

















ORIGINAL

Multimedia data processing in an intelligent medical system featuring embedded elliptic curve cryptography

Tratamiento de datos multimedia en un sistema médico inteligente con criptografía de curva elíptica incorporada

Muslima Abdullaeva¹  , Nafisa Turaeva²  , Shaxodat Yadgarova¹  , Dilrabo Khalimova³  , Elnora Eshonkulova⁴  , Madina Yormatova¹  , Qiyom Nazarov⁵  

¹Bukhara State Medical Institute named after Abu Ali ibn Sino. Bukhara, Uzbekistan.

²Samarkand State Medical University. Samarkand, Uzbekistan.

³Bukhara State Medical Institute. Uzbekistan.

⁴Bukhara University of Innovative Education and Medicine, Uzbekistan

⁵“Tashkent Institute of Irrigation and Agricultural Mechanization Engineers” National Research University. Tashkent, Uzbekistan.


Cite as: Abdullaeva M, Turaeva N, Yadgarova S, Khalimova D, Eshonkulova E, Yormatova M, et al. Multimedia data processing in an intelligent medical system featuring embedded elliptic curve cryptography. Health Leadership and Quality of Life. 2024; 3:199. <https://doi.org/10.56294/hl2024.199>

Submitted: 03-03-2024

Revised: 23-06-2024

Accepted: 15-10-2024

Published: 16-10-2024

Editor: PhD. Prof. Neela Satheesh 

Corresponding Author: Muslima Abdullaeva 

ABSTRACT

Currently, global disease diagnosis is prevalent, and the evaluation of digital medical images (MI) is integral to Intelligent Medical Systems (IMS), which facilitates the early diagnosis and treatment of prevalent and severe illnesses. In this scenario, modifying or altering just one pixel of an MI during transmission across an insecure channel might result in an erroneous diagnosis, jeopardizing patient health and causing detrimental delays. Consequently, transmitting IMS multimedia information to healthcare providers presents several security issues. This study presents a Multimedia Data Processing framework using Embedded Elliptic Curve Cryptography (MDP-EECC) inside an IMS. The suggested MDP architecture comprises an Edge Level (EL), a Fog Computing (FC) stage, a Cloud computing Storage (CS) level, and a Blockchain (BC) tier. The EL gathers and transmits regular health data from the patient to the upper layer. The multimedia information from the EL is safely stored in BC-assisted CS via FC nodes using simple cryptography. Medical professionals conduct secure searches of such data for therapy or monitoring purposes. Inexpensive cryptographic methods are suggested via the use of Elliptic Curve Cryptography (ECC) with ECC-Diffie-Hellman (ECDH) and ECC-Digital Signature (ECDS) algorithms to ensure the security of MDP while preserving privacy. The suggested approach is tested using publicly accessible chest X-ray pictures. The efficacy of the suggested version is assessed and validated via comprehensive experimentation using the latest security techniques available. Compared to state-of-the-art approaches, the suggested version demonstrates superior security characteristics and can withstand different known assaults.

Keywords: Data Processing; Multimedia; Cloud Computing; Edge; Blockchain; Elliptic Curve Cryptography; Intelligent Medical Systems.

RESUMEN

En la actualidad, el diagnóstico global de enfermedades está muy extendido, y la evaluación de imágenes médicas digitales (IM) forma parte integral de los Sistemas Médicos Inteligentes (SMI), que facilitan el diagnóstico precoz y el tratamiento de enfermedades prevalentes y graves. En este escenario, la modificación o alteración de un solo píxel de una IM durante la transmisión a través de un canal inseguro podría dar lugar

a un diagnóstico erróneo, poniendo en peligro la salud del paciente y causando retrasos perjudiciales. En consecuencia, la transmisión de información multimedia IMS a los proveedores de asistencia sanitaria presenta varios problemas de seguridad. Este estudio presenta un marco de procesamiento de datos multimedia mediante criptografía de curva elíptica incorporada (MDP-EECC) dentro de un IMS. La arquitectura MDP sugerida comprende un nivel Edge (EL), una etapa Fog Computing (FC), un nivel Cloud Computing Storage (CS) y un nivel Blockchain (BC). El EL recopila y transmite los datos sanitarios periódicos del paciente al nivel superior. La información multimedia procedente del EL se almacena de forma segura en el CS asistido por BC a través de nodos FC utilizando criptografía simple. Los profesionales médicos realizan búsquedas seguras de estos datos con fines terapéuticos o de seguimiento. Se sugieren métodos criptográficos económicos mediante el uso de criptografía de curva elíptica (ECC) con algoritmos ECC-Diffie-Hellman (ECDH) y ECC-Firma Digital (ECDS) para garantizar la seguridad del MDP preservando la privacidad. El método propuesto se prueba con radiografías de tórax de acceso público. La eficacia de la versión propuesta se evalúa y valida mediante experimentos exhaustivos en los que se utilizan las últimas técnicas de seguridad disponibles. En comparación con los enfoques más avanzados, la versión propuesta demuestra unas características de seguridad superiores y puede resistir diferentes ataques conocidos.

