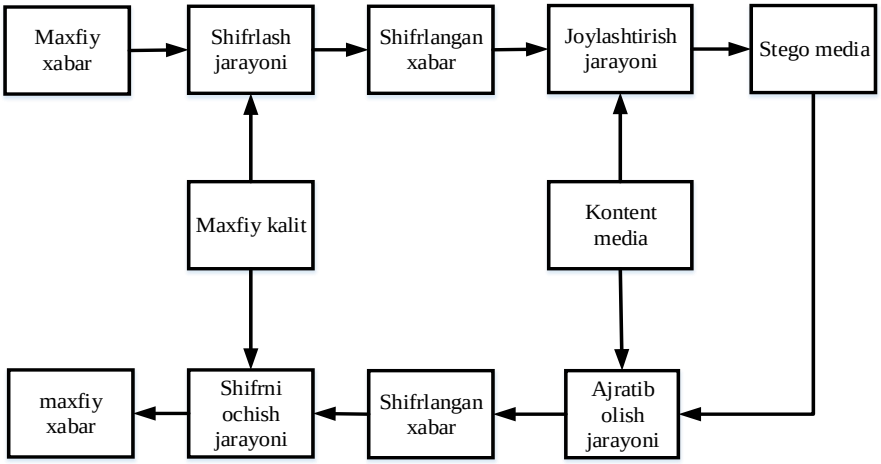
Taklif etilayotgan algoritmning yashirish qobiliyati GET so‘rov paketning uzunligiga bog‘liq. Uni aniqlash uchun yuqorida aytilganidek, 100 ta turli web-sayt ishtirokida tahlil amalga oshirildi. Tadqiqot mobaynida HTTP paketining maksimal hajmi 1514 bayt, minimal hajmi esa 150 bayt o‘lchamda bo‘lganligi kuzatildi. Buzg‘unchining e’tiborini jalb qilmaslik uchun yashirin ma’lumotni tashuvchi GET so‘rov paketining maksimal hajmi 1514 baytdan oshirmaslik kerakligi aniqlandi.

Tarmoq steganografiyasi usullaridan foydalanib uzatilayotgan paketlarni tutib, uning tarkibidan yashirilgan xabarni topish imkoniyati mavjud. Shuning uchun, taklif qilingan real vaqtda ma’lumotni yashirish algoritmi tarkibida kriptografik shifrlash usulidan foydalanish maqsadga muvofiq. Ushbu masala hal qilish uchun kriptosteganografiya usulidan foydalanib ikkalasini birga qo‘llash usuli ishlatilsa maqsadga muvofiq bo‘ladi.

Ma’lumki, kriptografiyada ruxsatsiz o‘qishdan himoyalash maxfiy xabarlar ma’nosini o‘zgartirish orqali amalga oshiriladi. Shuningdek, kriptografiya ma’lumotlarning yaxlitligi, obyektning va ma’lumotlarning haqiqiyligi tekshirish kabi axborot xavfsizligi bilan bog‘liq masalalarni yechadi. Biroq, shifrlab uzatilgan xabarlar o‘rtada turib tinglovchi shaxslar uchun muhim bo‘lganligi uchun ularni kalitsiz ochishga qaratilgan kriptotahlil usullari ham rivojlangan. Kriptotahlil usullari yordamida shifrlangan xabarlarni kalitsiz ochish imkoniyati mavjud. Shuning uchun shifrlangan xabarlarni steganografik usullar

yordamida yashirib uzatish uning xavfsiz yetib borish imkoniyatini oshiradi.

Shu kunga qadar, ko‘plab kripto-steganografik usullar ishlab chiqilgan. Umumiy holda kriptografik va steganografik himoya usullarining birgalikda foydanishning sxemasi 2-rasmda keltirilgan.



2-rasm. Steganografiya va kriptografiyani birlashtirish sxemasi.

Hingmire, Ojha va boshqalar tomonidan olib borilgan tadqiqot ishida kriptografiya va steganografiyaning o‘ziga xos zaif tomonlari tufayli ma’lumotlarni xavfsiz uzatish uchun etarli emasligi aytilgan [3]. Shuning uchun ikkila usulni birlashtirishga asoslangan tizim taklif qilingan. Unda uchinchi tomon tizim xavfsizligini buzishi va maxfiy ma’lumotlarni olishi deyarli imkonsiz. Taklif etilgan tizimda shifrlash jarayoni uchun Twofish algoritmi, steganografiya uchun esa Adaptiv B45 algoritmi ishlatilgan.

