MA’LUMOTLARNI YO‘QOTISHLARSIZ XAVFSIZ SIQISH UCHUN 3D XAOTIK AKSLANTIRISHLAR

Yo‘ldashboyev Shahzod Rashid o‘g‘li
Urganch davlat universiteti magistranti,
Maxmudjonov Orifjon Maxmudjon o‘g‘li
Urganch davlat universiteti magistranti,

ANNOTATSIYA

Ushbu maqolada WAM 3D xaotik akslantirishi hamda Huffman va LZW algoritmlari asosida matnli ma’lumotlarni xavfsiz siqish usuli tadqiq etiladi. Tizim 10^165 gacha bo‘lgan keng kalitlar fazosi orqali kiberhujumlardan ishonchli himoyani ta’minlaydi. Tajribalar hosil qilingan ketma-ketliklarning barcha NIST testlaridan o‘tganini va entropiya ko‘rsatkichi 7.9993 ga tengligini ko‘rsatdi.

Kalit so‘zlar: *3 o‘lchamli xaotik akslantirishlar, WAM 3D diskret xaritasi, shifrlash, xaos nazariyasi, Huffman kodlash, LZW algoritmi, NIST testlari.*

3D ХАОТИЧЕСКИЕ ОТОБРАЖЕНИЯ ДЛЯ БЕЗОПАСНОГО СЖАТИЯ ДАННЫХ БЕЗ ПОТЕРЬ

Юлдашбоев Шахзод Рашидович
магистрант Ургенчского государственного университета
Махмуджонов Орифжон Махмуджонович
магистрант Ургенчского государственного университета

АННОТАЦИЯ

В статье исследуется интегрированный метод безопасного сжатия текстовых данных с использованием хаотической карты WAM 3D и алгоритмов Хаффмана и LZW. Система обеспечивает защиту от атак «грубой силы» благодаря пространству ключей 10^165. Результаты подтверждают успешное прохождение тестов NIST и достижение информационной энтропии уровня 7.9993.

Ключевые слова: *Трехмерные хаотические отображения, WAM 3D, шифрование, теория хаоса, кодирование Хаффмана, алгоритм LZW, тесты NIST.*

3D CHAOTIC MAPS FOR SECURE LOSSLESS DATA COMPRESSION

Shakhzod Yuldashboyev
Master's student at Urgench State University
Orifjon Maxmudjonov
Master's student at Urgench State University

ABSTRACT

This article presents an integrated method for secure, lossless text compression using the WAM 3D discrete chaotic map alongside Huffman and LZW algorithms. The system ensures robust protection against brute-force attacks with a key space of 10^165. Results show that the sequences pass all NIST tests, achieving an ideal information entropy of 7.9993.

Keywords. *3D chaotic mappings, WAM 3D discrete map, encryption, chaos theory, Huffman coding, LZW algorithm, NIST tests.*

KIRISH

Hozirgi raqamli davrda raqamli ma’lumotlar, ayniqsa matnli va multimedia fayllari hajmining geometrik progressiya bilan ortishi aloqa kanallarining o‘tkazish qobiliyati va saqlash resurslariga bo‘lgan ehtiyojni keskin kuchaytirmoqda. An’anaviy shifrlash algoritmlari (masalan, AES va DES) ma’lumotlarni himoya qilishda samarali bo‘lsa-da, ular yuqori redundantlikka (ortiqchalik) ega bo‘lgan katta hajmli fayllarni qayta ishlashda resurslarni ko‘p iste’mol qiladi va uzatishda kechikishlarni yuzaga keltiradi. Shu sababli, cheklangan tarmoq kengligi sharoitida ma’lumotlarni bir vaqtning o‘zida ham samarali siqish (compression), ham xavfsiz shifrlash (encryption) imkonini beruvchi integrallashgan yondashuvlarni ishlab chiqish zamonaviy axborot texnologiyalarining eng dolzarb vazifalaridan biri hisoblanadi.

