TASVIRLARNI SHIFRLASHDA KRIPTO TAHLIL VA XAVFSIZLIK JIHATIDAN BAHOLASH MEZONLARI

Asadbek Ne'matjonov Umidjon o'g'li,
Andijon davlat universiteti magistranti
asadbeknematjonov02@gmail.com

ANNOTATSIYA

Ushbu maqolada raqamli tasvirlarni shifrlashda qo'llaniladigan kriptografik algoritmlar va ularning xavfsizlik jihatidan baholash mezonlari tadqiq etilgan. Asosiy e'tibor simmetrik (AES-256, DES) va asimmetrik (RSA-2048, ECC) shifrlash usullarining tasvirlarni muhofaza qilishdagi samaradorligiga qaratilgan. Baholash mezonlari sifatida entropiya tahlili, piksellar korrelyatsiyasi, NPCR/UACI ko'rsatkichlari, gistogramma tekisligi, kalit sezgirligi hamda statistik hujumlarga chidamlilik ko'rib chiqilgan. Tadqiqot natijalari ushbu mezonlar asosida algoritmlarni qiyosiy tahlil qilish metodologiyasini shakllantiradi.

Kalit so'zlar: tasvirni shifrlash, kriptografik algoritm, AES, RSA, kripto tahlil, xavfsizlik mezonlari, entropiya, statistik hujum, NPCR, UACI.

ABSTRACT

This article investigates cryptographic algorithms used in digital image encryption and their security evaluation criteria. The study focuses on the effectiveness of symmetric (AES-256, DES) and asymmetric (RSA-2048, ECC) encryption methods in protecting digital images. Evaluation criteria such as entropy analysis, pixel correlation, NPCR/UACI indicators, histogram uniformity, key sensitivity, and resistance to statistical attacks are examined. The research results form a comparative analysis methodology for assessing algorithms based on these criteria.

Keywords: image encryption, cryptographic algorithm, AES, RSA, cryptanalysis, security criteria, entropy, statistical attack, NPCR, UACI.

1. KIRISH

Zamonaviy axborot texnologiyalarining jadal rivojlanishi bilan raqamli tasvirlarni uzatish va saqlash masalasi tobora muhim ahamiyat kasb etmoqda. Tibbiy tasvirlar, harbiy razvedka ma'lumotlari, moliyaviy hujjatlar va shaxsiy fotosuratlar kabi nozik ma'lumotlarni ruxsatsiz kirishdan himoya qilish zaruriyati kriptografik shifrlash usullarini keng qo'llashga olib keldi.

Tasvirlarni shifrlash — bu tasvirning piksellar qiymatlarini yoki tuzilmasini kriptografik algoritm yordamida o'zgartirish jarayonidir. Natijada asl tasvirni faqat maxfiy kalit egasi tiklay oladi. Biroq, tasvirlarni shifrlash oddiy matnlarni shifrlashdan bir qator xususiyatlari bilan farq qiladi: tasvirlar katta hajmda bo'ladi, kuchli piksellar korrelyatsiyasiga ega va ko'pincha real vaqt rejimida qayta ishlanishi lozim.

Tadqiqotning dolzarbligi: Ma'lumotlarga noqonuniy kirish, kiberjosuslik va raqamli tasvirlarni soxtalashtirishga qaratilgan hujumlar soni yil sayin oshib bormoqda. Shu bois, tasvirlarni shifrlash algoritmlarini to'g'ri tanlash va ularning xavfsizligini ishonchli baholash metodologiyasini ishlab chiqish bugungi kunda nihoyatda zarur.

Tadqiqot maqsadi: Tasvirlarni shifrlashda ishlatiladigan kriptografik usullarni kripto tahlil nuqtai nazaridan o'rganish va ularning xavfsizligini baholash uchun kompleks mezonlar tizimini shakllantirish.

2. ADABIYOTLARNI O'RGANISH

Tasvirlarni shifrlash sohasidagi ilmiy tadqiqotlar o'tgan asrning oxirlaridan boshlab faol rivojlana boshladi. Dastlabki ishlar AES va DES kabi simmetrik algoritmlarni tasvirlarga bevosita qo'llashga qaratilgan edi [1, 2]. Biroq bu yondashuv tasvirlarning statistik xususiyatlarini yetarli darajada buzmasligini

ko’rsatdi, chunki shifrlangan tasvirda ham qo’shni piksellar o’rtasida ma’lum ma’noda korrelyatsiya sezilib qolardi.