Ma’lumotlarni yashirish uchun Xaffman kodlash usuliga asoslangan zamonaviy usul R. Das va T. Tuithunglar tomonidan taqdim etilgan [4]. Bu usulda mxn o‘lchamdagi kontent rasm, maxfiy tasvir esa pxq o‘lchamida olingan. Shundan so‘ng, maxfiy tasvirda Xaffman kodlash jarayoni amalga oshirilgan va maxfiy tasvirni Xaffman kodining har bir bitini kontent rasmga joylashtirish uchun LSB algoritmidan foydalanilgan.

LSBga asoslangan ma’lumotlarni joylash-tirishdan oldin maxfiy ma’lumotlarni shifrlash uchun Blowfish algororitmini qo‘llash yondashuvi T.Barhoom va S. Mousalar tomonidan taklif qilingan [5].

S.E. Thomas, S.T. Philip va boshqalar maxfiy ma’lumotlarni shifrlash uchun AES va xeshlash uchun SHA-1 algoritmlaridan foydalanib tashqi hujumlarning oldini olish usulini taklif etishgan [6].

Keyinchalik, ular LSB usuli yordamida rasm ma’lumotlarni shifrlashgan. Xabarni tiklash uchun qabul qiluvchi jo‘natuvchi tomonidan taqdim etilgan xesh qiymatni tekshirishi kerak. Maxfiy ma’lumotlarni yashirish uchun har xil turdagi kontentlardan foydalanish mumkin, bu esa ko‘proq darajadagi xavfsizlikni ta’minlashga yordam bergan.

Shuningdek, steganografiya va kripto-grafiyaning qiyosiy tahlili Almuhammadi va boshqalar tomonidan amalga oshirilgan [7]. Ular kriptografik va steganografik usullarni bir tizimda birlashtirishning bir necha usullarini tadqiq etgan. Bundan tashqari, mualliflar tomonidan ushbu usullarning tasnifi va foydalanish mumkin bo‘lgan kriptografik, steganografik algoritmlar va kontent sifatida ishlatiladigan fayl turi bo‘yicha ma’lumotlar keltirilgan. Shunday qilib, ular kriptografiya usullari steganografiya usullariga qaraganda keng tarqalgan va shifrlash yaxshi xavfsizlikni ta’minlaydi degan xulosaga kelishgan bo‘lsada, [10] da steganografik usullarning yagona afzalligi sifatida maxfiy ma’lumotlarning yashirib uzatilishi ko‘rsatilgan.

Yuqorida keltirilgan steganografiya va kriptografiyani birlashtirishga asoslangan usullarning aksariyatida ma’lumotlarni shifrlash uchun simmetrik algoritmlardan foydalanishni taklif qilgan. Ma’lumki, simmetrik shifrlash algoritmlarida kalitni qabul qiluvchiga xavfsiz yetkazib berish muammosi mavjud. Ushbu muammoni yechish uchun asimmetrik algoritm-lardan foydalanish maqsadga muvofiq.

III. HISOBLASH METODI

Kriptografiyaning simmetrik shifrlash algoritmlari asosan ma’lumotlarni shifrlashda, asimmetrik algoritmlar esa kalitlarni almashishda

qo‘llaniladi. Shuning uchun kriptobardoshligi yuqori bo‘lgan simmetrik blokli shifrlash algoritmidan (O‘z DST 1105:2009, ГОСТ 34.12-2018, AES, Camellia va hak.) va bardoshli ochiq kalitli shifrlash algoritmidan (RSA, El-gamal va hak.) foydalanish tavsiya etiladi.

Umuman olganda kriptografiya va stegonografiyani birgalikda qo‘llash quyidagi standart formulaga asoslanadi:

