The Open Bioinformatics Journal
DOI: 10.2174/0118750362303634240624112446, 2024, 17, e18750362303634

ISSN: 1875-0362
1

RESEARCH ARTICLE **OPEN ACCESS**

Enhancing Medical Image Security through a Novel Framework: Crypto-aware Elliptic Curve Diffie-hellman with Key Derivation Function

M. Senthilkumar[1], K. Suthendran[1,*] and Vinayakumar Ravi[2,*]

[1]*School of Computing, Kalasalingam Academy of Research and Education, Krishnankoil, India*
[2]*Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar, Saudi Arabia*

Abstract:

Aim: To develop and apply advanced methods to enhance medical image security, ensuring patient data integrity, confidentiality, and authenticity throughout the stages of image collection, transmission, and storage.

Background: Retaining patient privacy and data accuracy in the context of accessible healthcare require the secure broadcast and storage space of medical imaging. Because of the increasing dependence on digital medical imaging technology, it is essential to protect these private images from illegal access and possible cyber attacks.

Objective: Work addresses the drawbacks of conventional encryption techniques in the healthcare sector and offers a novel Crypto-Aware Elliptic Curve Diffie Hellman with Key Derivation Function (CAECDH-KDF) encryption technique to improve the security of medical images.

Methods: The suggested encryption architecture combine domain-specific methods designed for medical imaging data with sophisticated cryptographic algorithms. The framework, in difference to conservative encryption methods, employs an effective tactic that strikes a compromise between processing speed and security. To achieve this, better encryption methods for medical image characteristics are incorporated.

Results: Comparisons are made between the suggested method's security, computation time (0.003001), encryption time (0.001998s), decryption time (0.001001s), entropy (7.997633), and throughput (4.0887) of conventionally encrypted approaches.

Conclusion: A large amount of test images have been utilized to evaluate the effectiveness of the suggested technique. According to numerous tests, the suggested strategy outperforms conventional methods.

Keywords: Encryption, Elliptic curve diffie hellman with key derivation function (CAECDH-KDF), Decryption, Medical images, Patients, Images.

*Address correspondence to these authors at the Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar, Saudi Arabia and School of Computing, Kalasalingam Academy of Research and Education, Krishnankoil, India; E-mails: vinayakumarr77@gmail.com and k.suthendran@klu.ac.in

Cite as: Senthilkumar M, Suthendran K, Ravi V. Enhancing Medical Image Security through a Novel Framework: Crypto-aware Elliptic Curve Diffie-hellman with Key Derivation Function. Open Bioinform J, 2024; 17: e18750362303634. http://dx.doi.org/10.2174/0118750362303634240624112446

Received: January 10, 2024
Revised: May 08, 2024
Accepted: June 14, 2024
Published: June 28, 2024

1. INTRODUCTION

The patient and the medical expert are in separate places, telemedicine, a fast-growing field, provides the people with remote medical services. Sensitive patient information, such as clinical photographs is exchanged across many communication channels. To save these clinical images, which is accessible to the authorized people stationed at any location, the health sector has to be upgraded [1]. This specific type of service is provided using the cloud storage systems and if they are constructed improperly or in a way that doesn't fulfill the

security standards, these arrangements are susceptible to cybersecurity threats. Numerous people are trading massive amounts of encrypted information over the internet, an extensive network. The methods for securing sensitive information, including communication and storage networks, have taken little longer than expected [2]. In this case, only one technique of keeping medical images provides excellent security and is valuable for people with cryptographic credentials. Using dynamical arrangements with predictable values, ergodicity, and complexity of structure, a larger key area, flexibility and extraordinary periodicity follow. They are also responsive to primary values [3].

Diagnostic information from patients from imaging tests, such as X-rays, MRIs, and CT scans, *etc*., which is essential, especially if the patient has a severe condition. Instance of even a small modification and adjustment to this crucial information might put the patient in danger of dying [4]. Take a look at an example of a patient receiving telehealth and telemedicine care while some fisheries engage anonymously and manipulate the patient's vital health records throughout the exchange. In this scenario, medical professional on another side receives inaccurate information, which might lead to wrong treatment or put someone's health or life in danger [5]. Securing medical images has numerous significant benefits. First, it protects a patient privacy and ensures that data protection laws are followed.

Furthermore, by limiting unauthorized access to and alteration of confidential medical data, it protects data integrity. Using access controls and audit trails, healthcare organizations can keep an eye on and restrict access to data. Robust security protocols not only prevent security breaches and their attendant legal ramifications but also promote professional teamwork among healthcare personnel, boost patient trust, and save costs. In general, maintaining the confidentiality, correctness, and dependability of patient data requires protecting medical images [6]. This research offers a unique Crypto-Aware Elliptic Curve Diffie Hellman with Key Derivation Function (CAECDH-KDF) strategy for encryption, improving medical image security and addressing limitations about traditional encryption approaches in healthcare.

1.1. Contribution of the Paper

- This research addresses the issues with conventional encryption techniques in healthcare and provides a novel CAECDH-KDF scheme for encryption to enhance the medical image security.
- We gathered the image dataset and applied the Sobel and Scharr filter technique to preprocess the data.
- The suggested encryption architecture combine domain-specific methods designed for medical imaging data with sophisticated cryptographic algorithms.
- By comparing entropy, encryption, decryption, and computation times with those of conventional methods, it shows the viability and efficacy of the suggested framework.

The sections of the article that follow: part 2 provides a number of related work; part 3 provides a more detailed description of the approach; and part 4 offers and discusses simulation results, experimental data sets, and discussion. The analysis is concluded in Part 5 with suggestions for more research.