Palabras clave: Procesamiento de Datos; Multimedia; Cloud Computing; Edge; Blockchain; Criptografía de Curva Elíptica; Sistemas Médicos Inteligentes.

INTRODUCTION

The dissemination of biological knowledge is a significant advancement for developing innovative therapies and treatments for illnesses in contemporary cultures and organized groups. The primary factors supporting the IMS are digitization, digital storage, and specialists' online access to MI data. Patients own exclusive ownership of electronic health information generated by hospitals after their visits. Sharing information enhances the value of unexplored possibilities, which is attributable to the advent of the technological age and the accumulation of vast data quantities that have initiated the era of big data.⁽¹⁾ With appropriate incentives, companies that gather, process, evaluate, store, and share data with other stakeholders have emerged due to the value of information and the significance of its distribution. This has captured the interest of several businesses, particularly regarding CS and processing methods, data analysis, and authenticity, leading conventional industries to rely on data for their business activities and viability. Cloud vendors must let clients exchange and explore MI data stored in their libraries in a controlled cross-domain, and adaptable way.⁽²⁾

Cloud Service Suppliers (CSS) have a deficiency in collaborative data exchange due to the adverse consequences of releasing their information.⁽³⁾ The obtained data poses a risk of exploitation by unethical users for owners and administrators. Numerous encryption methods have been devised to address the challenges associated with MI data sharing, yet they remain inadequate.⁽⁴⁾ Cryptographic methods are introduced due to the untrustworthiness of CS servers and the need to safeguard clients' data privacy, necessitating data encryption before transmission to the cloud. Conventional encryption methods, meanwhile, inhibit users' ability to search, leading to a worse user interface. Accessible encryption systems have been formulated in two-sample contexts, including symmetric-key and public-key frameworks,^(5,6) to preserve search capabilities over encrypted MI information. Despite the greater efficiency of symmetric-key configurations compared to public-key alternatives, several challenges remain unresolved regarding search terms on encoded MI information, whether conducted by patients or healthcare professionals. The primary risks to healthcare information safety are user-side authentication (ensuring the patient is an authentic user), server-side authentication, and storing, retrieving, and searching MI information without reliance on an authorized third party.

Recently, the BC technique has shown superior security and computational efficiency relative to traditional cryptographic systems for cloud MDP. Consequently, BC is an essential technology for the upcoming Healthcare 4.0 regulations. A nuanced transformation in the healthcare sector is imminent, driven by wireless digital health record methodologies, real-time MI data collection via wearable devices, Artificial Intelligence (AI), and enhanced data analysis. It will improve healthcare presentation and the calculation of results in the next years. Healthcare 4.0 denotes the forthcoming upheaval. The phrase has emerged from Industry 4.0 and the following evaluation of Internet of Things (IoT) applications.⁽⁷⁾

Consequently, Healthcare 4.0-enabled e-healthcare is developing technology to monitor the wellness of isolated patients. The MDP of health information, including digital images, is susceptible to several security concerns. These vulnerabilities may occur during the transfer of electronic MI from the EL to the CS level or while obtaining stored data from the CS to the authorized user at the EL.⁽⁸⁾ Existing BC-based safety measures provide promising outcomes; nevertheless, they are hindered by constraints such as processing ineffectiveness,

vulnerability to quantum threats, and challenges in effective MI archiving and retrieving. This research proposes a unique architecture that integrates efficient image processing algorithms, an inexpensive cryptographic mechanism, safeguards against quantum threats, and robust security measures to address these limitations.

Literature review

Safeguarding MI data is crucial in light of the increasing frequency of cybercriminal assaults. Recently, there has been a concerning increase in the number and magnitude of MI data breaches. Furthermore, as MI equipment increasingly links to other healthcare facilities and worldwide networks, the risk of many cyberattacks emerges as a significant hazard. Attacks on hardware and software infrastructures may jeopardize the wellness of patients, impair electronic health information, and result in loss of information.⁽⁹⁾ In 2021, security breaches in healthcare impacted around 25 percent of consumers in the United States. Images are disseminated over social channels, using integrated hidden data such as steganography and watermarking or encryption methods, including symmetrical and asymmetrical cryptographic methods, e.g., ECC, chaotic approaches, and sophisticated encryption standards.