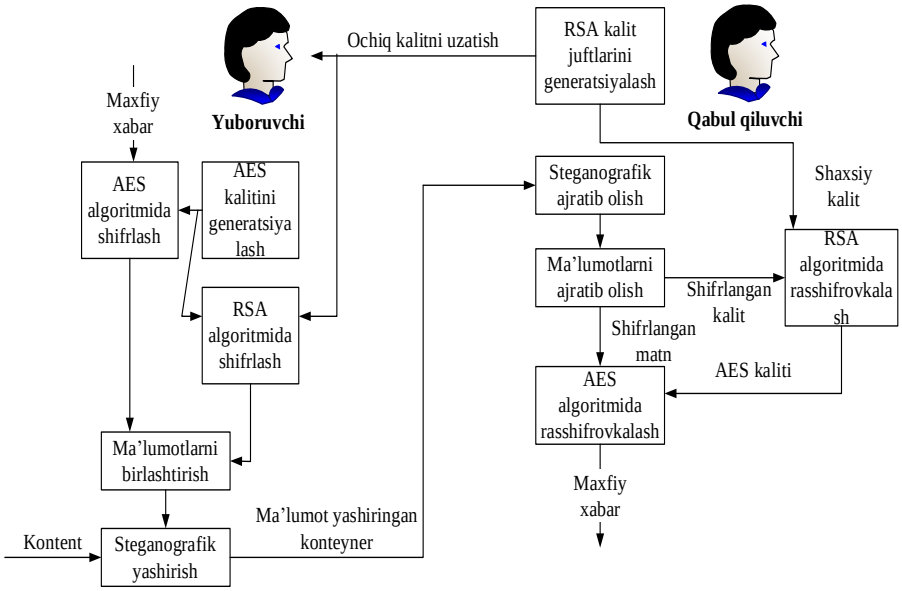
$$C' = E_m\left(C, E\left(S, k_1\right), k_2\right), \qquad (1)$$

bu yerda, S - maxfiy ma’lumot, C- kontent, E – shifrlash funksiyasi, k_1 va k_2 shifrlash va steganografik kalitlar, E_m – biriktirish (yashirish) funksiyasi.

Rasshifrovkalash uchun esa, yuqoridagiga teskari formuladan foydalaniladi:

$$s_r = D\left(E_x\left(C', k_2\right), k_1\right), \qquad (2)$$

bu yerda, D– rasshifrovka funksiyasi, E_x – ajratib olish funksiyasi [8].



3-rasm. Kripto-steganografik xavfsizlik usuli.

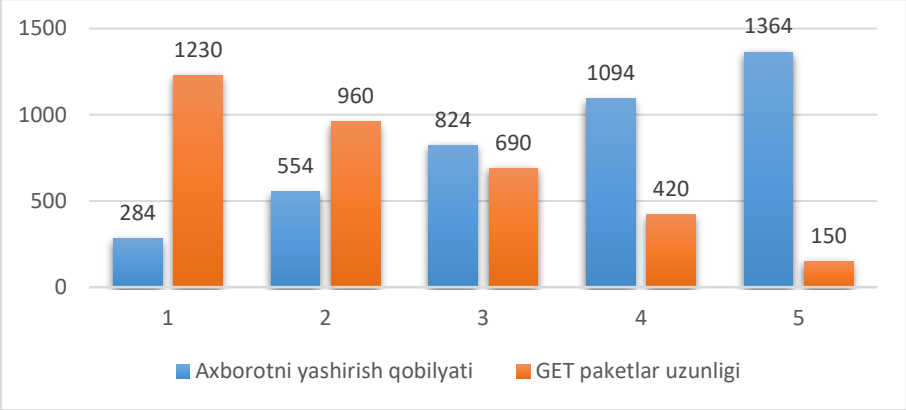
Taklif etilgan kriptografik-stegonografik himoyalash sxemasi uchun AES simmetrik shifrlash algoritmi va RSA ochiq kalitli shifrlash algoritmi tanlab olindi. [9]. Umumiy holda taklif etilgan sxemaning ishlash bosqichlari quyidagicha (3-rasm):

- axborotni qabul qiluvchi RSA algoritmida kalit juftliklarini yaratadi va ochiq kalit sertifikatini xabar yuboruvchiga uzatadi;
- axborotni yuboruvchi tasodifiy AES256 kalitini yaratadi;
- yuboriladigan axborot AES algoritmi yordamida, AES shifrlash kaliti esa qabul qiluvchining ochiq kaliti yordamida shifrlanadi;
- shifrlangan kalit va maxfiy xabar kontentga steganografik usullar yordamida yashiriladi;
- qabul qiluvchi shifrlangan ma’lumot va shifrlangan kalitni qabul qiladi;
- kontentdan yashiringan maxfiy xabar steganografik usul yordamida ajratiladi;
- qabul qiluvchi RSA algoritmi yordamida shifrlangan kalitni rasshifrovkalaydi;
- ma’lumotlar qabul qiluvchi tomonidan rasshifrovkalangan AES kaliti yordamida ochiladi;
- rasshifrovkalangan ma’lumotlarning ichidan steganografik usul yordamida yashirilgan xabar ajratib olinadi.