2. RELATED WORK

An article [7] proposed a Grasshopper optimization and particle swarm optimization (GO-PSO), a unique cryptographic model with optimization methodologies to investigate the security of medical imaging in the Internet of Things (IoT). Security is essential since the hospital stores patient data on a cloud server. This execution's outcomes are contrasted and compared in various encryption algorithms with their optimization techniques, discovered most important peak signal-to-noise ratio measurements. A study [8] created an effective image encryption method for the healthcare sector, a powerful lightweight encryption algorithm. Numerous tests demonstrated that the suggested algorithm for image cryptosystems outperforms traditional methods in terms of efficiency. Clustering Convolutional Neural Networks (CLU-CNNs) are proposed, which are a domain adaptation framework for medical image processing [9, 10]. Without specialized domain adaptation training, to improve domain adaptability capability, CLU-CNNs use BN-IN Net and Agglomerative Nesting Clustering Filtering (ANCF). A highly secure and energy-efficient healthcare 5.0 system was created, where “elliptic curve cryptography-based energy-efficient routing protocol (ECC-EERP)” was followed. Paper [11] addressed challenges such as an inability to distribute annotated medical image data, adversarial assaults on deep neural networks (DNN)and designs with distorted medical image information, a loss of user and patient confidence in privacy and ethical concerns about medical information. A method focuses on building an algorithm that first extracts the noise-affected pixels in a medical image using a Switched Mode Fuzzy Median Filter (SMFMF), then replaces noisy pixels with a median pixel's value [12]. A study [13] described a method for creating a deep recurrent architecture-based medical image captioning model it integrates a Long Short-Term Memory (LSTM) model with a Multi-Level Transfer Learning (MLTL) structure. Another study [14] focused on the use of related neural networks to biological image encryption and the brain-like start enhancing coexisting hyper chaos. They start building in MCNN model, which consists of one multi-stablememristor synapse and two sub-neural networks. An effective and blind watermarking technique to secure telemedicine's transmission of medical images appropriately has been proposed. In the sphere of telemedicine, this strategy guarantees the integrity and traceability of critical medical images. The digital medical images are sent using these techniques with open-source networks.

2.1. Research Gap

Exploratory hybrid cryptography models which incorporate several optimization techniques for increased

security and efficiency is a crucial area of study that needs to be done in the body of literature currently accessible on medical imaging security in the context of the IoT. While numerous studies have proposed individual optimization-based cryptographic models, such as particle swarm optimization (GO-PSO) and Grasshopper optimization, there is still a research gap regarding the integration of different optimization methodologies within a single cryptographic framework specifically designed for medical imaging data. Furthermore, while several research have examined the effectiveness and efficacy of encryption approaches, nothing is known about how effectively these algorithms scale and relate to large-scale medical imaging data stored on cloud servers. The study could significantly affect how medical image data is kept private, secure, and authentic in cloud-based healthcare environments. The CAECDH-KDF technique uses a key derivation function and authenticated Diffie-Hellman key exchange to improve security, efficiency, scalability, flexibility, and privacy in IoT healthcare applications.

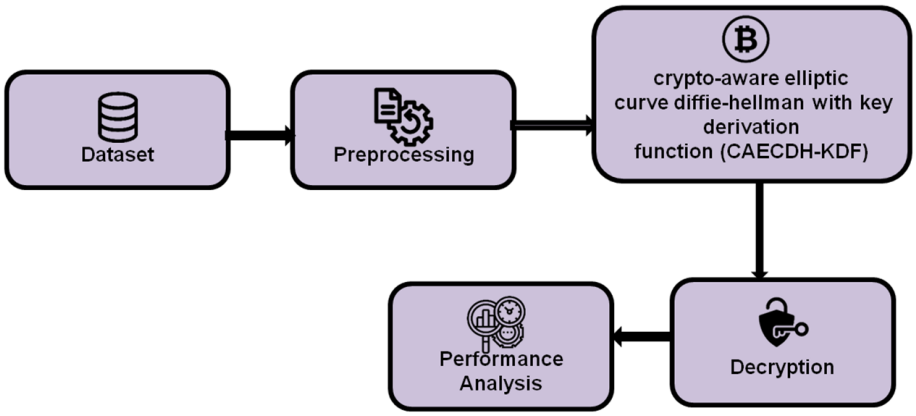

Fig. (1). Proposed method.