Keyinchalik J. Fridrich xaotik tizimlarni tasvirlarni shifrlashda qo’llash konsepsiyasini taklif etdi [3]. Shundan so’ng turli xaotik xaritalar (Lorenz attraktori, Logistik xarita) asosidagi shifrlash sxemalari keng tarqaldi. Bu yondashuvning o’ziga xos afzalligi — yuqori sezgirlik va keng kalit fazosini ta’minlash qulayligida edi. So’nggi yillarda esa chuqur o’rganish (Deep Learning) va neyron tarmoqlar asosidagi yangi shifrlash hamda kripto tahlil usullari paydo bo’ldi [4, 5].

Garchi xalqaro miqyosda bu borada ko’plab izlanishlar olib borilayotgan bo’lsa-da, respublikamiz sharoitiga mos keluvchi, xususan, mahalliy tizimlar talablariga javob beradigan tasvirlarni shifrlash hamda ularni baholash metodologiyasini shakllantirish masalasi o’z dolzarbligini saqlab qolmoqda. Kriptografiyaning asosiy qoidalaridan biri bo’lgan “Kerkxoffs prinsipi” ta’kidlaganidek, tizim xavfsizligi faqatgina kalitning maxfiyligiga asoslanishi kerak [6].

3. METODOLOGIYA

3.1. Tadqiqot yondashuvi

Tadqiqot doirasida quyidagi metodologiyadan foydalanildi:

- Tasvirlarni shifrlashda qo’llaniladigan algoritmlarni tasniflovchi xalqaro adabiyotlarni tahlil qilish;
- Baholash mezonlarini aniqlash va ularni matematik formulalar asosida tizimlashtirish;
- AES-256, RSA-2048 va xaotik tizimlar asosidagi algoritmlarni tanlangan mezonlar bo’yicha eksperimental taqqoslash.

3.2. Eksperimental ma’lumotlar

Taqqoslash uchun USC-SIPI ma’lumotlar to’plamidan standart 256×256 va 512×512 o’lchamdagi tasvirlar (Lena, Baboon va boshqalar) ishlatildi. Har bir tasvir 50 marta turli kalitlar bilan shifrlandi va o’rtacha qiymatlar hisobga olindi. Barcha

tajribalar Python 3.11 muhitida, NumPy, SciPy va OpenCV kutubxonalaridan foydalangan holda amalga oshirildi.

4. TASVIRLARNI SHIFRLASHDA XAVFSIZLIK BAHOLASH MEZONLARI

4.1. Entropiya tahlili

Shennon axborot entropiyasi shifrlangan tasvirning tasodifiylik darajasini o'lchaydi. Ideal shifrlangan tasvir uchun entropiya maksimal qiymat — 8 bitga teng bo'lishi lozim (256 ta intensivlik darajasi uchun). AES-256 bilan shifrlangan tasvirlar odatda 7.999 dan yuqori entropiya ko'rsatkichiga ega bo'ladi. Entropiyaning 7.9 dan past bo'lishi algoritmning zaifligi belgisi hisoblanadi va statistik hujumlar uchun imkon yaratadi.

4.2. Piksellar korrelyatsiyasi tahlili

Asl tasvirda qo'shni piksellar o'rtasida doimo yuqori korrelyatsiya mavjud (odatda 0.95–0.99 atrofida). Sifatli shifrlash algoritmining vazifasi ana shu aloqadorlikni uzish va korrelyatsiyani nolga yaqin qiymatga tushirishdir. Agar ko'rsatkich -0.01 dan +0.01 gacha bo'lgan oraliqdan chiqsa, algoritm tasvirni yetarli darajada tarqatib yubora olmayapti, degan xulosaga kelinadi.

4.3. NPCR va UACI tahlili

NPCR (Number of Pixel Change Rate) va UACI (Unified Average Changing Intensity) — bir piksel o'zgarganda shifrlangan tasvirda qanday katta o'zgarish ro'y berishini o'lchovchi mezonlardir. Bu ko'rsatkichlar differensial hujumlarga chidamlilikni baholashda asosiy vosita hisoblanadi. Ideal holatda NPCR kamida 99.6% va UACI taxminan 33.46% bo'lishi kerak. Bu qiymatlardan og'ish algoritmning differensial kripto tahlilga dosh bera olmasligini bildiradi.

4.4. Gistogramma tekisligi

Asl tasvirning gistogrammasi odatda ma'lum bir vizual shaklga mos ravishda notekis taqsimlanadi. Shifrlangan tasvirning gistogrammasi esa deyarli tekis

bo'lishi, ya'ni barcha intensivlik qiymatlari taxminan bir xil chastotada uchrashi kerak. Gistogramma tekisligi xi-kvadrat (chi-square) testi yordamida baholanadi.

