IKKI O'LCHAMLI XAOTIK AKSLANTIRISHLAR ASOSIDA TASVIRLARNI XAVFSIZ SIQISH VA SHIFRLASH TEXNOLOGIYALARI

Maxmudjonov Orifjon Maxmudjon o'g'li
Urganch davlat univesiteti magistranti
orifjonmaxmudjonov72@gmail.com

ANNOTATSIYA

Ushbu maqolada ikki o'lchamli (2D) xaotik akslantirishlarning nazariy asoslari va ularning raqamli tasvirlarni siqish hamda shifrlashdagi istiqbollari tahlil qilinadi. Tadqiqotda 2D xaotik tizimlarning (masalan, 2D-ELSCM, 2D-SQSM) 1D tizimlarga nisbatan ustunligi, xususan, kengroq kalitlar fazosi va yuqori Lyapunov eksponenti (8.3175 gacha) isbotlanadi.

Kalit so'zlar: *2D xaotik akslantirishlar, Lyapunov eksponenti, tasvirni siqish, kvant xavfsizligi, entropiya, DWT*

АННОТАЦИЯ

Данная статья анализирует теоретические основы двумерных (2D) хаотических отображений и их применение в сжатии и шифровании изображений. Показано, что 2D хаотические системы (например, 2D-ELSCM, 2D-SQSM) превосходят одномерные системы благодаря более широкому пространству ключей и более высоким показателям экспоненты Ляпунова (до 8.3175).

Ключевые слова: *двумерные хаотические отображения, экспонента Ляпунова, сжатие изображений, квантовая безопасность, энтропия, DWT.*

ABSTRACT

This paper analyses the theoretical foundations of two-dimensional (2D) chaotic mappings and their applications in image compression and encryption. It demonstrates that 2D chaotic systems (e.g., 2D-ELSCM, 2D-SQSM) outperform 1D systems due to a larger key space and higher Lyapunov exponents (up to 8.3175).

Keywords: *2D chaotic mappings, Lyapunov exponent, image compression, quantum security, entropy, DWT.*

KIRISH

Hozirgi raqamli texnologiyalar shiddat bilan rivojlangan davrda tasvirlar axborot almashinuvining asosiy vositasiga aylandi, biroq ularni ochiq tarmoqlar orqali uzatish va saqlash xavfsizlik bilan bog'liq jiddiy maxfiylik muammolarini keltirib chiqarmoqda. Raqamli tasvirlarning o'ziga xos xususiyatlari, ya'ni ma'lumotlar hajmining o'ta kattaligi va qo'shni piksellar orasidagi kuchli korrelyatsiya bog'liqligi

sababli, matnlar uchun mo‘ljallangan an’anaviy shifrlash algoritmlari (masalan, AES va DES) ularga ishlov berishda past samaradorlik va yetarsiz xavfsizlik kabi kamchiliklarni namoyon etmoqda. Shu sababli, xaotik tizimlarning boshlang‘ich sharoitlarga o‘ta sezgirligi, ergodikligi va bashorat qilib bo‘lmasligi tasvir ma’lumotlarini ham himoyalash, ham ularning hajmini samarali siqishda fundamental matematik asos bo‘lib xizmat qilmoqda.