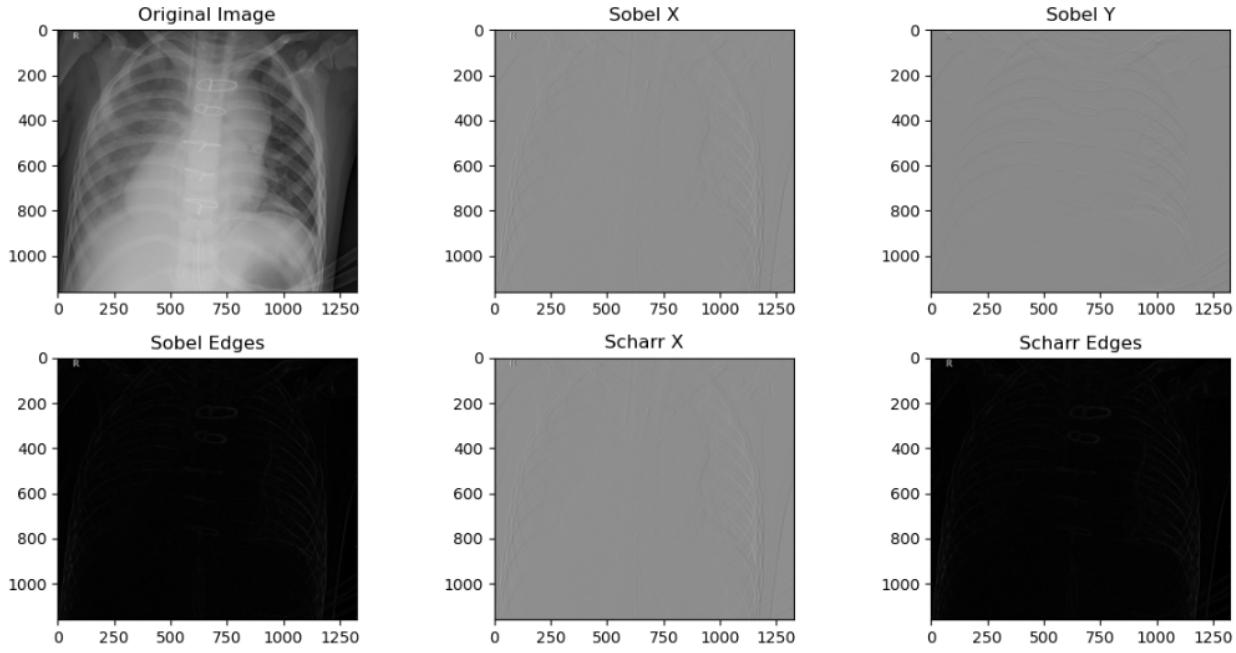

Fig. (2). Preprocessing result of sobel and scharr filter.

3. METHODS

The Crypto-Aware Elliptic Curve Diffie-Hellman with Key Derivation Function (CAECDH-KDF), a novel encryption technique, is presented in this portion of the paper, which employs a proposed model. The Sobel and Scharr filter is applied after the picture dataset has been gathered and preprocessed. The decryption process is employed for medical images. Fig. (**1**) shows the proposed model for medical image security. Here is a detailed description of each step.

3.1. Preprocessing using Sobel and Scharr Filter

3.1.1. Sobel Filter

A simple approximation to the idea of a gradient with smoothing is the Sobel filter. A common technique for detecting gradients in *w* and *z* axes, which is used for 3 x 3 convolution mask. The kernels is used to create gradient components $H_w H_z$ for the input images.These numbers are added together using Eq. (**1**) to estimate the gradient's magnitude and direction at each place.

$$H = \sqrt{H_w^2 + H_z^2} \quad \textbf{(1)}$$

G is a gradient's value, and G_x and G_y are its respective components.

3.1.2. Scharr filter

We provide the Scharr filtering for time series data in this subsection. They also describe the data is divided up for learning and prediction. We employ the complicated Scharr operator as described by the mask in Eq. (**2**) to remove noise and outliers from time series data.

$$H_w + iH_z = \begin{bmatrix} -4-4i & 0-11i & +4-4i \\ -10\_0i & 0+0i & +10+0i \\ -4+4i & 0+11i & +4+4i \end{bmatrix} \quad \textbf{(2)}$$

Where the vertical gradient is G_y and the horizontal gradient is G_x. The real component of G_x and the imaginary part of G_y are used in this complicated operator. Fig. (**2**) depicts the preprocessing result of Sobel and Scharr filter.

3.2. Crypto-aware Elliptic Curve Diffie Hellman with Key Derivation Function (CAECDH-KDF)

ECC became a common public-key encryption scheme and became quite popular. It is used in many other sectors and is a prominent topic of study in the field of cryptography. Elliptic curve cryptography is used by the CAECDH cryptographic protocol to provide safe key exchange between two parties. The Diffie-Hellman algorithm and elliptic curves are combined to create CAECDH. It is essentially viewed more as a key-agreement system than an encryption method. In other words, the process of key creation and key exchange between parties is defined (at least in part) by CAECDH. Now, it is up to the system to use those keys to encrypt the data. It makes use of the elliptic curve discrete logarithm problem's computational complexity to guarantee the integrity and secrecy of the sent keys. Using a single shared secret value, one or more secret keys can be obtained using the cryptographic technique known as KDF. By creating keys that are distinct and autonomous, it improves security even in the event that the original shared secret is compromised. Cryptographic hash functions and other pseudorandom approaches are commonly utilized by KDFs to generate keys that possess desired attributes like unpredictability and randomness. Because CAECDH-KDF allows for secure key generation and sharing, it can improve the security of medical images. It protects patient privacy and stops unwanted access by utilizing strong key derivation techniques and elliptic curve cryptography to guarantee the confidentiality and integrity of critical medical images. Elliptic Curve images as shown in Fig. (**3**).

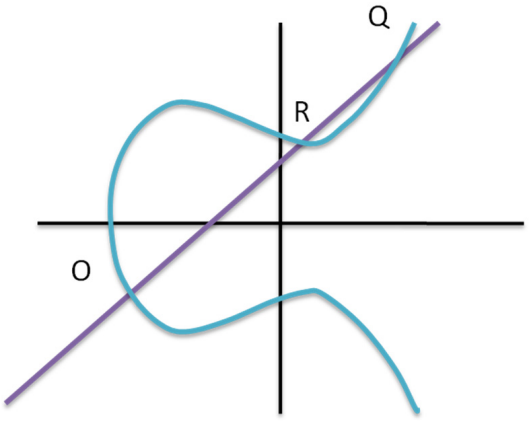

Fig. (3). Elliptic curve.