4.5. Kalit sezgirligi va PSNR/SSIM ko'rsatkichlari

Kalit sezgirligi — bitta bitning o'zgarishi shifrlangan matnda qanchalik o'zgarish yasashini ko'rsatadi.

Shuningdek, PSNR (Peak Signal-to-Noise Ratio) shifrlangan tasvir sifatini baholash uchun ishlatiladi (shifrlangan holatda past ko'rsatkich bo'lishi ma'qul). SSIM (Structural Similarity Index) esa asl va shifrdan chiqarilgan tasvirlar o'rtasidagi o'xshashlikni o'lchaydi va u mukammal shifrdan chiqarish jarayoni uchun aynan 1 ga teng bo'lishi shart.

5. NATIJALAR VA MUHOKAMA

Tajriba natijalari ko'rsatishicha, AES-256 algoritmi deyarli barcha baholash mezonlari bo'yicha eng yuqori ko'rsatkichlarga ega. Entropiya tahlilida AES-256 orqali shifrlangan tasvirlar uchun o'rtacha 7.9993 bit/piksel qiymatiga erishildi — bu ideal 8.0 qiymatiga juda yaqin natijadir.

Piksellar korrelyatsiyasi bo'yicha AES-256 gorizontal va vertikal yo'nalishlarda mos ravishda r = -0.0021 va r = 0.0018 ko'rsatkichlarini namoyon etdi. Xaotik tizimlar asosidagi algoritm ham amaliy jihatdan nol korrelyatsiyaga erisha oldi. NPCR (99.63%) va UACI (33.51%) tahlili shuni ko'rsatdiki, AES-256 differensial hujumlarga juda chidamli.

RSA-2048 esa to'g'ridan-to'g'ri tasvirga qo'llanilganda o'zining sekinligi bilan muammoga duch keldi. 512×512 o'lchamdagi tasvirni shifrlash uchun RSA qariyb 4.7 soniya sarflagan bo'lsa, AES-256 bunga atigi 0.023 soniya sarfladi. Bu holat amaliyotda nima uchun gibrid shifrlash tizimlaridan (ya'ni RSA faqat kalit almashish uchun, AES esa ma'lumotning o'zini shifrlash uchun) foydalanish maqsadga muvofiq ekanligini isbotlaydi.

6. XULOSA

Tadqiqot davomida tasvirlarni shifrlashda xavfsizlikni baholash mezonlari tizimli tahlil qilindi va quyidagi asosiy xulosalar shakllantirildi:

- Tasvirlar xavfsizligini baholash uchun faqat bitta mezon (masalan, faqat korrelyatsiya) yetarli emas; jarayon entropiya, NPCR/UACI va gistogramma mezonlarini o'z ichiga olgan kompleks yondashuvni talab qiladi.
- AES-256 algoritmi barcha mezonlar bo'yicha ishonchli natijalar ko'rsatib, tasvirlarni real vaqt rejimida shifrlash uchun eng maqbul yechim bo'lib qolmoqda.
- Xaotik tizimlar yaxshi raqobatbardosh bo'lsa-da, ularning matematik davriyligi bilan bog'liq masalalar hali ham qo'shimcha o'rganishni talab qiladi.
- Amaliyotda ishlash tezligi va xavfsizlikni birdek ta'minlash uchun gibrid (AES + RSA) tizimlarini joriy etish eng samarali yo'ldir.

ADABIYOTLAR RO'YXATI

1. National Institute of Standards and Technology. (2001). Advanced Encryption Standard (AES). FIPS Publication 197. NIST, Gaithersburg, MD.
2. Shannon, C. E. (1949). Communication Theory of Secrecy Systems. Bell System Technical Journal, 28(4), 656–715.
3. Fridrich, J. (1998). Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. International Journal of Bifurcation and Chaos, 8(6), 1259–1284.
4. Zhang, X., & Wang, X. (2019). Multiple-Image Encryption Algorithm Based on DNA Encoding and Chaotic System. Multimedia Tools and Applications, 78(6), 7841–7869.
5. Hua, Z., Jin, F., Xu, B., & Huang, H. (2019). 2D Logistic-Sine-Coupling Map for Image Encryption. Signal Processing, 149, 148–161.
6. Kerckhoffs, A. (1883). La Cryptographie Militaire. Journal des Sciences Militaires, 9, 5–38.