Ushbu muammolarni hal qilishda uch o‘lchamli (3D) xaotik akslantirishlar nazariyasi o‘zining boshlang‘ich qiymatlarga o‘ta sezgirligi, deterministik tasodifiyligi va murakkab dinamik trayektoriyalari bilan yuqori samaradorlik ko‘rsatmoqda. Mazkur tadqiqotda 3D xaotik akslantirishlar yordamida matnli fayllarning hajmini yo‘qotishlarsiz (lossless) kichraytirish va ularning konfidensialligini ta’minlash algoritmlari tahlil qilinadi, bu esa ma’lumotlarni xavfsiz va resurs-tejamkor usulda uzatish uchun ilmiy asos bo‘lib xizmat qiladi.

MAVZUGA OID ADABIYOTLARNING TAHLILI

Xaotik tizimlarning axborotni himoya qilish va siqishdagi o‘rni so‘nggi yillarda ko‘plab tadqiqotlar markazida bo‘lib kelmoqda. Dastlabki ilmiy izlanishlarda asosan Logistic va Tent kabi bir o‘lchamli (1D) va ikki o‘lchamli (2D) xaotik akslantirishlar qo‘llanilgan. Biroq, 1D tizimlar o‘zining sodda tuzilishi va kalitlar fazosining cheklanganligi sababli kiberhujumlarga, xususan, "brute-force" (to‘liq saralash) hujumlariga nisbatan zaif ekanligi isbotlangan. Shu sababli, zamonaviy tadqiqotchilar murakkab dinamik trayektoriyaga va yuqori entropiyaga ega bo‘lgan uch o‘lchamli (3D) va undan yuqori tartibli giperxaotik tizimlarga e’tibor qaratmoqdalar[1].

Ilmiy adabiyotlarda ma’lumotlarni siqish va shifrlashni integratsiyalash bo‘yicha bir necha asosiy yo‘nalishlar mavjud. Masalan, Liu va uning hamkasblari (2024) o‘z ishlarida giperxaotik tizimni Compressed Sensing (CS) texnologiyasi bilan birlashtirib, tasvirlarni bir vaqtning o‘zida ham siqish, ham himoya qilish metodikasini taklif etganlar. Shuningdek, Haddad (2025) va Gong (2018) kabi tadqiqotchilar Zigzag skanerlash texnikasi va 3D fraktal xaotik tizimlardan foydalanib, piksellar o‘rnini samarali chalkashtirish (permutation) orqali ma’lumotlar redundantligini kamaytirishga erishganlar.

Shu bilan birga, ko‘plab tadqiqotlarda CS texnologiyasining asosiy afzalligi shundaki, u tasvirni to‘liq tiklash uchun barcha piksellarni emas, balki uning siyrak ifodasini ifodalovchi kam sonli o‘lchov koeffitsiyentlarini saqlashga imkon beradi. Agar ushbu o‘lchov jarayoni oddiy tasodifiy matritsa orqali emas, balki xaotik ketma-ketliklar asosida shakllantirilsa, siqish jarayonining o‘zi kriptografik himoya vazifasini ham bajaradi. Bunda o‘lchov matritsasining elementlari xaotik tizim parametrlariga, boshlang‘ich shartlarga va iteratsiya soniga bog‘liq bo‘ladi. Natijada ruxsatsiz foydalanuvchi tasvirning asl holatini tiklash uchun nafaqat siqilgan ma’lumotlarga, balki xaotik tizimning aniq matematik modeli, parametrlar to‘plami va boshlang‘ich qiymatlariga ham ega bo‘lishi kerak. Bu holat siqilgan his qilish asosidagi qo‘shma shifrlash tizimlarini oddiy transformatsion siqish usullariga nisbatan xavfsizroq qiladi. Ayniqsa, DWT yoki DCT kabi klassik siqish usullari bilan CS texnologiyasini birlashtirish orqali tasvirning muhim chastotaviy komponentlari ajratib olinadi, ortiqcha ma’lumotlar kamaytiriladi va qolgan koeffitsiyentlar xaotik permutatsiya hamda diffuziya bosqichlari orqali shifrlanadi. Bunday yondashuvda siqish koeffitsiyenti, tiklash sifati, hisoblash murakkabligi va xavfsizlik darajasi o‘rtasidagi muvozanat asosiy mezon sifatida qaraladi[2].

