Qabul qilindi: 23-noyabr 2026-yil • Ma’qullandi: 25-noyabr 2026-yil • Nashr qilindi: 27-noyabr 2026-yil

KRIPTOGRAFIYADA TASVIR VA SIGNALNI KODLASH TEXNOLOGIYALARI

Xakimov Kamronbek
Farg‘ona davlat texnika universiteti, 3-kurs bakalavr talabasi
Dalibekov L. R.
Ilmiy rahbar

Annotatsiya. Maqolada raqamli tasvir va signallarni kodlash hamda kriptografik himoyalash usullari tahlil qilinadi. Kodlash va shifrlash tushunchalari farqlanib, AES ning ECB, CBC va CTR rejimlari, permutatsiya–substitutsiya sxemalari hamda xaotik xaritalar solishtiriladi. 256×256 sintetik tasvirda AES-128 bilan o‘tkazilgan tajriba entropiya, korrelyatsiya, χ^2, NPCR, UACI va tezlik bo‘yicha baholanadi. Statistik ko‘rsatkichlar xavfsizlikni to‘liq ifodalamasligi va rejim tanlovi hal qiluvchi ekani ko‘rsatiladi.

Kalit so‘zlar: kriptografiya; tasvirni shifrlash; signalni kodlash; AES; ish rejimlari; xaotik xarita; entropiya; NPCR va UACI.

Kirish

Raqamli tasvir, audio va video axborot oqimining katta qismini tashkil etadi: ular tibbiyot, video kuzatuv, masofaviy ta’lim va bulutli xizmatlarda saqlanadi va uzatiladi. Tasvir matndan farqli o‘laroq hajmi katta, qo‘shni piksellari esa o‘zaro kuchli bog‘langan, shu sababli matn uchun mo‘ljallangan usullarni mexanik qo‘llash shifrmatnda tasvir tuzilishini oshkor qilishi mumkin [3, 5]. Bu tasvir va signallarni kodlash hamda himoyalash texnologiyalarini tizimli o‘rganishni dolzarb qiladi.

Tadqiqot maqsadi — raqamli tasvir va signallarni kodlash hamda shifrlash usullarini tahlil qilish va AES asosidagi shifrlash samaradorligini baholash. Vazifalar: (1) kodlash va shifrlashni farqlash; (2) AES, uning ish rejimlari, permutatsiya–substitutsiya va xaotik sxemalarni solishtirish; (3) baholash mezonlarini matematik ifodalash; (4) AES bilan tajriba o‘tkazib, natijalarni nazariy bayondan ajratib berish.

1. Kodlash va shifrlash tamoyillari

Kodlash axborotni boshqa shaklga o‘tkazadi va kalitga tayanmaydi: manba kodlash (JPEG, MP3, H.264) ortiqchalikni kamaytirib hajmni qisqartiradi, kanal kodlash xatolarni tuzatish uchun qo‘shimcha bitlar kiritadi. Shifrlash esa ma’lumotni faqat kalit egasi tiklay oladigan qiladi, ya’ni xavfsizlik kalit sirliligiga tayanadi. Shennon yaxshi shifrning ikki xossasini — chalkashtirish va diffuziyani — ta’riflagan [1]. Simmetrik algoritmlar (AES) bir kalit bilan ishlaydi va katta hajmli tasvir hamda signal uchun tez; assimetrik algoritmlar (RSA, ECC) kalitlar juftligiga tayanadi, sekinroq bo‘lgani uchun odatda tasvirning o‘zini emas, sessiya kalitini almashishda qo‘llanadi.

2. AES algoritmi va ish rejimlari

AES 128 bitli blok bilan ishlaydi, kalit 128, 192 yoki 256 bit bo‘lib, raundlar soni mos ravishda 10, 12 va 14 [2]. Blok 4×4 bayt holat matritsasiga joylanadi va har raundda SubBytes ($GF(2^8)$ da teskari element va affin almashtirish — substitutsiya), ShiftRows (qatorlarni siljitish — permutatsiya), MixColumns (ustunlarni aralashtirish — diffuziya; oxirgi raundda yo‘q) va AddRoundKey (raund kaliti bilan XOR) bajariladi [2, 4]. Maydon $x^8+x^4+x^3+x+1$ ko‘phad bo‘yicha quriladi. AES bitta blokni shifrlaydi, uzun tasvir uchun ish rejimi kerak [3]:

$$C_i = E_K(P_i) \quad (1)$$

$$C_i = E_K(P_i \oplus C_{i-1}),\ C_0 = IV \quad (2)$$

$$C_i = P_i \oplus E_K(T_i),\ T_i = \text{nonce} \parallel i \quad (3)$$

Bu yerda P_i — ochiq matn bloki, C_i — shifrmatn bloki, E_K — K kalitli AES shifrlash funksiyasi, IV — boshlang‘ich vektor, T_i — hisoblagich bloki, $\oplus$ — XOR. (1) ECB bir xil bloklarni bir xil shifrlaydi, shuning uchun tekis sohali tasvirda naqsh saqlanadi; (2) CBC bloklarni zanjirlaydi, lekin ketma-ket bajariladi; (3) CTR oqimli shifr kabi ishlaydi, parallellashadi, ammo nonce takrorlanmasligi shart [3].