METODOLOGIYA

Bir o‘lchamli (1D) xaotik akslantirishlar amalga oshirishda sodda bo‘lsa-da, ularning xaotik diapazoni cheklanganligi va traektoriya tanaffuslari zamonaviy kriptografik hujumlarga qarshi yetarli bardoshlilikni ta’minlay olmaydi. Ushbu muammolarni bartaraf etish maqsadida ishlab chiqilgan 2D-SQSM, 2D-LASM va 2D-ELSCM kabi ikki o‘lchamli tizimlar murakkab chiziqli bo‘lmagan dinamikasi, yuqori Lyapunov eksponentlari (8.3175 gacha) va ulkan kalitlar fazosi (masalan, 2^732 gacha) bilan ajralib turadi. Hozirgi kunda ushbu tizimlarni tasvirlarni siqish (DWT, DCT yoki Siqilgan his qilish, Compressed Sensing) va shifrlash jarayonlarini birlashtirilgan tizimga (Joint Compression-Encryption)[1] integratsiya qilish sohaning eng istiqbolli yo‘nalishlaridan biri hisoblanadi. Tasvirlarni himoyalash va siqish jarayonlarini yagona arxitekturada birlashtirishda xaotik tizimlardan foydalanish, avvalo, piksel qiymatlari va ularning fazoviy joylashuvini nazorat qilib bo‘lmaydigan darajada murakkab tarzda o‘zgartirish imkonini beradi. An’anaviy yondashuvlarda tasvir avval siqilib, so‘ngra alohida shifrlansa, qo‘shma siqish-shifrlash modelida bu ikki bosqich o‘zaro bog‘liq holda bajariladi. Bunda tasvirning ortiqcha statistik axboroti kamaytiriladi, shu bilan birga qolgan muhim koeffitsiyentlar xaotik ketma-ketliklar yordamida diffuziya va permutatsiya qilinadi. Masalan, DWT asosida tasvir past va yuqori chastotali komponentlarga ajratilganda, inson ko‘zi uchun muhim bo‘lgan past chastotali soha saqlanib, yuqori chastotali qismlardagi ortiqcha ma’lumotlar kamaytiriladi. Shundan so‘ng 2D-LASM yoki 2D-SQSM kabi xaotik xaritalar yordamida koeffitsiyentlarning tartibi almashtiriladi va ularning amplituda qiymatlari o‘zgartiriladi[2]. Bu jarayon nafaqat tasvir hajmini qisqartiradi, balki shifrlangan tasvirda asl tasvirga xos bo‘lgan gistogramma, korrelyatsiya va energiya taqsimoti belgilarini ham yo‘qotadi. DCT asosidagi yondashuvda esa tasvir bloklarga bo‘linib, har bir blok chastota koeffitsiyentlariga aylantiriladi. Xaotik tizim bu bloklarning tanlanishi, kvantlash darajasi, koeffitsiyentlarning joylashuvi va shifrlash ketma-ketligini boshqaradi. Natijada kalitga bog‘liq adaptiv transformatsiya hosil bo‘ladi. Siqilgan his qilish usuli bilan integratsiyalashgan modelda esa tasvir siyrak ko‘rinishga o‘tkaziladi va tasodifiy o‘lchov matritsasi orqali kam sonli o‘lchovlar olinadi. Agar ushbu o‘lchov matritsasi

xaotik ketma-ketlik asosida shakllantirilsa, u bir vaqtning o‘zida ham siqish, ham maxfiy shifrlash vazifasini bajaradi. Bunday holatda tasvirni tiklash uchun nafaqat o‘lchovlar, balki xaotik tizim parametrlari, boshlang‘ich qiymatlari va matritsa generatsiyasi tartibi ham zarur bo‘ladi. Shu bois qo‘shma siqish-shifrlash sxemalari hisoblash xarajatlarini kamaytirish, uzatish tezligini oshirish va xavfsizlikni kuchaytirish jihatidan alohida shifrlash hamda alohida siqish algoritmlariga nisbatan ustunlikka ega bo‘ladi.

TAHLIL

Ikki o‘lchamli xaotik xaritalarning tasvir kriptografiyasidagi afzalligi ularning dinamik murakkabligi, parametrlar sezgirligi va ko‘p o‘lchamli kalitlar fazosi bilan belgilanadi. 1D xaotik xaritalarda ayrim parametrlar oralig‘idagina xaotik xatti-harakat kuzatilgani sababli, ularning ketma-ketliklari ba’zi hollarda davriy yoki taxmin qilinadigan xususiyatga ega bo‘lib qoladi. 2D-SQSM, 2D-LASM va 2D-ELSCM kabi tizimlarda esa ikkita o‘zgaruvchi o‘zaro chiziqli bo‘lmagan bog‘lanish orqali rivojlanadi. Bu esa hosil bo‘ladigan xaotik ketma-ketliklarning murakkabligini oshirib, piksellar orasidagi tabiiy korrelyatsiyani keskin pasaytiradi. Tasvir shifrlashda odatda ikki asosiy bosqich qo‘llanadi: permutatsiya va diffuziya. Permutatsiyada piksel yoki transformatsiya koeffitsiyentlarining joylashuvi o‘zgartiriladi, diffuziyada esa ularning qiymatlari kalitga bog‘liq tarzda yangilanadi[3]. 2D xaotik xaritalar ushbu ikki bosqichni kuchaytiradi, chunki ular yordamida har bir piksel pozitsiyasi va qiymatini mustaqil, ammo kalitga bog‘liq tarzda boshqarish mumkin. Masalan, birinchi xaotik ketma-ketlik indekslarni aralashtirish uchun, ikkinchi ketma-ketlik esa XOR, modul qo‘shish yoki bit darajasidagi aylantirish amallarini bajarish uchun ishlatiladi. Bundan tashqari, shifrlash algoritmiga ochiq tasvirga bog‘liq xesh qiymatini kiritish orqali bir xil kalit ishlatilgan taqdirda ham har xil tasvirlar uchun turlicha shifrlash natijalari olinadi. Bu tanlangan ochiq matn hujumlariga qarshi bardoshlilikni oshiradi. Xavfsizlik tahlilida kalitlar fazosi, kalit sezgirligi, gistogramma tekisligi, qo‘shni piksellar korrelyatsiyasi, axborot entropiyasi, NPCR va UACI ko‘rsatkichlari muhim hisoblanadi. Yaxshi loyihalangan xaotik shifrlash tizimida shifrlangan tasvir gistogrammasi deyarli bir tekis taqsimlanadi, gorizontal, vertikal va diagonal yo‘nalishlardagi korrelyatsiya nolga yaqinlashadi, entropiya esa ideal 8 qiymatiga yaqin bo‘ladi. NPCR va UACI ko‘rsatkichlarining yuqori bo‘lishi tasvirdagi bitta piksel o‘zgarishi butun shifrlangan tasvirga sezilarli ta’sir qilishini ko‘rsatadi. Bu diffuziya mexanizmining kuchli ekanini bildiradi va algoritmni differensial hujumlarga nisbatan ishonchli qiladi.