Adabiyotlarda uchraydigan yana bir muhim yo‘nalish — bu tasvirni bloklarga bo‘lish, har bir blokning statistik xususiyatlarini aniqlash va xaotik tizimlar yordamida adaptiv shifrlashni amalga oshirishdir. An’anaviy algoritmlarda barcha

bloklarga bir xil ishlov berilishi natijasida ba’zi hollarda shifrlangan tasvirda statistik izlar saqlanib qolishi mumkin. Adaptiv yondashuvda esa bloklarning entropiyasi, energiyasi, yorqinlik darajasi yoki tekstura murakkabligi hisobga olinadi. Masalan, yuqori detalli bloklar kuchli diffuziya bilan, silliq fon qismlari esa kuchli permutatsiya bilan qayta ishlanishi mumkin. Bu usul tasvirning lokal xususiyatlariga moslashgan holda ishlagani uchun xavfsizlikni oshiradi va ortiqcha hisoblash xarajatlarini kamaytiradi. 3D va giperxaotik tizimlar bunday adaptiv sxemalar uchun ayniqsa qulay hisoblanadi, chunki ular bir vaqtning o‘zida bir nechta mustaqilga yaqin xaotik ketma-ketliklarni hosil qila oladi. Ushbu ketma-ketliklarning biri bloklar tartibini aralashtirishga, ikkinchisi piksel qiymatlarini o‘zgartirishga, uchinchisi esa kalitga bog‘liq transformatsiya parametrlarini tanlashga xizmat qilishi mumkin. Natijada shifrlash jarayoni ko‘p bosqichli va murakkab xarakterga ega bo‘ladi[3].

Giperxaotik tizimlarning ustunligi ularning kamida ikki yoki undan ortiq musbat Lyapunov eksponentlariga ega bo‘lishi bilan izohlanadi. Bu esa tizim traektoriyasining oddiy xaotik tizimlarga qaraganda tezroq ajralishini va bashorat qilish imkoniyatining yanada pasayishini anglatadi. Tasvir kriptografiyasida bunday xususiyat juda muhim, chunki shifrlash algoritmi kalitdagi juda kichik o‘zgarishga ham butunlay boshqa natija berishi kerak. Agar boshlang‘ich qiymatning 10^-14 darajadagi farqi shifrlangan tasvirni tubdan o‘zgartirsa, bu kalit sezgirligi yuqori ekanini ko‘rsatadi. Shu sababli so‘nggi tadqiqotlarda Lorenz, Chen, Lü, Rossler va ularning modifikatsiyalangan giperxaotik variantlari keng qo‘llanmoqda. Bundan tashqari, sinus, cosine, exponential, logistic va tent komponentlarini birlashtirgan yangi aralash xaotik xaritalar ham taklif qilinmoqda. Bunday kombinatsion modellar klassik xaritalardagi cheklangan xaotik oraliq, past murakkablik va davriylik kabi kamchiliklarni kamaytirishga xizmat qiladi.

Tasvirlarni shifrlashda xavfsizlik darajasini baholash uchun faqat algoritmning nazariy murakkabligini ko‘rsatish yetarli emas. Amaliy tahlilda kalitlar fazosi, kalit sezgirligi, gistogramma tahlili, korrelyatsiya koeffitsiyenti, axborot entropiyasi, NPCR, UACI, shovqinga chidamlilik va kesilgan tasvirni tiklash imkoniyati kabi mezonlar qo‘llanadi. Shifrlangan tasvirning gistogrammasi imkon qadar tekis taqsimlangan bo‘lishi kerak, chunki tekis taqsimot tajovuzkorning piksel chastotalari asosida asl tasvir haqida xulosa chiqarishini qiyinlashtiradi. Korrelyatsiya tahlilida esa asl tasvirda qo‘shni piksellar orasida kuchli bog‘liqlik mavjud bo‘lsa, shifrlangan tasvirda bu bog‘liqlik nolga yaqinlashishi lozim. Axborot entropiyasining 8 ga yaqin bo‘lishi 8 bitli tasvirlarda piksel qiymatlari tasodifiyga yaqin taqsimlanganini bildiradi. NPCR ko‘rsatkichi tasvirdagi bitta piksel o‘zgarishi shifrlangan natijaning qancha foiziga ta’sir qilishini ko‘rsatsa, UACI o‘rtacha intensivlik o‘zgarishini

ifodalaydi. Ushbu ko‘rsatkichlarning yuqori bo‘lishi algoritmning differensial hujumlarga bardoshli ekanini ko‘rsatadi[4].