3. Permutatsiya–substitutsiya va xaotik algoritmlar

Klassik sxema ikki bosqichli: piksellar o‘rni almashtiriladi (permutatsiya), so‘ng qiymatlari o‘zgartiriladi (substitutsiya), jarayon bir necha raund takrorlanadi [5].

Permutatsiya korrelyatsiyani buzadi, lekin gistogrammani o‘zgartirmaydi; substitutsiya gistogrammani tekislaydi. Xaotik sxemalarda boshqaruvchi ketma-ketlik dinamik tizimdan olinadi, masalan logistik va Arnold xaritalaridan [5, 6]:

$$x_{n+1} = \mu\, x_n(1 - x_n) \quad (4)$$

$$(x', y') = ((x + y) \bmod N, (x + 2y) \bmod N) \quad (5)$$

Bu yerda $x_n \in (0; 1)$ — holat, $\mu \in (3{,}57; 4]$ — xaotik rejimdagi parametr, (x, y) — piksel koordinatasi, N — tasvir tomoni. Bunday sxemalar tez va boshlang‘ich shartga sezgir, ammo kalit fazosi kichik bo‘lishi, chekli aniqlikda davriylik va kriptotahlil xavfi kuzatilgan; ular AES kabi standartlashtirilmagan [6, 7].

4. Audio va video signallarni himoyalash

Audio bir o‘lchamli oqim bo‘lgani uchun real vaqtda oqimli shifrlash (masalan, CTR) qulay. Video siqilgan bit oqimi tuzilishiga ega, shu sababli tanlama shifrlash qo‘llanadi: faqat muhim qism (tayanch kadrlar yoki DCT koeffitsiyentlari ishoralari) shifrlanadi. Bu hisoblash yukini kamaytiradi va kodek formatini saqlaydi, ammo ochiq qolgan qismdan ma’lumot sizib chiqishi xavfini tug‘diradi.

5. Baholash mezonlari va matematik asoslar

$$H = -\sum_{i=0}^{255} p_i \log_2 p_i \quad (6)$$

$$r = \operatorname{cov}(x, y) / (\sigma_x \sigma_y) \quad (7)$$

$$\chi^2 = \Sigma\, (f_i - e)^2 / e, \quad e = M \cdot N / 256 \quad (8)$$

$$NPCR = (1/(M \cdot N))\, \Sigma\, D(i, j) \times 100\ \% \quad (9)$$

$$UACI = (1/(M \cdot N))\, \Sigma\, |C_1(i, j) - C_2(i, j)| / 255 \times 100\ \% \quad (10)$$

Bu yerda p_i — i-kulrang sathining ehtimolligi (8 bitli tasvirda ideal H = 8 bit [1]); x, y — qo‘shni piksellar qiymatlari, σ — o‘rtacha kvadratik chetlanish; f_i — chastota, e — kutiladigan chastota (255 erkinlik darajasi va α = 0,05 da kritik qiymat 293,25); C_1, C_2 — ochiq tasvir bir bit farq qilgandagi shifrtasvirlar, M×N — o‘lcham; D(i, j) = 0 agar $C_1(i, j) = C_2(i, j)$, aks holda 1. Tasodifiy 8 bitli tasvir uchun NPCR ≈ 99,61 %, UACI ≈ 33,46 % kutiladi [9]. Bu ko‘rsatkichlar zarur, lekin yetarli emas: xavfsizlik kalit fazosi, ma’lum va tanlangan ochiq matnli hujumlarga chidamlilik hamda NIST SP 800-22 testlari [8] bilan ham baholanadi.

6. Amaliy tajriba (haqiqiy hisoblash natijalari)

Quyidagi raqamlar haqiqiy dasturiy hisoblashdan olingan. Tajriba Python 3.13 va cryptography kutubxonasida bajarildi: 256×256 o‘lchamli 8 bitli kulrang sintetik tasvir (gradiyent, doira, to‘rtburchak va σ = 4 Gauss shovqini; haqiqiy fotosurat emas) AES-128 bilan ECB, CBC va CTR rejimlarida shifrlandi. Kalit va IV faqat tajriba uchun qat’iy tanlangan. Korrelyatsiya 5000 ta tasodifiy juftlikda, NPCR/UACI markaziy pikselning bitta bitini o‘zgartirib hisoblandi; tezlik 16 MB tasodifiy ma’lumotda 7 o‘lchashning eng yaxshisi bilan topildi. Natijalar bitta tasvir va bitta urinishga tegishli, shuning uchun umumlashtirib bo‘lmaydi.

