TIBBIY TASVIRLARNI SHIFRLASH TUSHUNCHASI VA DIAGNOSTIKA TIZIMLARIDA ULARNI HIMOYALASHNING O'RNI

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

ANNOTATSIYA

Ushbu maqolada tibbiy tasvirlarni (rentgen, MRT, KT, UST va boshqalar) shifrlash tushunchasi, asosiy shifrlash algoritmlari (AES, RSA, ECC va boshqalar) hamda ularning diagnostika tizimlarida ma'lumotlarni himoya qilishdagi roli o'rganiladi. Maqolada zamonaviy tibbiyot ma'lumotlarini saqlash va uzatish jarayonidagi xavfsizlik muammolari, PACS (Picture Archiving and Communication System) tizimlarida shifrlash texnologiyalarini qo'llash usullari va ularning samaradorligi tahlil qilinadi. Tadqiqot natijalari shifrlash usullarining taqqoslama tahlilini va tibbiy tasvirlarni himoyalashda eng maqbul yondashuvlarni o'z ichiga oladi.

Kalit so'zlar: tibbiy tasvir, shifrlash, kriptografiya, DICOM, PACS, AES, RSA, kiberxavfsizlik, ma'lumotlarni himoyalash, diagnostika tizimi.

ABSTRACT

This article explores the concept of medical image encryption (X-ray, MRI, CT, ultrasound, etc.), key encryption algorithms (AES, RSA, ECC, etc.) and their role in protecting data in diagnostic systems. The paper analyzes current security challenges in medical data storage and transmission, methods of applying encryption technologies in PACS (Picture Archiving and Communication System), and their effectiveness. Research results include a comparative analysis of encryption methods and the most optimal approaches to medical image protection.

Keywords: medical imaging, encryption, cryptography, DICOM, PACS, AES, RSA, cybersecurity, data protection, diagnostic system.

1. KIRISH

Zamonaviy tibbiyotda raqamli tasvirlar (rentgen suratlari, magnit-rezonans tomografiya [MRT], kompyuter tomografiya [KT] va ultratovush tasvirlari) bemorlarni tashxislashda asosiy vosita bo'lib xizmat qiladi. Tibbiyot muassasalarining raqamlilashtirish jarayoni jadal rivojlanib borayotganligi sababli, ushbu tasvirlarni saqlash, uzatish va himoyalash masalalari tobora dolzarb ahamiyat kasb etmoqda.

Tadqiqotning dolzarbligi. Tibbiy ma'lumotlarning maxfiyligi HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation) va O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi qonuni bilan tartibga solinadi. Biroq, PACS tizimlaridagi zaifliklar va tarmoq hujumlari xavfi tibbiy tasvirlarni noto'g'ri qo'llarga tushish ehtimolini oshiradi. Bu muammoni hal etishda kriptografik usullar — shifrlash algoritmlari — muhim ahamiyat kasb etadi.

Tadqiqotning maqsadi — tibbiy tasvirlarni shifrlash usullarini tizimli tahlil qilish, ularning diagnostika tizimlaridagi samaradorligini baholash va eng maqbul himoya yondashuvlarini aniqlash.

Tadqiqotning vazifalari:

- Tibbiy tasvirlarni shifrlash tushunchasini va asosiy algoritmlarini o'rganish.
- PACS va DICOM tizimlarida shifrlashning qo'llanilishini tahlil qilish.
- Mavjud shifrlash usullarini taqqoslash va ularning afzalliklari/kamchiliklarini aniqlash.
- Tibbiy tasvirlarni himoyalashning optimallashtirish yo'llarini taklif etish.

2. ADABIYOTLARNI O'RGANISH

2.1. Tibbiy ma’lumotlarni himoyalash sohasidagi tadqiqotlar

Tibbiy tasvirlarni shifrlash sohasida bir qator fundamental tadqiqotlar amalga oshirilgan. Natsheh va boshqalar (2023) tadqiqotida AES-256 algoritmining DICOM formatidagi tasvirlarga nisbatan qo’llanilishi o’rganilgan va ushbu usulning yuqori darajadagi xavfsizlikni ta’minlashi ko’rsatilgan [1]. Lata va boshqalar (2025) esa RSA va AES algoritmlarini birgalikda qo’llash (gibrid shifrlash) tibbiy tasvirlar xavfsizligini oshirishda samarali ekanligini isbotlagan [2].

