Medical Data Security in IoT Healthcare with Hybrid Encryption

Posted on November 3, 2026

View this essay online:
https://academic-master.com/medical-data-security-iot-healthcare-hybrid-encryption/

Abstract

The rapid proliferation of IoT devices in healthcare has significantly increased the vulnerability of medical data to unauthorized access, tampering, and interception. Traditional security measures often struggle to keep pace with the evolving techniques employed by cybercriminals. Moreover, efficient and secure data retrieval without compromising privacy remains a challenge. Therefore, this research introduces a pioneering secure transmission model for IoT-based healthcare systems, incorporating advanced encryption and data protection techniques. The proposed framework consists of the following stages: (a) Medical Data Encryption utilizing Optimized 3DES and RSA algorithms, (b) Region of Non-Interest Extraction employing Optimized K-Means Clustering, (c) Data Encoding and Watermark Embedding through Koblitz Method of Encoding and Hyperelliptic Curve Cryptography (HECC), (d) Image Compression via Improved Discrete Wavelet Transform (I-DWT), and (e) Data Decryption. These steps ensure the confidentiality and integrity of medical data during transmission. Additionally, the research integrates a Zero-Knowledge Data Retrieval (ZKDR) protocol with Blockchain-based Trust Scores, enhancing data privacy and authentication during retrieval processes. With high PSNR (32.45 dB) and low MSE (12.34), the proposed approach demonstrated exceptional data preservation during encryption and transmission. The method's precise extraction of non-interest regions and efficient data compression led to improved SSIM (0.987) values. These results underscore the model's effectiveness in enhancing healthcare data security within IoT environments.

Keywords: WSN, Medical Data, Cryptography, Security, Optimization, IoT, Confidentiality.

Introduction

In the rapidly advancing landscape of healthcare technology, Wireless Sensor Networks (WSN) have emerged as a pivotal area of research, particularly in the domain of IoT (Internet of Things) [1, 2]. Within this realm, Wireless Body Area Networks (WBAN) have revolutionized the healthcare industry, offering real-time transmission of vital medical data, especially in emergency situations and remote

locations [3]. WBAN, a subset of WSN, integrates wearable and implantable devices equipped with various sensors capable of monitoring crucial health parameters like blood pressure, heart rate, arrhythmia, and cerebral fluid pressure.

However, the efficient transmission of this medical data poses a significant challenge. Ensuring both the speed and security of these transmissions is paramount, given the sensitive nature of the data being relayed [4-6]. This research article delves into this complex terrain, aiming to tackle the multifaceted issues of security, speed, and transmission load within the context of IoT healthcare [7].

The fundamental problem revolves around the WBAN, where medical devices must transmit data seamlessly in real-time. Despite its transformative potential, WBAN is plagued by security vulnerabilities [8, 9]. The challenge lies in establishing a robust mechanism for secure data transmission and user authentication within the confines of resource-constrained environments [10]. These constraints encompass limited energy reserves and spatial capacities, making the implementation of high-level security protocols a daunting task. Consequently, devising solutions that enhance security without compromising these constraints forms the core problem addressed in this research [11-14].

The motivation driving this research is rooted in the critical need to safeguard the confidentiality and integrity of patients' diagnostic information communicated via IoT devices [15, 16]. Patient data, being of a highly sensitive nature, demands not only encryption but also innovative techniques to conceal it effectively. Steganographic approaches, which involve hiding data within seemingly innocuous images, present a promising avenue [17]. Additionally, encryption cryptography plays a pivotal role in encoding messages, rendering them indecipherable to unauthorized entities [18].

Steganography, by covertly embedding information within images, ensures discreet data transmission. Simultaneously, encryption cryptography adds an extra layer of security, making the transmitted data indecipherable to malicious entities. This integration is further augmented by discrete wavelet transform, a technique characterized by spatial localization, frequency spread, and multi-resolution features akin to the human visual system [19, 20].

By combining steganographic methods and advanced cryptographic algorithms, the proposed model seeks to fortify the security of medical data transmission in IoT healthcare environments. Furthermore, the research endeavors to enhance the trustworthiness of access control mechanisms, ensuring that only authorized users can decipher and utilize the transmitted medical information. Through these efforts, this paper aims to contribute significantly in IoT healthcare, paving the way for secure, efficient, and confidential transmission of vital medical data in resource-constrained environments. The contributions made in this paper are as follows:

The IOA-based RSA-3DES algorithm significantly enhances the security of healthcare data. By leveraging I-AO, the algorithm optimally selects encryption keys for both RSA and 3DES, ensuring robust protection against unauthorized access and data breaches. Also, the optimal selection of encryption keys leads to more efficient resource utilization. The algorithm minimizes computational overhead while maintaining a high level of security.