Using patient-specific data to produce individual encryption keys using AKDF's adaptive capabilities improves privacy. When it is used with the Diffie-Hellman protocol, it creates secure communication channels that protect image transfer. By making it secure and guaranteeing that vetted individuals of access and decode important medical images, their method satisfies the crucial need for confidentiality and integrity in medical imaging. After the shares are created, the encryption procedure uses the ECC technique.

3.2.1. Key Generation

Let *E* be the specified elliptic curve. Its definition spans the prime field *Fp*. Given a point *T* on this elliptic curve (*Fp*), *T* needs to have a prime order of n.

1. KeyGen (o,F,H,m)
2. Pricey (C_b)←$Q|Q$ = *random* ([1,*m*-1]) ϵ E_o
3. Let *Co*(*H*) = *base point of generator* H
4. *PubKey*(G_b)←*pointMult* (*prikey*(C_b)*Ao(*H*))
5. return PubKey, Prikey
6. End

A public key cryptographic method called elliptical curve cryptography (CAEC) is based on the algebraic structure of elliptic curves traversing finite fields. It uses a tiny key with non-EC encryption to provide a comparable level of security. The private key is favored at the ECC, and the prime value is chosen as n_p. Next, the following is used to express it: (Eq 3).

$$F = o(j)^3 + v * o(j) + u \quad \textbf{(3)}$$

Where $v = u = 2$ is a constant, and u and v represent it. The best points for the CAEC are chosen when state $W = Z$ and W and Z are determined to be, (Eq 4).

$$W = mod(F, m_o)$$
$$Z = mod(o(i)^2, m_o) \quad \textbf{(4)}$$

The elliptic curve's point is indicated by the symbol $O(j, i)$. A prime number is defined by n_p. The W and Z values are defined using the doubling approach. The best point $O_f(k, l)$ and O_e implies a public key: (Eq 5).

$$O_e = G * O_f \quad \textbf{(5)}$$

Each share is divided into a block during the encryption process and every block comprises encrypted sections. $B(i, j)$ represents the column and row of the blocks, whereas i and j represent the total number of blocks. All information supplied as input to encrypt the data. In addition to the point, the data $C_w(j, i)$ and $C_z(j + 1, i)$ is stated as follows: (Eq 6).

$$D_1 = G * O_f,$$
$$D_2 = (C_w, C_z) + D_1 \quad \textbf{(6)}$$

The private key (H) is used in the decryption process for communication decryption, whereas point D_{11} is used to decrypt pixels. (Eq 7).

$$D_{11} = G * D_1,$$
$$D_{ji} = D_2 - D_{11} \quad \textbf{(7)}$$

The ultimate outcome of the decryption process is displayed in D_{ji}. Pixel values for the original color bands (RGB) and IR are preserved separately from the D_{ji} results.

An improved version of the traditional Diffie-Hellman (DH) key exchange protocol, Crypto-Aware DH, was developed to fend off quantum computing assaults. A symmetric key exchange technique used for encryption inDH key agreement protocol, commonly known as an exponential key agreement. The DH method's fundamental goal is to enable information sharing across a public communications channel between two or more parties to construct and exchange an identical and secret session key. A shared and symmetric key is generated by two users across an insecure network using the DHK agreement protocol.

The values for the shared keys range that 1 to (P - 1). Each party calculates the value of the shared secret key that will be used to encrypt the image data that is transferred over the network after exchanging their shared keys. DHKE relies on a straightforward characteristic of modular exponentiations. (Eq 8).

$$(H^{YB}) mod\ O = (H^{YC}) mod\ O \quad \textbf{(8)}$$

The following describes the Diffie-Hellman key exchange mechanism, where positive integers H, Y, C and O are present. The value of k is computed using the existing formulas $Y_B = H^B$ mod O and $Y_C = H^C$ mod O without exposing B and C, which are secret exponents. (Eq 9).

$$L = (H^{YC}) mod\ O \quad \textbf{(9)}$$

The shared secret key K between the client and server components was generated and distributed in this study using a DHK exchange technique. Then, a 256-bit integer was used to define and encode the DH encryption key K.

Improving the security of medical images requires the use of a KDF. An adaptive KDF guarantees that encryption keys are distinct and particular to each medical image by creating cryptographic keys using sensitive patient information and metadata, such as medical record identities and patient traits. The Advanced Encryption Standard (AES) key were derived using the shared secret key in employing a KDF. The KDF component prevents a man-in-middle technique, a severe problem with ECDH and adds another degree of protection. The KDF ensures that the (S) key created by SHA256 is hashed. Implementing the key derivation function (KDF) entails the following steps:

- Conversion of a shared key (S) to a byte
- The bytes are hashed with the SHA256 hash library, making a hash key (H).

The key length and H are the foundations for the AES key derivation. AES-256-GCM uses keys that are 256 bits long. The size of H must match the 256 key bits required to create an AES key and for encryption.The AES key chooses (S) key's first segment, while the second is chosen. Furthermore, the hash (shared) key (H) and key length were considered. The key's size, quality, and output size affect a strong cryptographic system. This size offers a significant production and key. The Diffie-Hellman algorithm and elliptic curves are combined to create CAECDH. It is essentially viewed more as a key-agreement system than an encryption method. In other words, the process of key creation and key exchange between parties is defined by CAECDH.

```
Encryption Key A: 949a6b4f221017a333fb562131c0a3259d4e608ccc09c3df9b87e13b27605b84
```