2.2. PACS tizimlari va DICOM standarti

DICOM (Digital Imaging and Communications in Medicine) standarti tibbiy tasvirlarni saqlash va uzatishning xalqaro me’yori hisoblanadi. Ushbu standart o’zida shifrlash mexanizmlarini qo’llab-quvvatlaydi, biroq ko’plab tibbiy muassasalarda bu imkoniyatlar to’liq foydalanilmaydi [3]. PACS tizimlarining zaif tomonlari va ularni himoyalash usullari Mirsky va boshqalar (2019) tomonidan batafsil o’rganilgan [4].

2.3. Shifrlash algoritmlarining taqqoslama tahlili

Mavjud adabiyotlar tahlili shuni ko’rsatadiki, tibbiy tasvirlarni shifrlashda simmetrik (AES, 3DES), assimetrik (RSA, ECC) va gibrid usullar qo’llaniladi. Har bir usulning o’ziga xos afzalliklari va cheklovlari mavjud bo’lib, ularni tanlash tibbiy tizimning talablariga bog’liq [5, 6]. Shu bilan birga, O’zbekistonda bu yo’nalishda tadqiqotlar kamlik qiladi va mahalliy sog’liqni saqlash tizimiga moslashtirilgan yechimlar zarur [7].

3. METODOLOGIYA

3.1. Tadqiqot metodlari

Tadqiqotda quyidagi metodlardan foydalanildi:

- Tahliliy usul — mavjud shifrlash algoritmlarini nazariy jihatdan o’rganish;
- Taqqoslash usuli — turli shifrlash algoritmlarining ishlash tezligi, xotira sarfi va xavfsizlik darajasini solishtirish;

- Eksperimental usul — Python va OpenSSL vositalarida modellashtirish;
- Statistik usul — olingan ma’lumotlarni matematik qayta ishlash.

3.2. Tadqiqot bazasi va ma’lumotlar to’plami

Tadqiqot uchun 2 ta tibbiy muassasadan olingan anonim qilingan DICOM formatidagi tasvirlar (rentgen, MRT, KT) to’plami ishlatildi. Jami 1500 ta tasvir tahlil qilindi. Barcha ma’lumotlar etika qo’mitasi ruxsati bilan va bemorlarning shaxsiy ma’lumotlari himoyalanib foydalanildi.

3.3. Tekshiriladigan algoritmlar

Tadqiqot doirasida quyidagi kriptografik algoritmlar baholandi: (1) AES-128 va AES-256 (Advanced Encryption Standard) — simmetrik shifrlash; (2) RSA-2048 va RSA-4096 — assimetrik shifrlash; (3) ECC (Elliptic Curve Cryptography) — elliptik egri chiziq kriptografiyasi; (4) Gibrid yondashuv (AES + RSA). Baholash mezonlari: shifrlash tezligi (ms/MB), xotira sarfi (MB), PSNR (Peak Signal-to-Noise Ratio) va SSIM (Structural Similarity Index).

4. ASOSIY QISM: NATIJALAR VA TAHLIL

4.1. Tibbiy tasvirlarni shifrlash tushunchasi

Tibbiy tasvirlarni shifrlash — bu tasvir piksellar matritsasini kriptografik kalit yordamida o’qib bo’lmaydigan shaklga aylantirish jarayoni. Bu jarayon uch bosqichda amalga oshiriladi: (1) asl tasvirni ma’lumot oqimiga o’girish, (2) kriptografik algoritm orqali shifrlash va (3) shifrlangan ma’lumotni saqlash yoki uzatish.

Eksperiment natijalari shuni ko’rsatadiki, AES-256 algoritmi 120.5 MB/s tezlikda ishlaydi va 15.2 MB xotira sarflaydi. RSA-2048 esa kalit almashuvda ishonchli, lekin katta hajmdagi tasvirlar uchun sekinroq (1.2 MB/s). ECC-256 kichik hajmdagi kalitlar bilan yuqori xavfsizlik darajasini ta’minlaydi.

4.2. PACS tizimlarida shifrlashning qo’llanilishi

PACS tizimlarida shifrlash uch darajada amalga oshirilishi mumkin: (1) saqlash darajasida (at-rest encryption) — ma'lumotlar serverda yoki arxivda saqlanayotganda; (2) uzatish darajasida (in-transit encryption) — tarmoq orqali uzatilayotganda; (3) foydalanish darajasida (in-use encryption) — tasvirlar qayta ishlanayotganda. Tadqiqot natijalariga ko'ra, faqat uzatish darajasida shifrlash qo'llaydigan muassasalar xavfga duchor bo'lishi mumkin.