Yuqorida keltirilgan usul, malumotni yuqori darajadagi himoyasini ta’minlashda kriptografiya va steganografiya usullarining afzalliklarini o‘zida birlashtirgan bo‘lib, uning bardoshliligi foydalanilgan algoritmlarning kriptobardoshligiga bo‘g‘liq.

IV. NATIJALAR TAHLILI

(2) bo‘yicha HTTP paketining o‘lchami va yashirish qobiliyati o‘rtasidagi bog‘liqlikni quyida keltirilganidek ifodalash mumkin (4-rasm).



4-rasm. GET paketining o‘lchami va yashirish qobiliyati.

Steganografiyani va kriptografiyani birgalikda ishlatishni taklif qilishda ularning har birining imkoniyatlari, afzallik va kamchiliklarini solishtirish muhim. Quyidagi 1-jadvalda imkoniyatlari, muammolari, bardoshliligi va boshqa mezonlari bo‘yicha ikkila usulning qisqacha tahlili keltirilgan.

1-jadval. Kriptografik va steganografik usullarning qiyosiy tahlili

Mezon / usul	Kriptografiya	Steganografiya
Maqsadi	Ma’lumotlarni himoya qilish	Yashirin aloqa
Kirish parametrlari	Bitta	Kamida ikkita
Chiqish	Shifrlangan matn	Stego fayl
Kalit	Majburiy	Ixtiyoriy
Tashuvchi	Odatda matn	Matn, xabar, audio, video, protokol va DNK
Xavfsizlik xizmati	Autentifikatsiya, maxfiylik, identifikatsiya, ma’lumotlar yaxlitligi va rad etmaslik	Identifikatsiya, autentifikatsiya, maxfiylik
Uzatilgan maxfiy axboortning ko‘rinishi	Har doim	Hech qachon
Tahlillash sohasi	Kriptoanaliz	Stegoanaliz
Hujumlar	Tajovuzkor maxfiy xabarni tushuna olsa, buziladi	Hujumchi steganografiya qo‘llanganligini aniqlaganida buziladi
Ko‘z bilan aniqlash	Ha, yashirin xabar boshqa yo‘l bilan o‘zgartiriladi.	Yo‘q, maxfiy xabar kontent tarkibiga yashiriladi
Axborot uzatishning muvaffaqiyatsizligi	Ruxsatsiz deshifrlanganda	Ruxsatsiz aniqlanganda
Yashirin ma’lumotlar	Oddiy matn	Foydali yuk maydoni
Ilovalar	Axborot xavfsizligi	Axborot xavfsizligi
Texnologiyaga xos muammolar	Kalit taqsimoti	Kalitlarni taqsimlash (kalitsiz foydalanishdan tashqari)

Tahlillar natijasi shuni ko‘rsatadiki steganografiya va kriptografiya axborot xavfsizligi uchun alohida-alohida ishlatilganda to‘lato‘kis emas. Shuning uchun ikkala usulni birlashtirish orqali yanada ishonchli va kuchli mexanizmga erishish mumkin. Ushbu usullarni birlashtirish yaxshilangan axborot xavfsizligini ta’minlaydi va muhim ma’lumotlarni ochiq kanallar orqali uzatish xavfsiz uzatish imkoniyatini beradi.

V. XULOSA

Steganografik himoyadaga mavjud kamchiliklarni bartaraf etishda kriptografik himoya mexanizmlaridan foydalanish mumkinligini inobatga olgan holda kriptografik-staganografik himoyalash usuli taklif etilib, ushbu usul asosida ishlab chiqilgan himoya mexanizmi to‘laqonli himoyani ta’minlashi isbotlandi. Ushbu usullarni birlashtirish yaxshilangan axborot xavfsizligini ta’minlaydi va muhim ma’lumotlarni ochiq kanallar orqali uzatish xavfsiz uzatish imkoniyatini berdi. Ma’lumotni uzatishda foydalanilgan kontent hajmi va yashirish sig‘imi parametrlari orqali steganografik algoritmlarning yashirish samaradorligi hisoblab chiqildi. Ishlab chiqilgan usul turli stegonografik usullar uchun

axborotni yashirish samaradorligini aniqlash imkonini yana ham oshirib berdi.

ADABIYOTLAR

[1] *Karthikeyan B, Kosaraju A C and Gupta S* 2016 March Enhanced security in steganography using encryption and quick response code In Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on (pp. 2308-2312) IEEE.