MUHOKAMA

Amaliy jihatdan bunday modellar tibbiy tasvirlar, masofaviy zondlash ma’lumotlari, biometrik identifikatsiya tizimlari, harbiy kuzatuv tasvirlari va bulutli saqlash xizmatlarida alohida ahamiyat kasb etadi. Masalan, tibbiy diagnostika tasvirlarida bemorning shaxsiy ma’lumotlari, kasallik belgilari va klinik xulosalar bevosita tasvir tarkibida aks etishi mumkin. Shu sababli MRT, KT yoki rentgen tasvirlarini ochiq tarmoq orqali uzatishda ularning maxfiyligini saqlash bilan birga, fayl hajmini kamaytirish ham zarur[4]. Qo‘shma siqish-shifrlash sxemasi bu ikki talabni bir vaqtning o‘zida bajaradi: uzatish kanali yuklamasi kamayadi va begona shaxs tasvir mazmunini tiklay olmaydi. Masofaviy zondlashda yuqori aniqlikdagi sun’iy yo‘ldosh tasvirlari juda katta hajmga ega bo‘lgani uchun ularni real vaqtga yaqin rejimda uzatish murakkabdir. Xaotik siqish-shifrlash yondashuvi bunday ma’lumotlarni ixcham, lekin himoyalangan shaklda uzatish imkonini beradi. Biometrik tizimlarda esa barmoq izi, yuz tasviri, ko‘z qorachig‘i yoki kaft tomir izi kabi ma’lumotlarning o‘g‘irlanishi qayta tiklab bo‘lmaydigan xavf tug‘diradi. Parolni almashtirish mumkin, ammo biometrik belgini almashtirib bo‘lmaydi. Shuning uchun biometrik tasvirlarni saqlashda oddiy shifrlashdan tashqari, kalitga bog‘liq transformatsiya, xaotik aralashtirish va siyrak o‘lchovlar orqali maxfiylik darajasini oshirish dolzarb hisoblanadi. Kelgusida ushbu yo‘nalishda yengil vaznli, apparatga mos, real vaqt rejimida ishlovchi va sun’iy intellekt bilan integratsiyalashgan algoritmlarni ishlab chiqish muhim vazifa bo‘lib qoladi. Ayniqsa, IoT qurilmalari, dronlar, aqlli kameralar va mobil tibbiy diagnostika tizimlarida hisoblash resurslari cheklanganligi sababli, algoritm nafaqat xavfsiz, balki energiya tejamkor va tezkor bo‘lishi ham kerak. 2D xaotik tizimlar asosidagi qo‘shma siqish-shifrlash modellari aynan shu talablarni qondirishga yaqin turadi, chunki ular oddiy matematik rekurrent formulalar orqali murakkab va tasodifiyga o‘xshash ketma-ketliklar hosil qiladi. Shu bilan birga, ularning kriptografik mustahkamligi faqat kalitlar fazosi kattaligi bilan emas, balki algoritmning umumiy konstruksiyasi, kalit generatsiyasi, diffuziya chuqurligi, transformatsiya bosqichlari va hujumlarga qarshi tahlil natijalari bilan ham baholanishi lozim.