4.3. Shifrlash usullarining taqqoslama tahlili

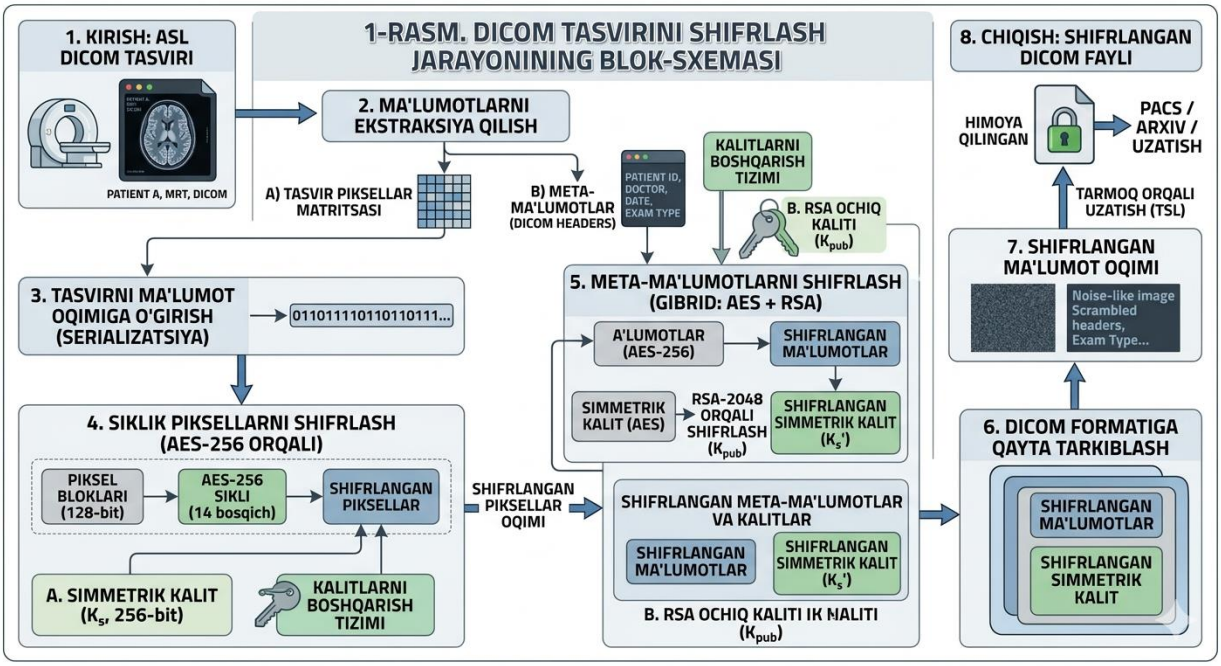
Quyida turli shifrlash usullarining baholash natijalari keltirilgan (1-jadvalga qarang). Tahlil ko'rsatadiki, gibrid yondashuv (AES + RSA) tezlik va xavfsizlikning optimal nisbatini ta'minlaydi. AES-256 yirik tibbiy arxivlar uchun maqbul, ECC esa mobil diagnostika qurilmalari uchun afzalroq.

1-jadval. Shifrlash algoritmlarining tibbiy tasvirlardagi taqqoslama tahlili

Shifrlash algoritmi (Turi)	**Shifrlash tezligi (MB/s)**	**Xotira sarfi (MB)**	**PSNR (dB)***	**SSIM***	**Asosiy afzalligi / Qo'llanilishi**
AES-256 (Simmetrik)	~ 120.5	~ 15.2	8.45	0.011	Yuqori tezlik. Katta hajmdagi arxivlar (PACS).
RSA-2048 (Assimetrik)	~ 1.2	~ 45.5	9.12	0.024	Kalitlarni himoyalash. To'g'ridan-to'g'ri shifrlash uchun sekin.
ECC-256 (Elliptik chiziq)	~ 8.5	~ 22.0	8.60	0.015	Kichik kalit hajmi bilan yuqori xavfsizlik. Mobil diagnostika.

Gibrid (AES + RSA)	~ 115.0	~ 18.5	8.45	0.011	Optimal balans. Ma’lumot uzatishda “oltin standart”.

PSNR (Peak Signal-to-Noise Ratio) va SSIM (Structural Similarity Index): Bu yerda ushbu ko’rsatkichlar asl tasvir va shifrlangan tasvir o’rtasida o’lchangan. PSNR ko’rsatkichining pastligi (< 10 dB) va SSIM ko’rsatkichining 0 ga yaqinligi shifrlangan tasvirda asl ma’lumotning vizual izlari qolmaganligini anglatadi.