In the present context of MI safeguarding, digital watermarking entails concealing information inside transmitted images in a manner that remains invisible to the human eye.⁽¹⁰⁾ The incorporated watermark will serve as a crucial instrument for detecting any compromise in the whole content of the data. Many critical criteria, including security, concealment, and payload, determine watermarking techniques' efficacy.⁽¹¹⁾ Watermarking is an exceptional option for safeguarding patients' confidential information during telehealth data transfers. Over the past ten years, several strategies for picture watermarking have been proposed in the literature, focusing on characteristics such as human interpretation, inclusion domain, and detection, among others.^(12,13)

Steganography involves concealing private data by embedding it within an innocuous message during interaction, ensuring that only the sender and intended recipient know the secret's presence. In contrast, the primary objective of watermarking is to integrate a message into a host item, rendering it irretrievable. Steganographic methods are categorized into spatial domain methods and transform domain methods.⁽¹⁴⁾

Cryptography is a crucial mathematical instrument for ensuring network security preventing the theft, duplication, and unauthorized dissemination of sensitive data. In recent years, many picture encryption techniques have been proposed in the literature to enhance the safety of MI communication.⁽¹⁵⁾ These strategies are based on fundamental mathematical ideas or established data encryption technologies. In recent years, chaos-based MI encryption algorithms have garnered significant academic attention due to their remarkable characteristics, including sensitivity to beginning circumstances and control variables, ergodicity, randomness, and volatility.

Zhang et al.⁽¹⁵⁾ proposed a novel multiple-image encryption technology using DNA encoding and a chaotic system, whereby the combination and diffusion processes are conducted on a 3D DNA matrix. Chen, J et al.⁽¹⁶⁾ suggested an effective MI encryption method based on autonomous permutation dispersion and DNA random coding. The proposed encryption technique consists of n rounds, each including four stages: DNA arbitrary encoding, autonomous combination, autonomous diffusion, and DNA random decoding. Conversely, Belazi, A et al.⁽¹⁷⁾ proposed a novel chaos-based encryption system for MI, developed via chaos theory and DNA computing synthesis. This system has two encryption stages, initiated with a key creation layer using the SHA-256 hash algorithm. Recently, Zefreh EZ⁽¹⁸⁾ proposed an innovative MI encryption approach using an intersection framework for DNA processing, chaotic systems, and hash algorithms. This approach entails DNA-level permutation and dispersion, whereby a mapping function derived from the logistic map is used on the DNA MI to alter the positions of pixels randomly.

Conversely, ECC has lately garnered significant academic interest because of its essential attributes, including minimal computing demands, reduced memory consumption, compact key sizes, and elevated security levels. Consequently, many ECC-based picture encryption techniques have been developed to tackle security concerns in recent years. In 2021, Benssalah, M et al.⁽¹⁹⁾ introduced a novel encryption strategy using chaotic systems, whereby the keys are generated after the exchange of an arbitrary spot on an elliptic curve (EC) via the ECDH key exchange algorithm. This approach uses the logistic map to produce chaotic sequences based on starting parameters obtained from the common EC point. In 2022, Hayat et al.⁽²⁰⁾ developed a unique picture encryption technique using elliptic curves over finite rings. The technique consists of three primary processes, with the first step including the masking of the plain picture using points from an EC over a limited ring. In the second stage, dispersion in the masked MI has been generated by mapping from the EC over the limited ring to the EC over the limited field. The approach seems safe in most respects, yet this strategy employs intricate ECC over the Galois field with a substantial quantity of rational points. In 2020, Farwa, S et al.⁽²¹⁾ introduced a novel MI encryption system that employs Fresnel dispersion in the wave-propagation field, coupled with an EC-based reversible scrambling impact to provide substantial uncertainty in encryption.

Multimedia Data Processing framework using Embedded Elliptic Curve Cryptography (MDP-EECC) inside an IMS

This study proposes a novel, reliable, and comprehensive framework for executing MI data operations, including secure multimedia MI archiving, sharing, and retrieval, using BC, FL nodes, and CS while minimizing space and time requirements.⁽²³⁾ To reduce computational expenses and provide stringent security standards, MI are encrypted with minimal EECC-based cryptographic algorithms that use ECDS for checking signatures and ECDH for decoding and encoding processes.⁽²⁴⁾ To safeguard against tampering, forgery, and quantum risks using BC technology, a BC layer that interfaces with the CS has been proposed to retain metadata obtained from the CS layer. The experimental investigation using various datasets demonstrates the privacy and dependability of the proposed integrated EECC architecture.⁽²⁵⁾

Many wireless and wired gadgets, detectors, and devices have been installed in medical facilities, nursing homes, drug stores, and many other care settings, resulting in the constant and exponential collection and dissemination of vast data.⁽²⁶⁾ Despite progress in intelligent and integrated healthcare, additional studies, innovation, dissemination, and impact are necessary to achieve IMS. Safety and privacy protection are critical problems in IMS.