Siqish va shifrlashni birlashtirgan tizimlarda yana bir muhim masala — tiklangan tasvir sifati va xavfsizlik o‘rtasidagi muvozanatdir. Kuchli siqish tasvir hajmini sezilarli kamaytiradi, biroq tiklash bosqichida sifat yo‘qotilishiga olib kelishi mumkin. Aksincha, past siqish darajasi yuqori sifatni saqlaydi, ammo uzatish va saqlash xarajatlarini kamaytirish imkonini cheklaydi. Shuning uchun adabiyotlarda PSNR, SSIM, MSE va CR kabi ko‘rsatkichlar keng qo‘llanadi. PSNR qiymatining yuqori bo‘lishi tiklangan tasvirning asl tasvirga yaqinligini bildiradi, SSIM esa strukturaviy o‘xshashlikni baholaydi. CR siqish darajasini ifodalaydi. Zamonaviy modellarda ushbu mezonlar xavfsizlik indikatorlari bilan birgalikda tahlil qilinadi. Ya’ni algoritm faqat tez yoki faqat xavfsiz bo‘lishi emas, balki real amaliy muhitda sifat, tezlik, xotira sarfi va himoya darajasi bo‘yicha optimal natija berishi kerak.

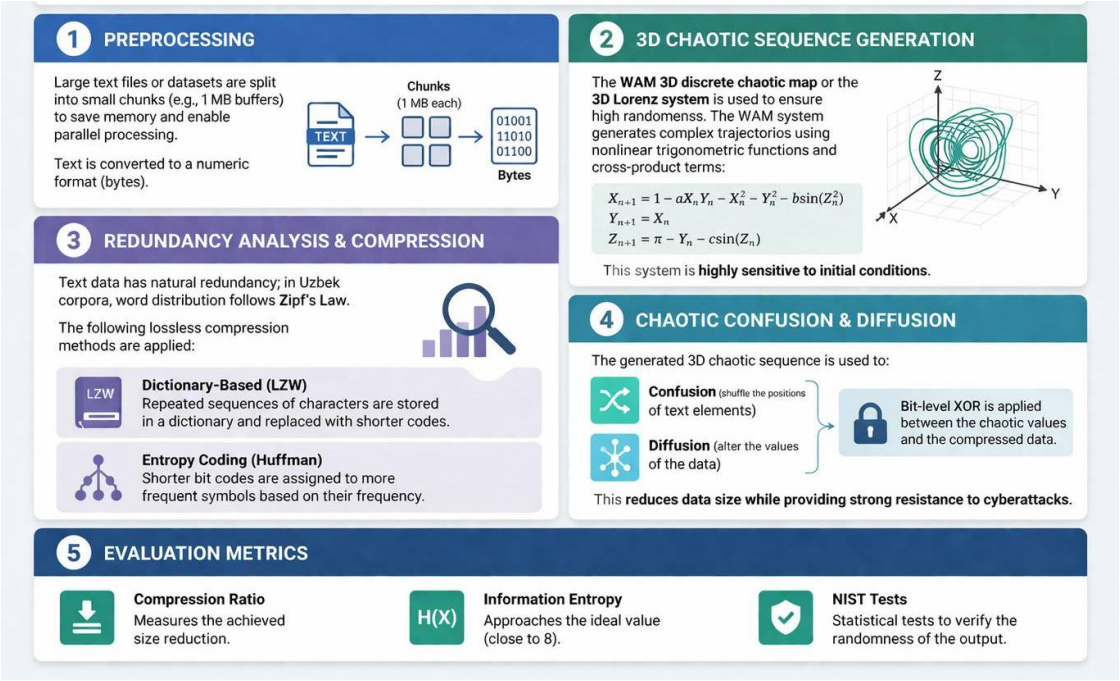
Bundan tashqari, so‘nggi yillarda sun’iy intellekt va chuqur o‘rganish texnologiyalarini xaotik shifrlash tizimlari bilan uyg‘unlashtirishga qaratilgan tadqiqotlar ham ko‘paymoqda. Neyron tarmoqlar yordamida tasvirning muhim sohalarini aniqlash, siqish koeffitsiyentlarini adaptiv tanlash yoki xaotik tizim parametrlarini optimallashtirish mumkin. Masalan, tibbiy tasvirlarda diagnostik ahamiyatga ega bo‘lgan sohalar kamroq yo‘qotish bilan saqlanib, fon yoki kam ahamiyatli qismlar kuchliroq siqilishi mumkin. Masofaviy zondlash tasvirlarida esa obyektlar chegarasi, yo‘l tarmoqlari, binolar yoki tabiiy resurslarga oid muhim hududlar alohida himoya qilinadi. Bu yondashuv tasvirni bir xil darajada qayta ishlash o‘rniga, uning semantik mazmuniga mos kriptografik va kompression ishlov berishga imkon beradi.