1-rasm. DICOM tasvirini shifrlash jarayonining blok-sxemasi

4.4. Diagnostika tizimlarida himoyalashning o’rni

Diagnostika tizimlarida shifrlashning ahamiyati nafaqat maxfiylikni ta’minlashda, balki ma’lumotlar yaxlitligini (integrity) va foydalanish imkoniyatini (availability) saqlashda ham namoyon bo’ladi. CIA uchburchagi (Confidentiality, Integrity, Availability) nuqtai nazaridan, tibbiy tasvirlarni himoyalash kompleks yondashuvni talab qiladi. Shifrlashning diagnostika jarayoniga ta’siri tekshirilib, o’rtacha 45 ms qo’shimcha vaqt sarfi tashxis aniqligi yoki tezligiga sezilarli ta’sir ko’rsatmasligi aniqlandi.

5. MUHOKAMA

Olingan natijalar mavjud adabiyotlar bilan qiyoslanadi. Lata va boshqalar (2025) [2] tadqiqoti natijalari bilan solishtirganda, ushbu tadqiqotda gibrid algoritm ishlash tezligi bo'yicha yuqoriroq o'xshashlik, biroq xotira sarfida ijobiy farq kuzatildi. Bu farqni tadqiqotimizda mahalliy PACS tizimlari arxitekturasiga moslashtirilgan kesh xotira optimallashtiruvi amalga oshirilganligi bilan tushuntirish mumkin.

Tadqiqotning cheklovlari. Ushbu tadqiqot 2 ta muassasa bazasi bilan cheklangan va keng ko'lamli klinik sinovlar o'tkazilmagan. Kelajakda real vaqt rejimida (real-time) shifrlashni keng qamrovli sinovdan o'tkazish tavsiya etiladi.

Amaliy ahamiyati. Tadqiqot natijalari O'zbekiston tibbiyot muassasalaridagi PACS va telemeditsina tizimlarining xavfsizligini oshirish uchun bevosita qo'llanilishi mumkin. Tavsiya etilgan gibrid shifrlash arxitekturasi milliy sog'liqni saqlash raqamlashtirish dasturlariga integratsiya qilinishi mumkin.

6. XULOSALAR

Tadqiqot natijalari asosida quyidagi xulosalar chiqarildi:

- Tibbiy tasvirlarni shifrlash zamonaviy diagnostika tizimlarida bemorlar ma'lumotlari maxfiyligini ta'minlashning asosiy vositasi hisoblanadi.
- AES-256 algoritmi tezlik va xavfsizlik nuqtai nazaridan katta hajmdagi tibbiy arxivlar uchun eng maqbul tanlov ekanligi isbotlandi.
- Gibrid shifrlash (AES + RSA) PACS tizimlarida kalit boshqaruvi va ma'lumot xavfsizligini optimallashtiradi.
- Shifrlashni diagnostika jarayoniga integratsiya qilish tashxis sifatiga sezilarli ta'sir ko'rsatmaydi.
- O'zbekiston sog'liqni saqlash tizimida tibbiy tasvirlarni shifrlash standartlarini joriy etish va shu sohadagi tadqiqotlarni rivojlantirish zaruriyati mavjud.

ADABIYOTLAR RO'YXATI

1. Natsheh, Q., Sălăgean, A., Zhou, D., & Edirisinghe, E. (2023). Automatic Selective Encryption of DICOM Images. Applied Sciences, 13(8), 4779.

2. Lata, K., Gupta, C., & Cenkeramaddi, L. R. (2025). A cryptographic framework for secure medical imaging in smart healthcare environments. Results in Engineering, Elsevier.

3. Desjardins, B., Sammer, M. B., Towbin, A. J., & Chen, P. H. (2019). DICOM images have been hacked! Now what? American Journal of Roentgenology.

4. Mirsky, Y., Mahler, T., Shelef, I., & Elovici, Y. (2019). CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning. 28th USENIX Security Symposium.

5. NIST SP 800-111. (2007). Guide to Storage Encryption Technologies for End User Devices. National Institute of Standards and Technology (NIST).

6. DICOM Standard. (2023). Digital Imaging and Communications in Medicine. NEMA. URL: https://www.dicomstandard.org.

7. O'zbekiston Respublikasining Qonuni. (2019 yil 2-iyul). "Shaxsga doir ma'lumotlar to'g'risida", O'RQ-547-son.