This section presents figure 1, which illustrates the proposed MDP-EECC for the IMS paradigm, including MDP with CSS and BC technologies.⁽²⁷⁾ A proposed cohesive framework has been developed, as seen in figure 1, by incorporating all significant advancements of the evolving IMS. The bidirectional links among the components facilitate MI's transfer and reception.⁽²⁸⁾ The suggested system has five elements: data holders (IoT nodes or patients), medical users, FL servers, CSS, and BC. Figure 1 illustrates the several strata of IMS creation, including an EL, an FC, a CS, and a BC layer. Wireless Body Area Network (WBAN) servers, mobile phones, personal computers, and other IoT gadgets constitute the EL.⁽²⁹⁾ FC layer registrations are fog authentication services that transfer data center processes to fog nodes to save bandwidth and ensure fast data rates.⁽³⁰⁾ The CS layer executes archiving functions, whereas the BC layers are liable for the circulation capacity of CSS information and logs within the chain of multiple blocks. This is purportedly the first effort to delineate the four layers of IMS.

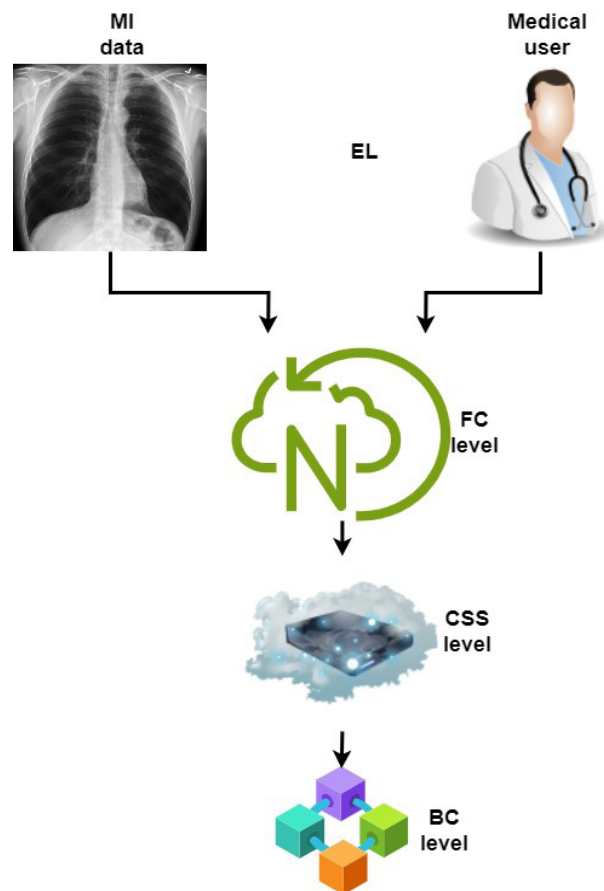


Figure 1. Proposed MDP-EECC for IMS

Initially, the MI detected by WBAN nodes affixed to every patient seems to have been gathered and authenticated by intelligent hospital methodologies. The identified data is then encrypted and sent to the FC nodes.⁽³¹⁾ Before transportation to CSS archiving, data undergoes an examination at fog nodes, requiring

indexing. To provide adequate security against diverse vulnerabilities, access records, and analytics were established and preserved on a distributed private BC for each inbound encrypted information from the victims.

Elements and Presumptions of the System

This section delineates the fundamental elements of the proposed model and their respective functions. Figure 1 illustrates the architecture of the EECC-enabled safe and IMS framework. Consequently, the proposed model has meticulously delineated components and their interrelations.⁽³²⁾ The following five elements comprise the suggested model:

- Internet of Things Node (IN): It is a component containing multimedia MI intended for storage or retrieval from the IMS. This entity has complete control over their medical information.⁽³³⁾ IoT nodes may establish access control rules for their MI and offer cryptographic keys and analytics. This node may do local audits and modify its data using newly generated cryptographic keys.
- Medical User (MU): An element that seeks to get MI from a CSS associated with a specific blockchain of an IN. It is only achievable with the consent of the designated IN. Healthcare personnel, including doctors, nurses, radiologists, physicians, and others, together with caregivers and medical insurance providers, often possess MU. The MU may send an inquiry to the CSS, which will retrieve the BC's meta-data, followed by the encrypted multimedia MI.
- FC: The FC is an element that facilitates fog operations via one or more tangible items equipped with detecting capabilities, such as gateways. IN transmits encrypted information to FC, while MU submits search queries to MU. FN authenticates the data and transmits it to CSS. It retrieves data from CSS, verifies it, and then transmits it to the specified recipient, IN or MU. FC functions as an intermediary between CSS and EL entities without data retention.
- CS: CSS may be either public or private. This element is responsible for saving the encrypted multimedia MI sent by IN. It also requires the retention of analytics and access records for all received encrypted information on the BC.
- Private BC: The function of Private BC is to encrypt the associated metadata and access logs of each newly created data segment inside the system. The system's data and MU records are distributed on the blockchain to facilitate search capabilities and address quantum hazards arising from parallel computing resources and other common dangers like manipulation. Hyperledger and Ripple are two prominent BC platforms used to decentralize BC technology.