Fig. (4). Result of encryption.

```
Decrypted person1000_bacteria_2931.jpeg.jpeg successfully.
Decrypted person1000_virus_1681.jpeg.jpeg successfully.
Decrypted person1001_bacteria_2932.jpeg.jpeg successfully.
Decrypted person1002_bacteria_2933.jpeg.jpeg successfully.
Decrypted person1003_bacteria_2934.jpeg.jpeg successfully.
Decrypted person1003_virus_1685.jpeg.jpeg successfully.
Decrypted person1004_bacteria_2935.jpeg.jpeg successfully.
Decrypted person1004_virus_1686.jpeg.jpeg successfully.
Decrypted person1005_bacteria_2936.jpeg.jpeg successfully.
Decrypted person1005_virus_1688.jpeg.jpeg successfully.
Decrypted person1006_bacteria_2937.jpeg.jpeg successfully.
Decrypted person1007_bacteria_2938.jpeg.jpeg successfully.
Decrypted person1007_virus_1690.jpeg.jpeg successfully.
Decrypted person1008_bacteria_2939.jpeg.jpeg successfully.
Decrypted person1008_virus_1691.jpeg.jpeg successfully.
Decrypted person1009_virus_1694.jpeg.jpeg successfully.
Decrypted person100_virus_184.jpeg.jpeg successfully.
Decrypted person1010_bacteria_2941.jpeg.jpeg successfully.
Decrypted person1010_virus_1695.jpeg.jpeg successfully.
Decrypted person1011_bacteria_2942.jpeg.jpeg successfully.
Decrypted person1012_bacteria_2943.jpeg.jpeg successfully.
Decrypted person1014_bacteria_2945.jpeg.jpeg successfully.
Decrypted person1015_virus_1701.jpeg.jpeg successfully.
Decrypted person1015_virus_1702.jpeg.jpeg successfully.
Decrypted person1016_bacteria_2947.jpeg.jpeg successfully.
Decrypted person1016_virus_1704.jpeg.jpeg successfully.
```

Fig. (5). Result of decryption process.

3.2.2. Encryption

Medical image encryption and decryption occur at two different stages according to the CAECDH-KDF architecture. The image passes through a number of processes during encryption to provide strong security. Among other things, the image's size, row, and column are initialized. Next, every row is treated independently, and a random integer is generated to mix up the pixel locations and effectively jumble the row. After that, encryption is used to conceal the contents of this jumbled row. The column pixel coordinates are additionally altered and encrypted for further security. The encryption procedure is made much more difficult by doing an XOR operation on each pixel. To multi-step procedure, medical images are far more secure and unreadable to unwanted parties. Using encryption techniques like CAECDH-KDF, which ensure the integrity and confidentiality of vital patient data, greatly increases the security of medical images. This reduces the possibility

of unauthorized access to medical images, safeguarding patient confidentiality and complying with stringent data protection regulations. Encryption results in images containing sensitive medical information that can only be viewed and understood by authorized individuals who possess the required decryption keys, therefore safeguarding patient privacy and confidentiality as illustrated in Fig. (**4**). In the context of the medical healthcare system, ANOVA (Analysis of Variance) may be used to evaluate the effects of various interventions or treatments on patient outcomes, taking into account variables like therapy type, patient demographics, illness severity, and other pertinent aspects.

3.2.3. Decryption Process

The first step in decrypting an encrypted image is using the XOR algorithm to every pixel. The data required to generate a unique number for processing each column and row is initialized into the CAECDH-KDF's row, column and size variables. Every encrypted image's row and column are processed with the produced random number to produce the original image once decrypted. Reversing encryption is required throughout the decryption process in order to safely access protected medical image data while utilizing CAECDH-KDF to improve medical image security and the result of decryption process as shown in Fig. (**5**). The following illustrates many phases in the CAECDH-KDF decryption phase as shown in Algorithm 1.

Algorithm 1: CAECDH-KSF

Step 1: Encrypt image to load

Step 2: Execute the XOR procedure

Step 3: Set CAECDH-KDF initialization values

Step 4: Utilize each column with a random number

Step 5: Decrypt an encrypted image column-by-column

Step 6: Each row should receive a random number

Step 7: Decrypt the encrypted image row-wise

Step 8: Get image decrypted

4. RESULT AND DISCUSSION

This work uses Python 3.11 to implement a secure medical images and laptop running Windows 10 with 32 GB of RAM and an Intel (R) CPU. By evaluating and comparing the outcomes, the recommended CAECDH-KDF. The dataset gathering from (https://www.kaggle.com/datasets/paultimothymooney/chest-xray-pneumonia).

4.1. Statistical Analysis using ANOVA

In the context of the medical healthcare system, ANOVA (Analysis of Variance) may be used to evaluate the effects of various interventions or treatments on patient outcomes, taking into account variables like therapy type, patient demographics, illness severity, and other pertinent aspects as shown in Table **1**.

The effectiveness and precision of a suggested method are contrasted with those of modern techniques such as the 5D logistic map (5D-LM) model [16], double chaotic cycle shift, and Josephus problem (JP-DCCS) to show that it is effective [17]. The overall execution time (sec), entropy (encrypt image) (bits/bytes), overall encryption time (sec), overall decryption time (sec)and Throughput (Bps) estimates are defined in the outcome for the given methodology.

Table 1. Statistical analysis.

-	Source	Sum of Square	Df	Mean Square	F	P- value
0	Between groups	4401.19501	1	234.9987	987.76	87.567
1	Within groups	2193.757151	3	731.252384	0.77654	7.13456
2	total	779.0865	4	556.7878	565.875	8.98765

The time frame it takes for a computer program and process to run from beginning to end is referred to the total execution time also known as runtime. In software development and computers, it is a key performance statistic. When coding is optimized and programs are made more effective, lowering execution time is a significant goal.