The Koblitz method of encoding, coupled with the utilization of hyperelliptic curves, forms a robust security framework. By converting cipher text into points on a complex mathematical curve, the system ensures that sensitive medical data is secured from unauthorized access and manipulation, even in the case of potential attacks during transmission. This intricate combination of techniques enhances the overall security, making it highly resilient against various cyber threats.

I-DWT technique optimizes the compression process by effectively transforming medical images into frequency-domain representations. This enhancement significantly reduces the data size while preserving essential image details, ensuring efficient storage and transmission of medical data.

The integration of Zero-Knowledge Data Retrieval with Blockchain-based Trust Scores establishes a robust and privacy-preserving protocol for accessing medical data. This innovative approach ensures secure, authenticated, and efficient data retrieval, promoting trust in the healthcare ecosystem while ensuring patients' confidentiality.

The rest of the paper is organized as follows: section 2 provides the literature review, section 3 gives the proposed I-AO based hybrid encryption and embedding scheme for securing medical data, section 4 provides the experimental results and analysis, and finally, section 6 gives the conclusions of the paper.

Literature Review

In the study by Shabbir et al. [21], a novel health information security model, termed SecureHI, was introduced for Mobile Cloud Computing (MCC) environments. They employed Modular Encryption Standard (MES) to ensure robust security measures for healthcare data. MES encompasses a multifaceted approach, incorporating various encryption techniques such as key generation, permutation, substitution, and addition. The model adopts a requirement-centric approach, tailoring encryption techniques based on the sensitivity levels of Health Information. This customized encryption enhances data security and confidentiality. However, it does not address the challenge of securely handling encrypted data sent to cloud servers for Deep Neural Network (DNN) model training, potentially risking exposure of sensitive health information.

Hasan et al. [22] proposed lightweight encryption technique for medical images while mitigating challenges related to data size limitations and transmission over open channels. The method involves segmenting the image into sub-blocks and employing a carefully designed encryption process involving binary value calculations, key application, transformation table utilization, XOR operations, and circular shift operations. The encryption scheme achieves high entropy values, indicating strong security and resistance against brute force attacks. However, a potential limitation lies in the need for rigorous testing across diverse medical imaging scenarios to confirm its robustness against various security threats and performance consistency.

Geetha et al. [23] proposed Pigeon Inspired Optimization with Encryption-based Secure Medical Image Management (PIOE-SMIM) technique addresses the challenge of securing medical images in open channels. The method involves secret share creation (SSC) and encryption, where medical images are converted into 12 shares using SSC and encrypted using elliptic curve cryptography (ECC). The PIO technique optimizes key generation for ECC, maximizing Peak Signal-to-Noise Ratio (PSNR). But, the computational complexity of PIO may pose challenges in real-time applications, requiring careful optimization for practical implementations.

Selvi et al. [24] integrated modified Salp Swarm Algorithm (SSA) with Chaotic Coupled Map Lattices (CML) for secure encryption and compression of medical images during data transmission. The algorithm utilizes CML for encryption and compression, generating encrypted images using modified SSA and Whale Optimization Algorithm (WOA) for enhanced efficiency. Chaotic maps are employed for image encryption, ensuring security, and the technique is resistant to various attacks. While offering efficient encryption and compression, the method may face challenges in handling complex medical image data, necessitating further validation and optimization.

Ahmad et al. [25] introduced MID-Crypt algorithm for securing medical images during transmission between laboratories and doctors' accounts. Utilizing a combination of Elliptic-curve Diffie–Hellman (ECDH) for image masking and updatable Advanced Encryption Standard (AES) for image encryption, MID-Crypt ensures high-security standards and effectively conceals sensitive medical image features. The system incorporates a robust key management system, digital signature authentication, integrity verification through Merkle tree, and efficient decryption processes, ensuring data confidentiality and authenticity. However, the effectiveness of MID-Crypt heavily relies on the proper management of encryption keys. If not managed securely, the compromise of encryption keys could lead to data breaches.