The presumptions of the proposed EECC for IMS are defined below.⁽³⁴⁾

- Each IN aids patients by transmitting multimedia MI directly via optical detectors.
- In the EL, connectivity among IN is safe and utilizes energy-efficient conventional routing and clustering methods. The FC layer comprises FC nodes, including access points, that are responsible for gathering encrypted data, validating it, and transmitting it to CSS.
- The CSS may be classified as public or private based on real-time application requirements.
- BC is believed to be confidential and to possess financial connections to a certain healthcare facility. Mutual contracts with hospital administrators govern financial interactions between BC CSSs and other physical infrastructures.
- The system has already registered and approved each IN, which may be an owner of information or a MU. The standard registration procedure for new IN will be implemented, and individual IDs will be created.
- Designated users possess connectivity to a BC (either the MU or the IN).
- The hospital management may provide a designated cohort of users.

EECC

The proposed approach is intended to store multimedia data inside a FC and BC framework safely.⁽³⁵⁾ Below is a sequential analysis of the proposed EECC method through an elucidation of the relevant notations:

Algorithm: MDP-EECC

Parameters:

IN: MI data (specifically, a chest X-ray picture).

TS: A timestamp produced by the system to guarantee authenticity.

Phase 1: At IN (EL node)

- 1.1. Scan the Chest X-ray picture: The image is transformed into a collection of pixels or MI data for analysis.
- 1.2. Implement inverse: A conversion is performed on the picture data (mod 256,255D).
- 1.3. Obtain arbitrary numbers: A generator, r , produces an arbitrary value used for encryption.

- 1.4. Key creation using ECC: the confidential key (Pr) and public key (Pu) of ECC are produced.
 - 1.5. Calculate the common secret key (Sh) using ECDH: Both the IN and the MI data owner derive a shared secret key from the EC of ECC.
 - 1.6. If a shared key is present, the MI information is encrypted with this key, producing ciphertext (μ encrypt).
 - 1.7. Upon success, the encrypted MI is processed using a safe hashing technique (SHA-2).
 - 1.8. Authenticate the encrypted MI using the pair (r,s) indicative of an ECDS. (r,s) denotes the ECDS signature pair that verifies the authenticity of the data.
 - 1.9. Transmit the encrypted MI information, index, and TS to the CS.
- If any component of the encryption procedure is unsuccessful, the MI is rejected.

Phase 2: At FC nodes

- 2.1. Acquire the Pu and authenticate it.
- 2.2. Generate a hash for the MI: Authenticate the reliability via SHA-2.
- 2.3. Verify signature: Authenticate the EC signature using (r,s).
- 2.4. If the signature is authenticated, transmit the data to the subsequent step (e.g., CS). Alternatively, the MI is rejected.

Phase 3: In CS level

- 3.1. Acquire the Pu and verify its authenticity.
- 3.2. Hash authentication: The hash of the encrypted information is computed and assessed for authenticity.
- 3.3. Signature validation: The signature is examined as in phase 2.
- 3.4. Upon verification, the MI information is saved in CS or private BC, and an index for the information is established and revised for further access. If authentication fails at any point, the MI data is eliminated.

Phase 4: Stop

The multimedia data is safely archived after successfully completing the whole procedure.

This method guarantees the secure transfer and storage of MI data by integrating FC with BC technology. Implementing ECDS and ECDH guarantees safe encryption and effective key exchange. Each phase incorporates verification measures such as hashing and digital signatures to ensure data authenticity.

RESULTS AND DISCUSSION

The suggested model was run on a Windows 10 machine with 4 GB of RAM and an Intel® Core i5 CPU. It has evaluated the proposed image processing techniques on chest X-ray MI of COVID-19-infected patients. We have gathered chest X-ray MI from the⁽²²⁾. A 150 chest X-ray MI collection has been obtained from this database for performance evaluation.