Table 2. Overall execution time.

Method/Ref	Execution Time (Sec)
5D-LM [16]	0.203
JP-DCCS [17]	1.175
Proposed	0.003001

The total comparison and outcomes of execution time of the suggested system is displayed in Fig. (**6**) and Table **2**. Execution time displays the recommended methods and the duration taken to implement CAECDH-KDF protocols for bolstering security in medical image transmission as shown in Fig. (**7**). Here are the recommended approach and the runtime of consumption forecasting in the existing systems. 5D-LM gains (0.203), JP-DCCS reaches (1.175), and the advanced system reaches the specified computation time in (0.003001).

The medical image security, encryption time is the length of time required to use cryptographic techniques to convert a medical picture into a safe, unreadable format, preserving its secrecy throughout transmission and storage. It is a key variable in the healthcare industry since it directly affects how well medical image exchange and access employment. The following equation may be used to express the encryption time: Fig. (**6**) depicts the encryption time for suggested method. (Eq 10).

$$Encryption\ Time = \frac{Image\ size}{Encrypted\ speed} \quad \textbf{(10)}$$

The time needed to convert an encrypted medical image back into its initial, unencrypted form is referred to as the decryption time in the context of medical image security. To examine and evaluate medical images safely, this procedure is necessary. Decryption time (Dt) can be represented by the equation: (Eq 11).

$$Dt = D + E \quad \textbf{(11)}$$

The decryption time is represented by *Dt*. *D* stands for the decryption algorithm's time complexity. *E* Stands for the amount of time that was spent throughout the decryption procedure on any further processing or verification stages. Fig. (**7**) depicts the outcome of execution time, encryption and decryption time.

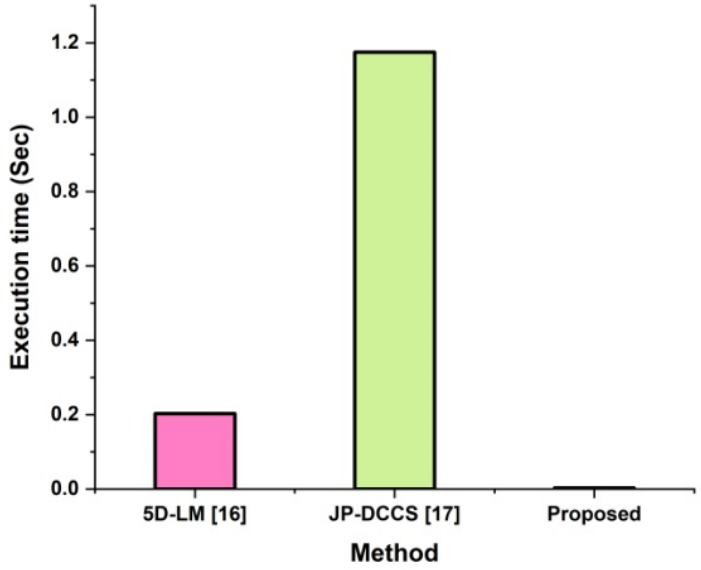

Fig. (6). Overall execution time.

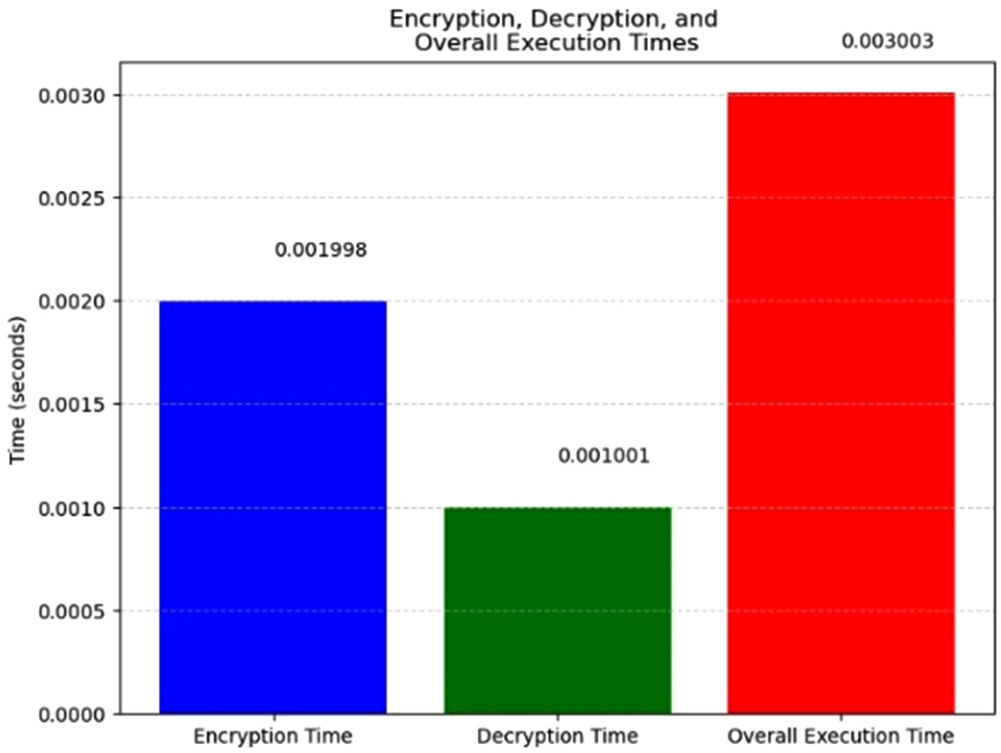

Fig. (7). Analysis of encryption, decryption and execution times.