1-jadval. AES-128 bilan shifrlash natijalari

Ko‘rsatkich	Ochiq tasvir	ECB	CBC	CTR
Entropiya, bit	7,518	7,9975	7,9973	7,9974
Korrelyatsiya (gor./vert./diag.)	0,981 / 0,980 / 0,973	0,013 / 0,013 / 0,009	0,005 / 0,000 / 0,020	−0,003 / −0,003 / 0,007
χ^2 (kritik 293,25)	40 219	232,4	249,5	239,1
NPCR, %	—	0,024	49,63	0,0015
UACI, %	—	0,009	16,71	≈ 0
Tezlik, MB/s	—	3498	847	5581

7. Natijalar va muhokama

Uch rejimda ham entropiya 7,997 bitga yaqin, χ^2 qiymatlari 293,25 dan kichik, korrelyatsiya nolga yaqin, ya’ni bu ko‘rsatkichlar rejimlarni ajratmaydi. Biroq tekis sohali, shovqinsiz tasvirda (4096 blokdan 35 tasi turlicha) ECB shifrmatnda ham 35 ta noyob blok qoldirdi, CBC va CTR esa barcha 4096 blokni noyob qildi. Demak, entropiya va korrelyatsiya ECB ning tuzilmaviy zaifligini ko‘rsatmaydi va yagona mezon bo‘la olmaydi.

NPCR va UACI rejim xossasini aks ettiradi: ECB va CTR da bir bitlik o‘zgarish mos ravishda bitta blok yoki bitta bayt bilan cheklanadi, CBC da esa keyingi bloklarga tarqaladi (NPCR 49,63 %). Kalitning bir biti o‘zgarganda CBC da NPCR 99,67 %, UACI 33,49 % chiqdi, bu ideal qiymatlarga yaqin. CBC ketma-ket bajarilgani uchun sekinroq; ECB va CTR orasidagi farq amalga oshirishga bog‘liq bo‘lishi mumkin, mutlaq tezlik esa uskunaga bog‘liq. Hamma rejimlarda murakkablik ma’lumot hajmiga chiziqli. Xaotik sxemalar tajribada sinalmadi, ularning tahlili adabiyotga asoslanadi [5–7]. Taqqoslash 2-jadvalda.

2-jadval. Algoritmlarni taqqoslash

Algoritm	Xavfsizlik	Tezlik	Qo‘llanish
AES-ECB	Bir xil bloklar sizadi [3]	Parallel	Tasvir uchun yaroqsiz
AES-CBC	Diffuziya keyingi bloklarga tarqaladi; IV tasodifiy bo‘lishi shart [3]	Shifrlash ketma-ket, sekinroq	Fayl va arxivlar
AES-CTR	Nonce noyob bo‘lsa xavfsiz; o‘zgarish lokal [3]	Parallel, eng tez	Audio va video oqim
Xaotik sxema	Kalit fazosi va kriptotahlil tekshirilishi kerak [6, 7]	Tez; amalga oshirishga bog‘liq	Tadqiqot yo‘nalishi

Xulosa

1. Kodlash kalitsiz bajariladi va maxfiylikni bermaydi, shifrlash kalitga tayanadi; ma’lumot avval siqiladi, so‘ng shifrlanadi. 2. Tasvirni AES bilan shifrlashda ECB qo‘llanmaydi; CTR (noyob nonce bilan) yoki CBC (tasodifiy IV bilan) tavsiya etiladi, [3] rejimlari yaxlitlikni ta’minlamagani uchun alohida autentifikatsiya kerak. 3. Baholashda entropiya va korrelyatsiya bilan cheklanmay, χ^2, NPCR/UACI, kalit sezgirligi, kalit fazosi va hujumlarga chidamlilik tekshiriladi. 4. Xaotik sxemalar istiqbolli yo‘nalish, lekin standart algoritmlar o‘rnini bosa olmaydi; keyingi ishda real tasvirlar to‘plami va xaotik sxemani amalga oshirib solishtirish ko‘zda tutilgan.

Foydalanilgan adabiyotlar

1. Shannon C. E. Communication theory of secrecy systems // Bell System Technical Journal. 1949. Vol. 28, No. 4. P. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x

2. NIST. Advanced Encryption Standard (AES): FIPS 197, updated May 9, 2023. DOI: 10.6028/NIST.FIPS.197-upd1

3. Dworkin M. Recommendation for Block Cipher Modes of Operation: Methods and Techniques: NIST SP 800-38A. 2001. DOI: 10.6028/NIST.SP.800-38A

4. Daemen J., Rijmen V. The Design of Rijndael. Berlin: Springer, 2002. DOI: 10.1007/978-3-662-04722-4

5. Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps // Int. J. Bifurcation and Chaos. 1998. Vol. 8, No. 6. P. 1259–1284. DOI: 10.1142/S021812749800098X

6. Chen G., Mao Y., Chui C. K. A symmetric image encryption scheme based on 3D chaotic cat maps // Chaos, Solitons & Fractals. 2004. Vol. 21, No. 3. P. 749–761. DOI: 10.1016/j.chaos.2003.12.022

7. Kocarev L. Chaos-based cryptography: a brief overview // IEEE Circuits and Systems Magazine. 2001. Vol. 1, No. 3. P. 6–21. DOI: 10.1109/7384.963463

8. Rukhin A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: NIST SP 800-22 Rev. 1a. April 2010.

9. Wu Y., Noonan J. P., Agaian S. NPCR and UACI randomness tests for image encryption // Cyber Journals: JSAT. April 2011. P. 31–38.