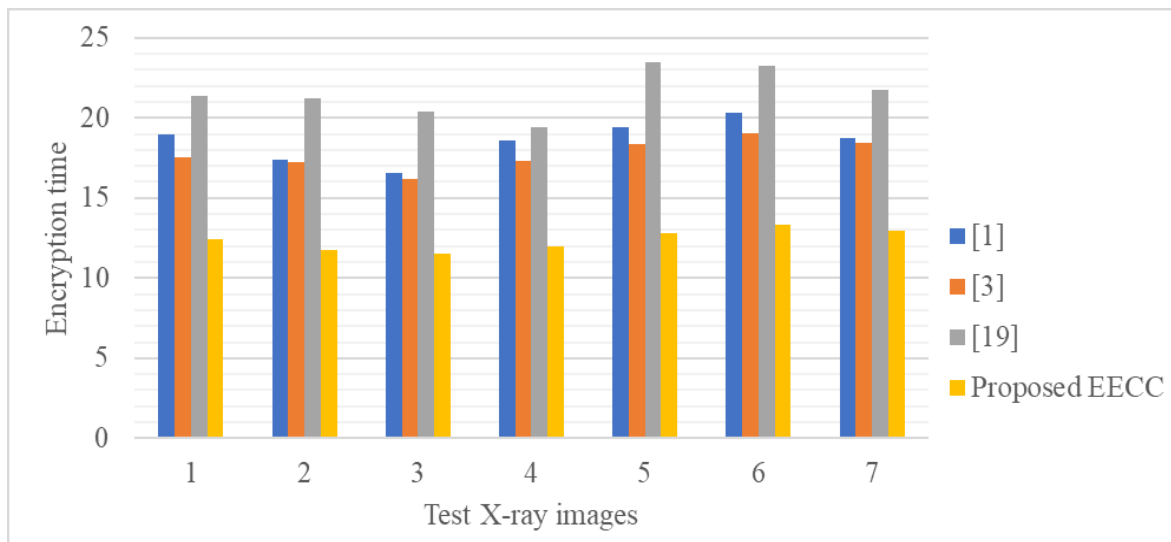


Figure 2. Encryption time analysis (in seconds) of various cryptographic schemes for MDP in IMS

Figure 2 shows the encryption time analysis of various cryptographic schemes for MDP in IMS. The suggested EECC consistently performs better than competing methods by exhibiting the shortest encryption time throughout the test images. For Test Image 1, EECC registers 12,45 seconds, while reference records 18,99 seconds,⁽¹⁾ records 17,51 seconds,⁽³⁾ records 21,34 seconds.⁽¹⁹⁾ Comparably, Test Image 7 demonstrates 12,99

seconds for EECC, while the alternative approaches exhibit longer timeframes. This illustrates that EECC offers a more efficient encryption mechanism than other cryptographic systems, particularly in managing multimedia MI in IMS.

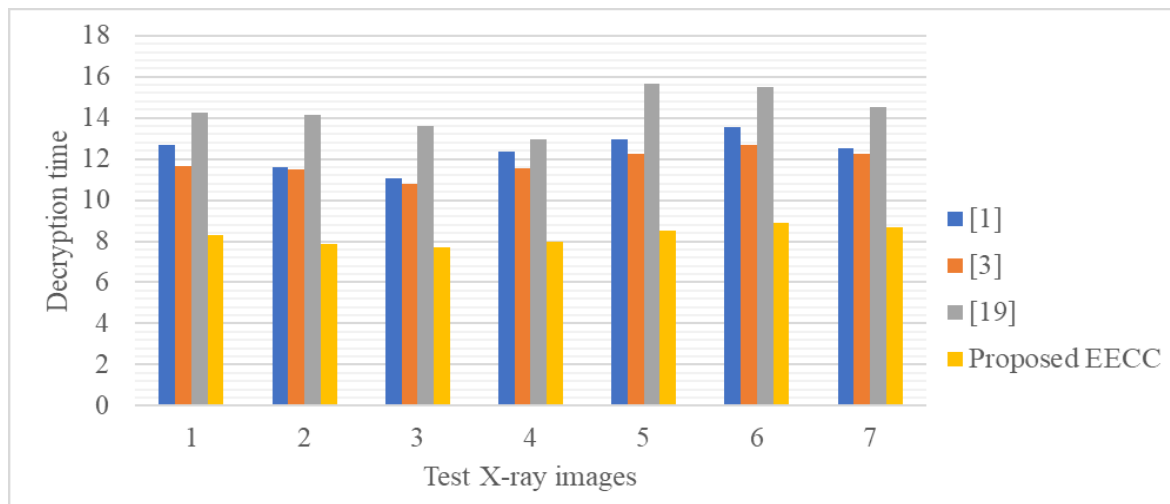


Figure 3. Decryption time analysis (in seconds) of various cryptographic schemes for MDP in IMS

Figure 3 depicts the decryption time analysis (in seconds) of various cryptographic schemes for MDP in IMS. The proposed EECC consistently demonstrates the shortest decryption times for all test images, underscoring its efficiency relative to alternative cryptographic algorithms. In test image 1, the proposed EECC attains a decryption duration of 8,30 seconds, whereas the durations for other methods vary from 11,67 to 14,23 seconds. This pattern persists across all images, whereby the proposed EECC exhibits markedly quicker decryption timings, establishing it as the most optimal and productive method for reducing decryption delays in MDP inside the IMS framework.

The encryption time refers to the complete duration for creating the encrypted message at the IN. In contrast, the decryption time denotes the entire time needed to retrieve the primary MI at the medical user node using the cryptographic decryption function. The findings indicate that the suggested ECC-based technique executes all cryptographic operations more swiftly than existing state-of-the-art approaches. The tiny key size necessitates reduced calculation time and space needs in the proposed EECC system for MDP in IMS.