Umuman olganda, mavjud ilmiy adabiyotlar tahlili shuni ko‘rsatadiki, xaotik tizimlar asosidagi siqish-shifrlash algoritmlari tasvir xavfsizligini ta’minlashda istiqbolli yo‘nalishlardan biri hisoblanadi. 1D xaotik akslantirishlar soddaligi sababli dastlabki bosqichda muhim rol o‘ynagan bo‘lsa-da, zamonaviy xavfsizlik talablariga javob berish uchun 2D, 3D va giperxaotik tizimlardan foydalanish zarurati ortib bormoqda. CS, DWT, DCT, zigzag skanerlash, fraktal xaos, adaptiv blokli ishlov berish va xeshga asoslangan kalit generatsiyasi kabi usullarni birlashtirish orqali yuqori xavfsizlikka, samarali siqishga va sifatli tiklash natijalariga erishish mumkin. Shu bilan birga, ushbu sohada hali hal qilinishi lozim bo‘lgan muammolar ham mavjud. Jumladan, algoritmlarning real vaqt rejimida ishlash tezligi, apparat qurilmalarga mosligi, energiya sarfi, kalit almashinuvi xavfsizligi va standart kriptografik tahlillardan o‘tkazilishi dolzarb vazifalar qatoriga kiradi. Kelgusida xaotik tizimlar, siqilgan his qilish va sun’iy intellektni integratsiyalashgan holda

ishlab chiqiladigan modellar tibbiyot, biometrika, harbiy aloqa, IoT qurilmalari va bulutli tasvir saqlash tizimlari uchun yanada ishonchli va samarali yechimlar yaratishga xizmat qiladi[5].

TADQIQOT METODOLOGIYASI.

Tadqiqot metodologiyasi uch o‘lchamli xaotik akslantirishlar va matnli ma’lumotlarni yo‘qotishlarsiz siqish (lossless compression) algoritmlarini integratsiyalashga asoslangan. Jarayon quyidagi ketma-ketlikdagi bosqichlardan iborat (1-rasm):



1-Rasm. uch o‘lchamli xaotik akslantirishlar va matnli ma’lumotlarni yo‘qotishlarsiz siqish (lossless compression) jarayoni bosqichlari.

1. Ma’lumotlarga dastlabki ishlov berish (Preprocessing): Ushbu bosqichda matndagi simvollar raqamli ko‘rinishga (baytlarga) o‘tkaziladi.

2. 3D xaotik ketma-ketlikni shakllantirish: WAM tizimi nochiziqli trigonometrik funksiyalar va o‘zaro ko‘paytma hadlari (xy,$x2$,$y2$,$z2$) yordamida murakkab trayektoriyalarni hosil qiladi:

$$x_{n+1} = 1 - ax_ny_n - x_{n_2} - y_{n_2} - bsin(z_{n_2})$$

$$y_{n+1} = x_n$$

$$z_{n+1} = \pi - y_n - csin(z_n)$$

Bu tizim boshlang‘ich qiymatlarga o‘ta sezgirligi bilan ajralib turadi.