Khare and Srivastava [26] presented a novel approach for telemedicine applications, integrating homomorphic transform (HT), redundant discrete wavelet transform (RDWT), and singular value

decomposition (SVD) to enhance robustness and security. By embedding the watermark in the reflectance component using stable singular values and employing RDWT, the method ensures excellent immunity under various attacks. The use of 2-D chaotic Arnold transform (AT) adds an extra layer of security, encrypting the watermarked image and safeguarding sensitive patient information. The technique prioritizes both robustness and imperceptibility, aiming to minimize the potential loss of essential diagnostic details. The proposed method stands out for its utilization of advanced transforms and encryption techniques, enhancing the security and integrity of embedded medical information. However, the computational complexity and the choice of optimal parameters could be potential challenges, requiring careful consideration for practical implementation

A content-aware DNA computing system was proposed by Wu et al. [27] to enhance the security of medical images, ensuring privacy and promoting secure healthcare environments. The system employed DNA encoding and content-aware permutation & diffusion modules, enhancing security by introducing random mechanisms and utilizing semantical information for encryption. The DNA encoding was performed using various rules, adding diversity and complexity to the encryption process. The content-aware permutation & diffusion module capitalized on DNA operations, enabling reversible, content-related encryption without additional data transmission. The system exhibited high speed, parallelism, minimal storage requirements, and real-time performance, ensuring robustness against various attacks during wireless data transmission. However, further evaluation was needed to assess its scalability and efficiency in large-scale healthcare systems.

Proposed I-AO based Hybrid Encryption and Embedding Scheme

In this research, a state-of-the-art secure transmission model has been developed for IoT-based healthcare systems, where the protection of clinical data is of paramount importance. The model, illustrated in Figure 1, operates between sender and receiver components. At the sender end, six pivotal phases are executed: firstly, medical data is encrypted to ensure its secure transformation. Subsequently, non-critical areas within medical images, termed the Region of Non-Interest, are extracted, optimizing data processing. The encrypted data is then encoded, enhancing its security, and a unique watermark is embedded for authentication. The medical images are compressed intelligently, maintaining essential details, making them efficient for transmission and storage. Finally, at the receiver end, the transmitted data is decrypted, ensuring that sensitive medical information is preserved, authenticated, and efficiently transmitted within the IoT-based healthcare framework.