CONCLUSIONS

This paper introduces a Multimedia Data Processing architecture using Embedded Elliptic Curve Cryptography (MDP-EECC) inside an IMS. The EL collects and transmits routine health data from the patient to the higher tier. The multimedia information from the EL is securely saved in BC-assisted CS via FC nodes using basic cryptography. Medical experts do secure searches of such data for therapeutic or monitoring objectives. Cost-effective cryptographic techniques are proposed via the implementation of EECC using ECDH and ECDS algorithms to guarantee the security of MDP while maintaining privacy. The proposed method is evaluated using publically available chest X-ray images. The suggested EECC consistently performs better than competing methods by exhibiting the shortest encryption time throughout the test images. The proposed EECC consistently demonstrates the shortest decryption times for all test images, underscoring its efficiency relative to alternative cryptographic algorithms. In test image 1, the proposed EECC attains a decryption duration of 8,30 seconds, whereas the durations for other methods vary from 11,67 to 14,23 seconds.

BIBLIOGRAPHIC REFERENCES

1. Mahajan, H. B., & Junnarkar, A. A. (2023). Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. *Multimedia Tools and Applications*, 82(28), 44335-44358.
2. Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and privacy of patient information in medical systems based on blockchain technology. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 17(2s), 1-17.
3. Ngabo, D., Wang, D., Iwendi, C., Anajemba, J. H., Ajao, L. A., & Biamba, C. (2021). Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. *Electronics*, 10(17), 2110.

4. Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2020). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*, 79(15), 9711-9733.
5. Pal, K. (2022). A decentralized privacy preserving healthcare blockchain for iot, challenges, and solutions. In *Prospects of Blockchain Technology for Accelerating Scientific Advancement in Healthcare* (pp. 158-188). IGI Global.
6. Christo, M. S., Jesi, V. E., Priyadarsini, U., Anbarasu, V., Venugopal, H., & Karuppiah, M. (2021). Ensuring improved security in medical data using ecc and blockchain technology with edge devices. *Security and Communication Networks*, 2021(1), 6966206.
7. Aceto, G., Persico, V., & Pescapé, A. (2020). Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. *Journal of Industrial Information Integration*, 18, 100129.
8. Abbas, A., Alroobaee, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and ubiquitous computing*, 28(1), 59-72.
9. Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: an exploratory analysis. *Perspectives in health information management*, 19(Spring).
10. Reddy, K. V. S. V., & Reddy, S. N. (2021). An Improved Medical Image Watermarking Technique Based on Weber's Law Descriptors. *Traitement du Signal*, 38(6).
11. Rajendran, S., Krithivasan, K., & Doraipandian, M. (2021). A novel cross cosine map based medical image cryptosystem using dynamic bit-level diffusion. *Multimedia Tools and Applications*, 80(16), 24221-24243.
12. Kahlessenane, F., Khaldi, A., Kafi, R., & Euschi, S. (2021). A robust blind medical image watermarking approach for telemedicine applications. *Cluster computing*, 24(3), 2069-2082.
13. Devi, H. S., & Mohapatra, H. (2023). A novel robust blind medical image watermarking using rank-based DWT. *International Journal of Information Technology*, 15(4), 1901-1909.
14. Alhomoud, A. M. (2021). Image steganography in spatial domain: Current status, techniques, and trends. *Intelligent Automation & Soft Computing*, 27(1).
15. Zhang, X., & Wang, X. (2019). Multiple-image encryption algorithm based on DNA encoding and chaotic system. *Multimedia Tools and Applications*, 78(6), 7841-7869.
16. Chen, J., Zhu, Z. L., Zhang, L. B., Zhang, Y., & Yang, B. Q. (2018). Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption. *Signal Processing*, 142, 340-353.
17. Belazi, A., Talha, M., Kharbech, S., & Xiang, W. (2019). Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE access*, 7, 36667-36681.
18. Zefreh, E. Z. (2020). An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions. *Multimedia Tools and Applications*, 79(33), 24993-25022.
19. Benssalah, M., Rhaskali, Y., & Drouiche, K. (2021). An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. *Multimedia Tools and Applications*, 80(2), 2081-2107.
20. Hayat, U., Ullah, I., Azam, N. A., & Azhar, S. (2022). A novel image encryption scheme based on elliptic curves over finite rings. *Entropy*, 24(5), 571.
21. Farwa, S., Bibi, N., & Muhammad, N. (2020). An efficient image encryption scheme using Fresnelet transform and elliptic curve based scrambling. *Multimedia Tools and Applications*, 79, 28225-28238. <https://www.kaggle.com/tawsifurrahman/covid19-radiography-database>