Entropy is the most important factor in the calculation of randomness and unpredictability. According to Shannon, information entropy characterizes the level of uncertainty in every communication system. Information entropy is calculated mathematically using the following formula: (Eq 12).

$$H(m) = \sum_{j=0}^{2^p-1} S(m_j) log \frac{1}{p(m_j)} \quad \textbf{(12)}$$

The probability of *mi* is represented by $S(m_j)$, where N displays the number of bits used to describe m_j. The entropy value will be K if we consider a random source with a capacity of $2K$ symbols.

Table 3. Entropy details.

Method/Ref	Entropy (Bits/Bytes)
5D-LM [16]	7.9962
JP-DCCS [17]	7.9033
Proposed	7.997633

Fig. (**8**) and Table **3** show the suggested system's outcomes and comparison of entropy. Using CAECDH-KDF to create encryption keys ensures secrecy and integrity in the result of entropy process of medical imagine security as shown in Fig. (**9**). It highlights the proposed approach and the entropy of consumption forecasting in the existing systems. While 5D-LM gains (7.9962) and JP-DCCS obtains (7.9033), the suggested entropy is attained by the advanced system in 7.997633.

The efficiency ina system, device and process an accomplish job and transfer data with a predetermined time is called throughput. It is frequently used to assess the effectiveness and performance of systems and procedures in various industries, including networking, computing, manufacturing, and telecommunications.

The suggested system's comparison and outcomes of throughput values are as shown in Fig. (**10**) and Table **4**. Using CAECDH-KDF for enhanced security during transmission, the throughput method describes the effective flow of medical images as shown in Fig. (**11**). The approach that is recommended and the throughput of consumption forecasting in the existing systems are mentioned. While 5D-LM gains (1.232) and JP-DCCS reaches (1.170), the advanced system achieves the proposed throughput in 4.0887. It represents that the recommended action technique is more efficient than the current one.

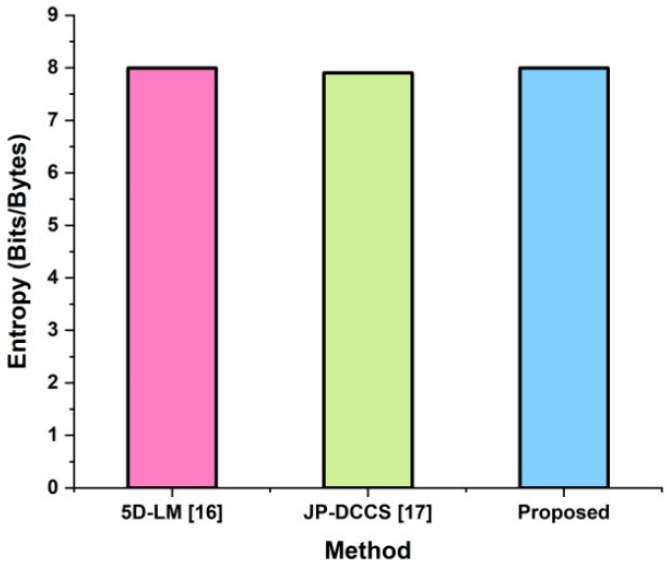

Fig. (8). Entropy.

```
Entropy (Original Image): 7.858563 bits/byte
Entropy (Encrypted Image): 7.997633 bits/byte
Entropy (Decrypted Image): 7.858563 bits/byte
```

Fig. (9). Result of entropy.

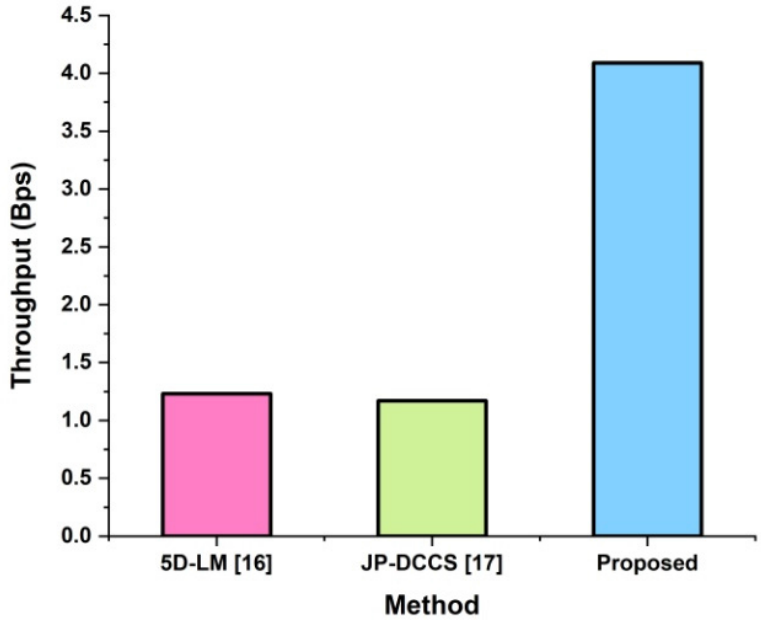

Fig. (10). Throughput.

Operation	Bps
Original Image	4.08832e+06
Encrypted Image	4.0887e+06
Decrypted Image	1.26869e+06

Fig. (11). Throughput results.

Table 4. Throughput details.