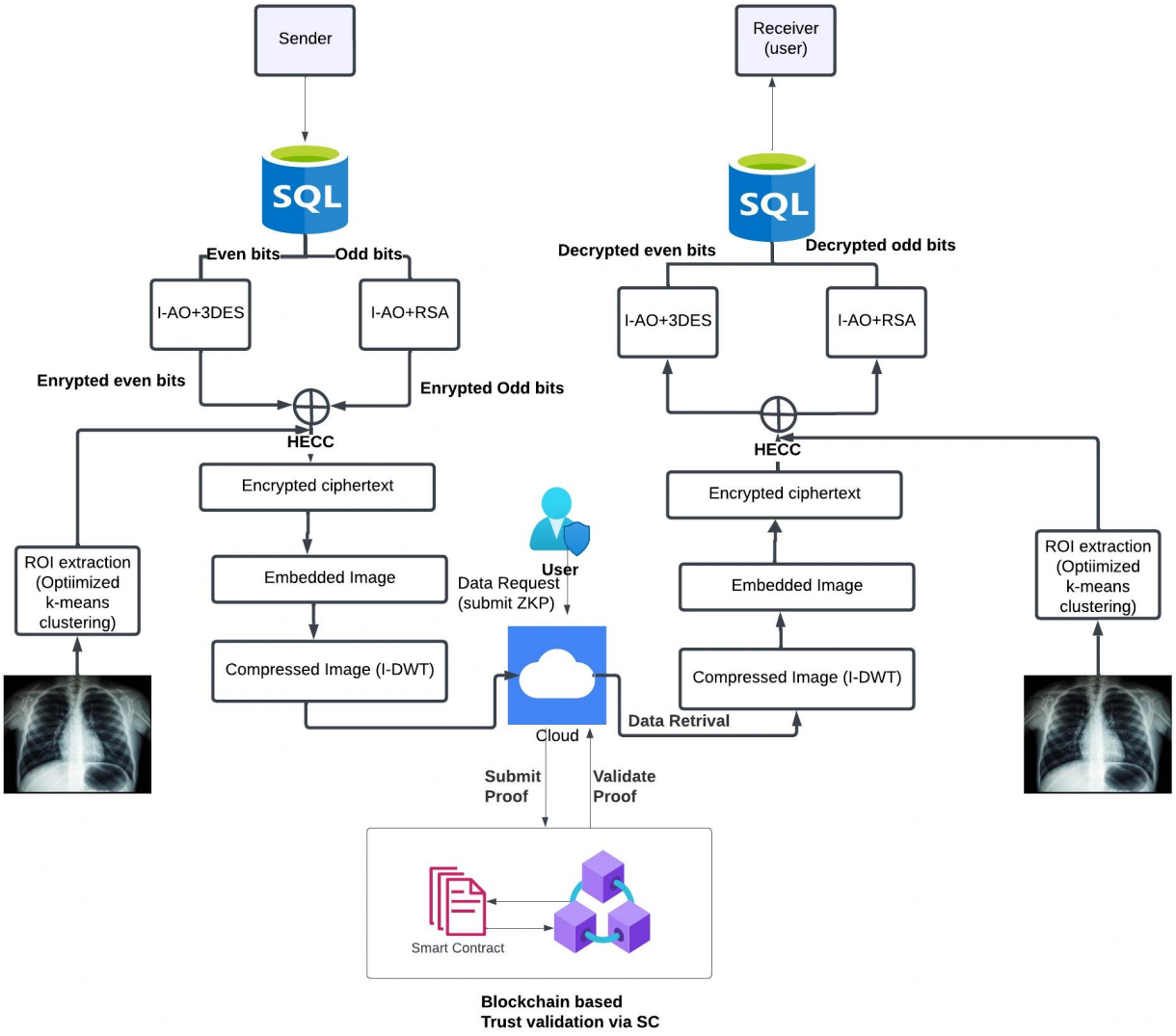


Figure 1: Architecture of the proposed Encryption and Embedding Scheme

Medical data encryption

Medical data encryption involves converting patient records, diagnostic images, and other healthcare information into unreadable code, which can only be accessed by authorized personnel with the appropriate decryption keys. This process plays a vital role in safeguarding patient data from unauthorized access, ensuring secure transmission between healthcare providers, and building trust in healthcare systems.

In the encryption process, the medical data are transformed into binary values, which are further

categorized into odd and even positions- B_{odd} and B_{even}, respectively. The odd positions are encrypted using the I-AO+RSA algorithm, and the even data-bits are encrypted through the I-AO+3DES algorithm. The improved meta-heuristic model, known as the Improved Aquila Optimizer (I-AO) model, is used for key selection in both 3DES and RSA algorithm.

3DES Algorithm

The Triple Data Encryption Standard (3DES) algorithm is a symmetric encryption algorithm, which means it uses the same key for both encryption and decryption. The working principle of 3DES involves applying the Data Encryption Standard (DES) algorithm three times in succession with different keys. 3DES provides a higher level of security than the original DES due to the triple application of the encryption algorithm.

3DES uses three 56-bit keys, making a total of 168 bits. These keys are often referred to as $K1$, $K2$, and $K3$.

Encryption:

Initial Permutation (IP): The 64-bit plaintext block is permuted according to a fixed permutation table.

First Encryption (DES): The permuted block is encrypted using $K1$.

Decryption: The result from the first encryption is decrypted using $K2$.

Second Encryption (DES): The decrypted block is encrypted again using $K3$.

Decryption:

Initial Permutation: The final encrypted block is permuted using the inverse of the initial permutation.

Decryption: The permuted block is decrypted using $K3$.

Encryption: The result from the previous step is encrypted using $K2$.

Final Decryption (DES): The decrypted block is encrypted again using K1.

RSA Algorithm

The RSA (Rivest-Shamir-Adleman) algorithm is a widely used asymmetric encryption algorithm that involves the use of a pair of public (e,n) and private key d for encryption and decryption.

where e is the public exponent and n is the modulus.

Encryption:

Convert the plaintext message M into an integer m such that $0 < m < n$.

Compute the ciphertext C using the public key: $C \equiv m^e \mathrm{mod} n$

Decryption:

Retrieve the ciphertext C.

Compute the original message m using the private key: $m \equiv C^d \mathrm{mod} n$.

Convert M back to original plaintext M.

Optimal Key Selection Using the Improved Aquila Optimizer

While Aquila Optimization (AO) [28] has demonstrated robust performance, its effectiveness can diminish when dealing with increasingly complex real-world problems. This decline in suitability could lead to sub-optimal outcomes or convergence on local optima. This limitation arises from the use of the Levy Flight Distribution in the second searching step of AO, which confines the search space and might trap solutions in local optima. Additionally, in the third searching step, two parameters determining the exploitation phase are kept constant, resulting in weak local exploitation. To address these shortcomings, an enhanced version called Improved Aquila Optimization (I-AO) is introduced. I-AO incorporates a function known as the ” Search Space Modulator (SSM),” which decreases iteratively. This SSM mitigates issues related to the Levy Flight Distribution by expanding Aquila’s search range, enhance both exploration and exploitation phases, thereby improving its overall performance.