Tizim metodologiyasi doirasida dastlab kirish tasviri Diskret Vavelet Almashtirish (2D-DWT) yoki DCT yordamida vaqt sohasidan chastota sohasiga o‘tkaziladi. Bunda tasvirning asosiy energiyasi past chastotali (LL) koeffitsiyentlarda jamlanadi, yuqori chastotali qismlar esa piksellardagi ikkinchi darajali detallarni aks ettiradi. Hajmni kichraytirish uchun faqat LL koeffitsiyentlari saqlab qolinadi va tasvir hajmini uning asl hajmidan bir necha barobar kichraytirish uchun Siqilgan his qilish (Compressed Sensing, CS) algoritmi qo‘llaniladi. Bunda 2D xaotik akslantirish

yordamida shakllantirilgan o‘lchov matritsalari tasvir sifatini (SSIM > 98%) saqlab qolgan holda ma’lumotlar uzatish kanalidagi yuklamani sezilarli darajada kamaytiradi[5].

Siqilgan ma’lumotlarning xavfsizligini ta’minlash uchun dinamik diffuziya bosqichida 2D xaotik tizimdan olingan pseudo-tasodifiy ketma-ketliklar normalizatsiya qilinib, siqilgan tasvir piksellari bilan bitma-bit XOR operatsiyasi orqali birlashtiriladi. Ba’zi ilg‘or metodlarda diffuziya jarayoni DNA kodlash va Zigzag almashtirishlari bilan boyitiladi, bu esa tizimning statistik hujumlarga va kvant tahlillariga qarshi bardoshliligini oshiradi. Tadqiqot natijalari shuni ko‘rsatadiki, meta-evristik optimallashtirish algoritmlari (GWO, COOT) bilan sintez qilingan tizim tasvirlarni qayta tiklash sifatini (SSIM > 98.8%) saqlab qolgan holda mutlaq chidamlilikni kafolatlaydi.

XULOSA

Xulosa qilib aytganda, ikki o‘lchamli xaotik akslantirishlar ochiq tarmoqlar orqali vizual ma’lumotlarni uzatishda ideal entropiya ko‘rsatkichlariga (7.999 ga yaqin) erishish imkonini beradi. 2D xaotik tizimlar taqdim etadigan ulkan kalitlar fazosi statistik, differensial va "brute-force" hujumlariga qarshi mutlaq xavfsizlikni ta'minlaydi. Kelajak istiqbollari ushbu jarayonlarni real vaqt rejimida ishlovchi apparat qurilmalariga (VLSI/FPGA) joriy etish hamda ularni kvant hujumlariga bardoshli metodlar bilan boyitishga qaratilgan. 2D xaotik akslantirishlar zamonaviy kiberxavfsizlik va ma’lumotlarni tejash texnologiyalarining fundamental asosi bo‘lib, vizual ma’lumotlarni himoyalashda eng ishonchli yechimdir.

FOYDALANILGAN ADABIYOTLAR

1. Liu, F., & Wu, S. (2025). A robust color image encryption algorithm based on 2D-SQSM hyperchaotic map and cyclic shift scrambling. PLOS One, 20(10), e0333640
2. Zhang, H., Liu, X., Chen, K., Te, R., & Yan, F. (2025). Robust Image Encryption with 2D Hyperchaotic Map and Dynamic DNA-Zigzag Encoding. Entropy, 27(6), 606
3. S. G. Matlatipov, J. Rajabov, E. Kuriyozov, and M. Aripov, “UzABSA: Aspect-Based Sentiment Analysis for the Uzbek Language,” in Proc. 3rd Annu. Meeting Special Interest Group Under-resourced Lang. @ LREC-COLING 2024, 2024, pp. 394–403.
4. B. Kutlimuratova, E. Kuriyozov, and M. Tillaeva, “Teaching English as a foreign language for primary school children: Literature review,” Foreign Language Teaching and Applied Linguistics, pp. 161–171, 2022.

5. J. Mattiev, U. Salaev, and B. Kavšek, “Advanced Word Game Design Based on Statistics: A Cross-Linguistic Study with Extended Experiments,” Big Data Cognit. Comput., vol. 9, no. 4, p. 103, 2025.
6. Hua, Z., & Zhou, Y. (2016). Image encryption using 2D Logistic-adjusted-Sine map. Information Sciences, 339, 237-253.