Method/Ref	Throughput (Bps)
5D-LM [16]	1.232
JP-DCCS [17]	1.170
Proposed	4.0887

CONCLUSION

In this paper, medical image security used CAECDH-KDF. Medical image security is the protection of private, reliable, and readily accessible medical images. Initially, medical images like X-rays, MRIs, and CT scans include highly sensitive and private patient information; this is an important part of managing healthcare data. Throughput (4.08), entropy (7.997633), encryption time (0.001998s), decryption time (0.001001s) and total execution time (0.003001) measurements were used to validate performance. The suggested CAECDH-KDF algorithm's effectiveness in terms of performance metrics is compared to other techniques. Medical image security procedures are necessary to safeguard patient information and privacy, but they have drawbacks. The application of medical image security encryption techniques on real-time medical images will be the main goal of future development.

AUTHORS' CONTRIBUTION

It is hereby acknowledged that all authors have accepted responsibility for the manuscript's content and consented to its submission. They have meticulously reviewed all results and unanimously approved the final version of the manuscript.

LIST OF ABBREVIATIONS

LSTM	=	Long Short-Term Memory
MLTL	=	Multi-Level Transfer Learning
DNN	=	Deep Neural Networks
IoT	=	Internet of Things
AES	=	Advanced Encryption Standard

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not applicable.

HUMAN AND ANIMAL RIGHTS

Not applicable.

CONSENT FOR PUBLICATION

Not applicable.

AVAILABILITY OF DATA AND MATERIALS

The data and supportive information is available within the article.

FUNDING

None.

CONFLICT OF INTEREST

Vinayakumar Ravi is the Associate Editorial Board Member of the journal The Open Bioinformatics Journal.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] Kiran , Parameshachari BD, Panduranga HT, Ullo S. Analysis and computation of encryption techniques to enhance security of medical images. IOP Conf Series Mater Sci Eng 2020; 925(1): 012028. http://dx.doi.org/10.1088/1757-899X/925/1/012028

[2] Sun T, Wang X, Lin D, *et al*. Medical image security authentication method based on wavelet reconstruction and fractal dimension. Int J Distrib Sens Netw 2021; 17(4) http://dx.doi.org/10.1177/15501477211014132

[3] Jain K, Aji A, Krishnan P. Medical image encryption scheme using multiple chaotic maps. Pattern Recognit Lett 2021; 152: 356-64. http://dx.doi.org/10.1016/j.patrec.2021.10.033

[4] Khare P, Srivastava VK. A secured and robust medical image watermarking approach for protecting integrity of medical images. Trans Emerg Telecommun Technol 2021; 32(2): e3918. http://dx.doi.org/10.1002/ett.3918

[5] Wang EK, Chen CM, Hassan MM, Almogren A. A deep learning based medical image segmentation technique in Internet-of-Medical-Things domain. Future Gener Comput Syst 2020; 108: 135-44. http://dx.doi.org/10.1016/j.future.2020.02.054

[6] Ghandour C, El-Shafai W, El-Rabaie S. Medical image enhancement algorithms using deep learning-based convolutional neural network. J Opt 2023; 1-11.

[7] Elhoseny M, Shankar K, Lakshmanaprabu SK, Maseleno A, Arunkumar N. RETRACTED ARTICLE: Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Comput Appl 2020; 32(15): 10979-93. http://dx.doi.org/10.1007/s00521-018-3801-x

[8] Hasan MK, Islam S, Sulaiman R, *et al*. Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access 2021; 9: 47731-42. http://dx.doi.org/10.1109/ACCESS.2021.3061710

[9] Li Z, Dong M, Wen S, Hu X, Zhou P, Zeng Z. CLU-CNNs: Object detection for medical images. Neurocomputing 2019; 350: 53-9. http://dx.doi.org/10.1016/j.neucom.2019.04.028

[10] Natarajan R, Lokesh GH, Flammini F, Premkumar A, Venkatesan VK, Gupta SK. A novel framework on security and energy enhancement based on internet of medical things for healthcare 5.0. Infrastructures 2023; 8(2): 22. http://dx.doi.org/10.3390/infrastructures8020022

[11] Dhar T, Dey N, Borra S, Sherratt RS. Challenges of deep learning in medical image analysis—improving explainability and trust. IEEE Trans Technol Soc 2023; 4(1): 68-75. http://dx.doi.org/10.1109/TTS.2023.3234203

[12] Balasamy K, Shamia D. Feature extraction-based medical image watermarking using fuzzy-based median filter. J Inst Electron Telecommun Eng 2023; 69(1): 83-91. http://dx.doi.org/10.1080/03772063.2021.1893231

[13] Aswiga RV, Shanthi AP. A multilevel transfer learning technique and LSTM framework for generating medical captions for limited CT and DBT images. J Digit Imaging 2022; 35(3): 564-80. http://dx.doi.org/10.1007/s10278-021-00567-7 PMID: 35217942

[14] Lin H, Wang C, Cui L, Sun Y, Xu C, Yu F. Brain-like initial-boosted hyperchaos and application in biomedical image encryption. IEEE Trans Industr Inform 2022; 18(12): 8839-50. http://dx.doi.org/10.1109/TII.2022.3155599

[15] Amine K, Fares K, Redouane KM, Salah E. Medical image watermarking for telemedicine application security. J Circuits Syst Comput 2022; 31(5): 2250097. http://dx.doi.org/10.1142/S0218126622500979

[16] Ahuja B, Doriya R, Salunke S, Hashmi MF, Gupta A. Advanced 5D logistic and DNA encoding for medical images. Imaging Sci J 2023; 71(2): 142-60.

http://dx.doi.org/10.1080/13682199.2023.2178097

[17] Wang R, Deng GQ, Duan XF. An image encryption scheme based on double chaotic cyclic shift and Josephus problem. J Inf Secur Appl 2021; 58: 102699.
http://dx.doi.org/10.1016/j.jisa.2020.102699