SSM governs Aquila’s search range, causing Aquila to narrow down its movement swiftly concerning the current epoch. Consequently, the search range becomes significantly narrower compared to the previous approach, leading to a much quicker discovery of optimal solutions. The SSM can be mathematically represented as follows:

$$\mathrm{SSM}(I) = 2 \times \exp(1 - (\frac{I \times (I \times 0.1)}{I_{\max}})) \times D_{\mathrm{CF}} \qquad (1)$$

$$D_{CF} = \begin{cases} 1 & \text{if } rand < 0.5 \\ -1 & \text{else} \end{cases} \quad (2)$$

where I_{max} represents the maximum iteration, I signifies the current iteration, $rand$ denotes a random number ranging from 0 to 1, while D_{CF} stands for the direction control factor. This factor plays a pivotal role in steering Aquila's flight direction. To improve search accuracy, SSM function is designed to achieve faster convergence by restraining Aquila's movement, ultimately reducing optimization latency.

Step 1: Initialization in I-AO (Keys Initialization)

Initialize the keys as a solution vector as given in Eqn. (3).

$$S_V = \{ky_1, ky_2, \ldots, ky_n\} \quad (3)$$

This initialization sets the foundation for the Aquila Optimization process.

Step 2: Fitness Evaluation in I-AO

The fitness evaluation equation for optimizing 3DES and RSA key pairs is combination of factors that represent the desired characteristics of the keys.

$$\text{Fit} = w_1 \times K_L + w_2 \times P + w_3 \times C_C \quad (4)$$

where w_1, w_2, and w_3 are weighting factors that determine the relative importance of each criterion. K_L, P, and C_C denotes key length, primality, and computational complexity.

Key Length: The length of the key in bits. Longer keys generally offer higher security.

Primality: A measure of how well the selected prime numbers satisfy primality tests.

Computational Complexity: The time required to generate the key pair. This is measured in terms of CPU cycles or time taken for key generation.

Step 3: Update new key

After evaluating the fitness of the current solutions, the Aquila Optimization algorithm proceeds to update the keys iteratively. Apply Aquila Optimization techniques, such as the Vertical Dive Attack, Short Glide, Search Around Prey and Attack, and Walk and Grab Attack, to explore the neighborhood of the best-performing solution. These techniques guide the algorithm in refining the keys to further improve the security. Update the keys in the solution vector based on the exploration results obtained

from Aquila Optimization steps. Through the incorporation of the SSM function, the proposed I-AO algorithm comprises four stages, outlined as follows:

(i) Vertical Dive Attack

Aquila initiates its search by identifying the target region and selecting the optimal hunting location through a high-altitude descent, a tactic commonly referred to as the vertical dive attack. This is mathematically represented as given in Eqn. (5).

$$T_1(I+1) = T_{\text{best}}(I) \times (1 - \frac{I}{I_{\max}}) + (T_{\text{mean}}(I) - T_{\text{best}}(I) \times \text{rand}) \quad (5)$$

where $T_{best}(I)$ signifies the best solution, $T_{mean}(I)$ signifies the mean value of the present solution, providing a comprehensive understanding of the evolving solutions throughout the iterative process. The term $(1 - \frac{I}{I_{\max}})$ is employed to regulate the exploration process within the search space.

(ii) Short Glide Attack

In the second step, Aquila conducts an extensive exploration of the target solution space. This exploration involves testing diverse speeds and directions before engaging the target. This phase is crucial for refining the search process and is expressed using Eqn. (6).

$$\text{GT}_2(I+1) = T_R(I) + \text{SSM}(I) \times (T_{\text{best}}(I) - T(I)) \times \text{rand} \times (v - u) + (T_{\text{mean}}(I) - T_{\text{best}}(I)) \quad (6)$$

where $\mathcal{U}$ and $\mathcal{V}$ denote the coordinates of the points shaping the spiral patterns in the ongoing search process. $SSM(I)$ represents the search space modulator as defined in Eqn. (1) and $T_R(I)$ denotes the random set of solution. Notably, we opted for SSM over the Levy Flight Distribution to overcome the challenge of getting trapped in local optima.

(iii) Prey search and attack

In the subsequent step, Aquila pinpoints the precise location of the prey following the GT_2 exploration. The algorithm conducts a thorough search around the prey and, employing a pseudo attack. This strategy is pivotal for refining the hunting process and ensuring an accurate targeting, thus enhancing the overall efficiency of the algorithm.

$$\text{GT}_3(I+1) = \text{LB} + \text{rand} \times (\text{UB} - \text{LB}) + \text{rand} \times (T_R(I) - T_{\text{best}}(I)) \times \text{SSM}(I) \times (1 - \frac{I}{I_{\max}}) \quad (7)$$

where $T_R(I)$ represents a set of random solutions, LB and UB represents the lower and upper bound respectively.