[2] Pillai B, Mounika M, Rao P J and Sriram P 2016 September Image steganography method using K-means clustering and encryption techniques In Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on (pp. 1206-1211) IEEE.

[3] *Hingmire A, Ojha S, Jain C, Thombare K* 2016 Image steganography using adaptive b45 algorithm combined with pre-processing by twofish encryption International Educational Scientific Research Journal 2 4.

[4] *L. M. Marvel, C. G. Boncelet and C. T. Retter*, "Spread spectrum image steganography," in IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug. 1999, doi: 10.1109/83.777088.

[5] *Barhoom T S and Mousa S M A* 2015 A Steganography LSB technique for hiding Image within Image Using blowfish Encryption Algorithm Int. J. Res. Eng. Sci, 3 61-66.

[6] *Thomas S E, Philip S T, Nazar S, Mathew A and Joseph N* 2012, May Advanced cryptographic steganography using multimedia files In International Conference on Electrical Engineering and Computer Science (ICEECS-2012).

[7] *Almuhammadi S and Al-Shaaby A* 2017 A survey on recent approaches combining cryptography and steganography Computer Science Information Technology (CS IT).

[8] *Pant, V.K.; Prakash, J.; Asthana, A.* Three step data security model for cloud computing based on RSA and steganography. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 8–10 October 2015; pp. 490–494.

[9] *Ganivev, Abduhalil, Obid Mavlonov, and Baxtiyor Turdibekov*. "Improving data hiding methods in network steganography based on packet header manipulation." 2021 International Conference on Information Science and Communications Technologies (ICISCT). IEEE, 2021.

[10] *Mavlonov O.* Advancements in retransmission steganography: an enhanced algorithm and its steganalysis approaches //International Scientific and Current Research Conferences. – 2023. – С. 127-131.

Поступила в редакцию 29.01.2024

Citation: *Ganiyev, A., Mavlonov, O., Shodmonov, D., & Maxmudov, J.* (2024). Kompyuter tarmoqlarida uzatilayotgan axborotni kriptografik himoyalash usuli. Международный Журнал Теоретических и Прикладных Вопросов Цифровых Технологий, 7(1), 73–79. https://doi.org/10.62132/ijdt.v7i1.166

METHOD OF CRYPTOGRAPHIC PROTECTION OF INFORMATION TRANSMITTED ON COMPUTER NETWORKS

Ganiev A.A.[1], Mavlonov O.N.[2], Shodmonov D.A.[2], Makhmudov J.I.[2]
[1] Tashkent University of information technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
[2] Samarkand branch of Tashkent university of information technologies named after Muhammad al-Khwarizmi, Samarkand, Uzbekistan
mavlonov8686@gmail.com

Abstract. *This paper presents a cryptosteganographic approach, which involves the use of cryptographic mechanisms in order to eliminate the known shortcomings of steganographic protection. The proposed method demonstrates the full effectiveness of protection by hiding secret messages in digital content in such a way that detection of such messages is extremely difficult. Steganography, as a technique, strives to mask secret data within a regular message while keeping its structure unchanged, making changes difficult to detect. It is important to note that the security of a steganographic method depends on its secrecy, while steganalysis methods aim to discover the patterns of a hidden message.*

Keywords: *Network steganography, Crypto-steganographic security method, RSA, AES.*

МЕТОД КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО КОМПЬЮТЕРНЫМ СЕТИ

Ганиев А.А.[1], Мавлонов О.Н.[2], Шодмонов Д.А.[2], Махмудов Ж.И.[2]

[1] Ташкентский университет информационных технологий имени Мухаммада ал-Хорезми, Ташкент, Узбекистан
[2] Самаркандский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хорезми, Самарканд, Узбекистан
mavlonov8686@gmail.com

Аннотация. *В данной работе представлен криптостеганографический подход, который предполагает использование криптографических механизмов в целях устранения известных недостатков стеганографической защиты. Предложенный метод демонстрирует полную эффективность защиты путем скрытия секретных сообщений в цифровом контенте таким образом, чтобы обнаружение таких сообщений оказывалось чрезвычайно затруднительным. Стеганография, как метод, стремится к маскировке секретных данных внутри обычного сообщения, при этом сохраняя его структуру неизменной, что затрудняет обнаружение изменений. Важно отметить, что безопасность стеганографического метода зависит от его секретности, в то время как методы стегоанализа направлены на обнаружение схем скрытого сообщения.*

Ключевые слова: *Сетевая стеганография, Криптостеганографический метод защиты, RSA, AES.*