22. Chukwusa, J. (2021). An Assessment of the Information Literacy Skills of Students in Nigerian Universities. *Indian Journal of Information Sources and Services*, 11(1), 9-15. <https://doi.org/10.51983/ijiss-2021.11.1.2649>
23. Rakesh, N., Mohan, B. A., Kumaran, U., Prakash, G. L., Arul, R., & Thirugnanasambandam, K. (2024). Machine learning-driven strategies for customer retention and financial improvement. *Archives for Technical Sciences*, 2(31), 269-283. <https://doi.org/10.70102/afts.2024.1631.269>
24. Ilori Maria, E., Shutti Bolaji, S., Oyintola Isiaka, A., Abdullahi Mostura, A., & Oluwafemi Segun, V. (2021). Evaluation of Public Services by its Users of an Academic Library, Lagos State University (LASU), Ojo, Nigeria. *Indian Journal of Information Sources and Services*, 11(1), 41-46. <https://doi.org/10.51983/ijiss-2021.11.1.2653>
25. Biswas, B., Neogi, S., & Roy, B. (2024). Application of delighting to optimize window-to-wall ratio (wwr) in buildings in indian climatic conditions. *Archives for Technical Sciences*, 2(31), 248-258. <https://doi.org/10.70102/afts.2024.1631.248>
26. Muthuraja, S., Lakshmisha, H., Nagaraja, H., & Arunkumar, M. P. (2021). Webometric Analysis of Selected Universities Websites in Karnataka: An Evaluative Study Using Alexa Internet. *Indian Journal of Information Sources and Services*, 11(1), 22-27. <https://doi.org/10.51983/ijiss-2021.11.1.2810>
27. Nandhinieswari, S., & Indumathi, A. (2024). Bilevel optimized recursive feature eliminator for cervical cancer feature selection process. *Archives for Technical Sciences*, 2(31), 311-328. <https://doi.org/10.70102/afts.2024.1631.311>
28. Ilori, M. E., Oluwafemi, V. S., & Odusina, E. S. (2020). School Library Services as a Catalyst for the Better Basic Education in Nigeria. *Indian Journal of Information Sources and Services*, 10(1), 1-6. <https://doi.org/10.51983/ijiss.2020.10.1.485>
29. Suljić, N., & Kovčić, O. (2018). Analysis of Time Oscillations of Water on Lake Modric as a Multi-Purpose Reservoir. *Archives for Technical Sciences*, 1(18), 31-40.
30. Saidova, K., & et al. (2024). Developing framework for role of mobile app in promoting aquatic education and conservation awareness among general people. *International Journal of Research and Environmental Studies*. 4. 58-63. [10.70102/IJARES/V4S1/10](https://doi.org/10.70102/IJARES/V4S1/10).
31. Saidova, K., & et al. (2024). Assessing the Economic Benefits of Climate Change Mitigation and Adoption Strategies for Aquatic Ecosystem. *International Journal of Research and Environmental Studies*. 4. 20-26. [10.70102/IJARES/V4S1/4](https://doi.org/10.70102/IJARES/V4S1/4).
32. Saidova, K., & et al. (2024). Assessing the impact of invasive species on native aquatic ecosystems and developing management strategies. *International Journal of Research and Environmental Studies*. 4. 45-51. [10.70102/IJARES/V4S1/8](https://doi.org/10.70102/IJARES/V4S1/8).
33. Deepthi, K. J., Balakrishnan, T. S., Krishnan, P., & Ebenezar, U. S. (2024, June). Optimized Data Storage Algorithm of IoT Based on Cloud Computing in Distributed System. In 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0 (pp. 1-5). IEEE.
34. Sasikala, R., Deepthi, K. J., Balakrishnan, T. S., Krishnan, P., & Ebenezar, U. S. (2024, June). Machine Learning-Enhanced Analysis of Genomic Data for Precision Medicine. In 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0 (pp. 1-5). IEEE.

FINANCING

No financing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Methodology: Muslima Abdullaeva, Nafisa Turaeva, Shaxodat Yadgarova, Dilrabo Khalimova, Elnora Eshonkulova, Madina Yormatova, Qiyom Nazarov.

Resources: Muslima Abdullaeva, Nafisa Turaeva, Shaxodat Yadgarova, Dilrabo Khalimova, Elnora Eshonkulova, Madina Yormatova, Qiyom Nazarov.

Display: Muslima Abdullaeva, Nafisa Turaeva, Shaxodat Yadgarova, Dilrabo Khalimova, Elnora Eshonkulova, Madina Yormatova, Qiyom Nazarov.

Drafting - original draft: Muslima Abdullaeva, Nafisa Turaeva, Shaxodat Yadgarova, Dilrabo Khalimova, Elnora Eshonkulova, Madina Yormatova, Qiyom Nazarov.

Writing - proofreading and editing: Muslima Abdullaeva, Nafisa Turaeva, Shaxodat Yadgarova, Dilrabo Khalimova, Elnora Eshonkulova, Madina Yormatova, Qiyom Nazarov.