3. Redundanlikni tahlil qilish va siqish: Matnli ma’lumotlar o‘ziga xos tabiiy redundantlikka (ortiqchalik) ega bo‘lib, o‘zbek tili korpuslarida so‘zlarning taqsimlanishi Zipf qonuniyatiga bo‘ysunadi.

4. Xaotik chalkashtirish va diffuziya: Hosil qilingan 3D xaotik ketma-ketlik matn elementlarining o‘rnini almashtirish (confusion) va ularning qiymatlarini o‘zgartirish (diffusion) uchun ishlatiladi.

5. Natijalarni baholash mezonlari: Algoritmning samaradorligi siqish koeffitsiyenti (Compression Ratio), axborot entropiyasi (ideal qiymat 8 ga yaqinligi) va NIST testlari orqali tekshiriladi.

Ushbu metodologiya matnli fayllarni ham hajmiy jihatdan optimallashtirish, ham yuqori darajadagi konfidensiallikni ta’minlash imkonini beradi.

TAHLIL VA NATIJALAR.

Xaotik tizimning dinamik xususiyatlari. Tizimning xaotik ekanligini tasdiqlash uchun Lyaponov koeffitsiyenti (LE) hisolandi. WAM 3D diskret xaotik xaritasi uchun olingan natijalar kamida bitta musbat LE (LE1 = 0.0193) mavjudligini ko'rsatdi, bu tizimning boshlang'ich qiymatlarga o'ta sezgirligini va aperiodik ekanligini isbotlaydi. Shuningdek, 0-1 testi natijalari (K qiymati 1 ga yaqinligi: Kx = 0.9958) tizimning deterministik xaotik tabiatini yana bir bor tasdiqladi.

NIST tasodifiylik testlari. Hosil qilingan xaotik ketma-ketliklarning kriptografik talablarga javob berishi NIST SP 800-22 test paketi yordamida tekshirildi. Frequency, Runs, FFT va Non-overlapping Template kabi barcha 15 ta testdan muvaffaqiyatli o'tildi (p-value > 0.01), bu ketma-ketliklarning yuqori darajadagi tasodifiylikka ega ekanligini ko'rsatadi.

Siqish samaradorligi (Compression Performance). Matnli fayllarni siqishda lug'atga asoslangan LZW va entropiya asosidagi Huffman kodlash usullari qo'llanilganida, ma'lumotlarning yo'qotishlarsiz (lossless) qayta tiklanishi ta'minlandi.

XULOSA

Uch o‘lchamli (3D) xaotik akslantirishlar nazariyasi matnli ma’lumotlarni xavfsiz shifrlash va samarali siqish uchun mustahkam ilmiy asos bo‘lib xizmat qiladi. WAM 3D va Lorenz tizimlari o‘zining yuqori dinamik murakkabligi hamda boshlang‘ich qiymatlarga sezgirligi bilan an’anaviy usullardan ustundir. Hosil qilingan ketma-ketliklar NIST SP 800-22 testlaridan muvaffaqiyatli o‘tib, kriptografik yaroqliligini tasdiqladi. Tizim 10^{165} gacha bo‘lgan keng kalitlar fazosi hamda yuqori NPCR va UACI ko‘rsatkichlari orqali kiberhujumlardan ishonchli himoyani ta’minlaydi. Huffman va LZW algoritmlarining xaotik tartiblash bilan integratsiyasi ma’lumotlar hajmini sifatini yo‘qotmasdan sezilarli darajada kichraytirishga va aloqa kanallaridagi yuklamani kamaytirishga imkon beradi.

FOYDALANILGAN ADABIYOTLAR

1. Abdul-Kareem, A. A., & Al-Jawher, W. A. M. (2023). WAM 3D Discrete Chaotic Map for Secure Communication Applications. *International Journal of Innovative Computing* , 13(1-2), 45-54.
2. Ali, N. A., Rahma, A. M. S., & Shaker, S. H. (2023). 3D Content Encryption Using Multi-Level Chaotic Maps. *Iraqi Journal of Science* , 64(5), 2521–2532.
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. K. Madatov, S. Matlatipov, and M. Aripov, "Uzbek text's correspondence with the educational potential of pupils: a case study of the School corpus," *arXiv preprint arXiv:2303.00465*, 2023.
5. 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.