(iv) Walk and Grab Attack

In the final stage, Aquila initiates an attack from above, taking cues from the prey's movements. This searching step is defined using Eqn. (8).

$$GT_4(I+1) = F_Q \times T_{best}(I) - (H_1 \times T(I) \times \text{rand}) - H_2 \times \text{lev(DM)} \quad (8)$$

$$F_Q = I^{\frac{2 \times \text{rand} - 1}{(1 - I_{max})^2}} \quad (9)$$

$$H_1 = 2 \times \text{rand} - 1 \quad (10)$$

$$H_2 = 2 \times (1 - \frac{I}{I_{max}}) \quad (11)$$

where $lev(DM)$ represents the Levy Distribution within the D-dimensional space. F_Q stands for the quality function employed to maintain a balanced search. H_1 encompasses the various movements Aquila makes during prey hunting, while H_2 denotes the flight slope of Aquila's pursuit. The flowchart of the proposed I-AO algorithm is depicted in Fig. 2.

Step 4: Termination criteria

Repeat the optimisation process for a predefined number of iterations or until a convergence criterion is met. During each iteration, the algorithm dynamically refines the keys. By iteratively updating the keys using Aquila Optimization techniques, the algorithm converges towards an optimal key configuration. The flowchart for the I-AO algorithm is depicted in Fig. 2

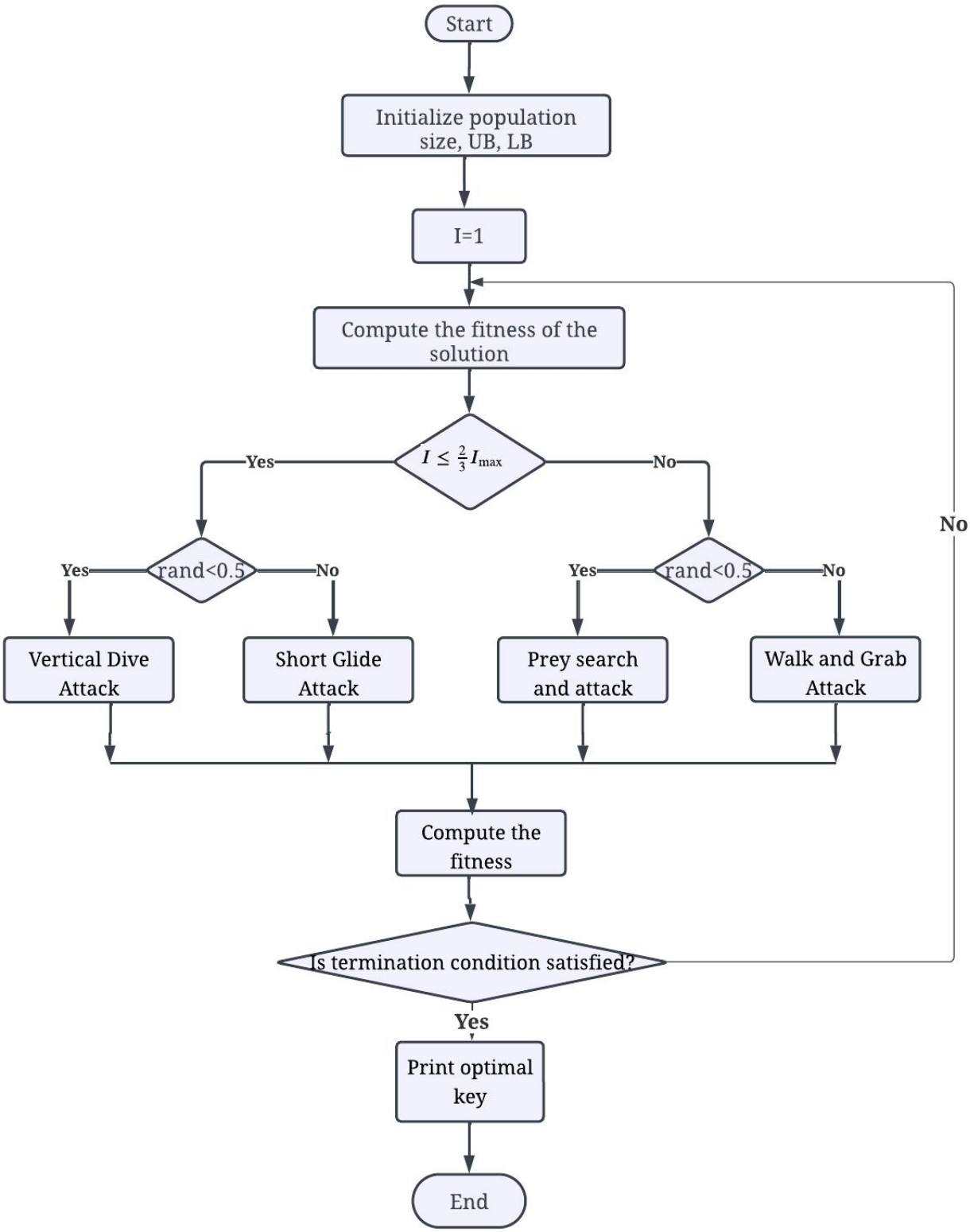

Start
Initialize population size, UB, LB
I=1
Compute the fitness of the solution
$I \leq \frac{2}{3} I_{max}$
Yes
No
rand<0.5
Yes
No
rand<0.5
Yes
No
Vertical Dive Attack
Short Glide Attack
Prey search and attack
Walk and Grab Attack
Compute the fitness
Is termination condition satisfied?
No
Yes
Print optimal key
End

Figure 2: Flowchart of the I-AO algorithm

The ciphertext obtained from optimized 3DES and optimized RSA are combined through XOR operation to form the binary matrix, which represents the encrypted data of the input medical information.

Algorithm 1: Proposed I-AO based Hybrid Encryption Algorithm
Input: Medical data D Output: Encrypted data E Convert medical data D into binary values, denoted as $B(D)$. Separate binary values into odd positions B_{odd} and B_{even}. Apply the I-AO algorithm for key selection in RSA encryption. Encrypt odd positions E_{odd} using RSA algorithm with the selected key. $E_{\text{odd}} = \text{RSA}_{\text{Encrypt}}(B_{\text{odd}}, I - \text{AO}_{\text{RSA}_{\text{key}}})$ Apply the Improved Aquila Optimizer (I-AO) algorithm for key selection in 3DES encryption. Encrypt even positions E_{even} using 3DES algorithm with the selected key. $E_{\text{even}} = 3\text{DES}_{\text{Encrypt}}(B_{\text{even}}, I - \text{AO}_3\text{DES}_{\text{key}})$. Concatenate the encrypted odd and even positions to obtain the final encrypted data E. $E = E_{odd} + E_{even}$

Region of noninterest extraction

Medical images often contain crucial diagnostic information. ROI extraction ensures that embedded data does not interfere with the diagnostic content of the image. By carefully selecting non-diagnostic regions, the medical context and integrity of the image are preserved. To achieve this, Region of non-interest extraction (ROI) regions in the medical images are identified using the optimized K-means clustering approach.

Let's represent the received medical data as a text sequence, denoted as $D = [d_1, d_2, \ldots, d_n]$. The medical image can be represented as a matrix I_M with pixel values, where each pixel is represented as $I_M(x, y)$ for coordinates (x, y).

Consider each pixel of the medical image as a feature vector $F_i = [I_M(x_i, y_i)]$ for i^{th} pixel. K-Means clustering is applied to the feature vectors F_i to group pixels into clusters. The clusters represent different regions in the image. The objective function is given in Eqn. (12).

$$J = \sum_{i=1}^{K} \sum_{x \in c_i} \|x - \mu_i\|^2 \qquad (12)$$

where K is the number of clusters, c_i represents i^{th}cluster, x signifies a data point, μ_i denotes the

centroid of the i^{th}cluster. The optimal number of clusters K are chosen by the proposed I-AO algorithm.

Algorithm 2: I-AO Optimized K-Means Clustering for ROI extraction
Input: – Image Pixel Feature Vectors F_i – Number of Clusters K – Maximum Number of Iterations – Convergence Criteria epsilon – I-AO Parameters (such as population size, iterations, etc.) Output: – Cluster Assignments C_i for ROI extraction. 1. Initialize the I-AO algorithm with appropriate parameters. 2. Randomly initialize K centroids for clusters from F_i. 3. Perform I-AO Optimized K-Means Clustering iterations until convergence: a. Apply I-AO to optimize the cluster centroids: – Evaluate fitness function. – Update centroids using I-AO mechanism. b. Assign each feature vector F_i to the nearest centroid to form clusters. c. Calculate the total intra-cluster distance. d. Check for convergence. e. Repeat until max_iter or convergence is achieved. 4. Output the final cluster assignments C_i for ROI extraction.

Data encoding and watermark embedding

Post-clustering, the clusters or regions where the medical data is null (no image details) is identified. These clusters are denoted as C_{null}. The encrypted data E is then embedded into the null clusters C_{null} to avoid disruption of existing image information.

(i) Koblitz Method of Encoding:

The Koblitz method of encoding plays a pivotal role in ensuring the confidentiality and integrity of transmitted data. It involves converting the cipher text, denoted as E, into points on a specific mathematical curve. This conversion mechanism serves as a cryptographic technique, preventing potential attackers from deciphering the original data merely by observing the encoded points. The method creates a layer of abstraction, making it exceedingly challenging for unauthorized entities to guess or intercept the transmitted information.

(ii) Integration with Hyperelliptic Curves (HECC):

To implement the Koblitz method, hyperelliptic curves are utilized. These curves serve as the carrier for the points generated through the Koblitz encoding process. The curves provide a secure foundation, ensuring that the encoded data remains confidential and tamper-proof during transmission.

Algorithm 3: Secure Data Transmission using Koblitz Encoding and Hyperelliptic Curves (Koblitz-HECC)
Input: Cipher text E Output: Encrypted data points on hyperelliptic curves 1. Koblitz Encoding (Step 1): Initialize a prime field F_p and and elliptic curve EL_{curve} over F_p. Convert the cipher text E into a binary representation. Apply the Koblitz encoding method to transform the binary data into points on the elliptic curve EL_{curve}. Let P_E represent the resulting points. 2. Hyperelliptic Curve Integration (Step 2): Select a suitable hyperelliptic curve $HECC$ over F_p. Encode the points P_E onto the hyperelliptic curve $HECC$. Let P_{HECC}represent the encoded points. 3. Data Transmission (Step 3): Transmit the points P_{HECC} securely to the intended recipient over the communication channel. 4.Decoding at the Receiver's End (Optional): If required, the recipient can decode the received points P_{HECC}back to the original elliptic curve EL_{curve}. Apply the inverse Koblitz encoding method to convert the points back into binary data. Obtain the decrypted cipher text E from the binary data.

Image compression

The secret data is first encoded into HECC points using the Koblitz method, providing secure carriers for the information. The embedded image, containing the HECC points representing the secret data, undergoes a five-level Discrete Wavelet Transform (DWT). DWT decomposes the image into different frequency bands, separating high-frequency components (detail information, like edges) from low-frequency components (overall structures and smooth areas). Huffman coding, a lossless data compression algorithm, is applied to the DWT coefficients.

Huffman coding assigns variable-length codes to different symbols (in this case, DWT coefficients) based on their frequencies of occurrence. This process effectively compresses the data. Huffman coding is particularly efficient for reducing redundancy in the data, ensuring that the compressed image retains all the information of the original image without loss. This process ensures that both the

integrity of the medical image and the confidentiality of the embedded secret data are maintained during storage and transmission. The image, now represented as DWT coefficients and compressed using Huffman coding, is specified for five-level decomposition. Higher frequency regions, capturing detailed edge information, are identified. Lower frequency regions are further divided into higher and lower frequency components. This hierarchical decomposition allows for efficient storage and transmission of the image data, preserving both the embedded secret data and the structural details of the medical image.

Data Retrieval

After the compressed image is obtained, it is securely stored in a cloud-based data storage solution. This step ensures data availability and redundancy while maintaining security measures to protect against unauthorized access.

The Zero-Knowledge Data Retrieval (ZKDR) protocol, coupled with Blockchain-based Trust Scores, establishes a secure framework for accessing sensitive medical data without compromising confidentiality. ZKDR ensures that authorized users can retrieve specific medical information without revealing the entire dataset, safeguarding patients' privacy. The integration of Blockchain technology enhances the protocol by providing a transparent, immutable record of trustworthiness through Trust Scores, ensuring secure and authenticated data retrieval processes. The Protocol Steps are as follows:

(i) User Authentication and Authorization:

Users authenticate themselves via secure credentials. Blockchain-based identity verification establishes trustworthiness and assigns a Trust Score to each user.

(ii) Request Generation:

Authorized users generate a specific data request without revealing the full dataset. The request includes query parameters without disclosing sensitive information.

(iii) Zero-Knowledge Proof Generation:

Users create a Zero-Knowledge Proof (ZKP) demonstrating their eligibility for the requested data without revealing their identity or the data specifics. ZKP confirms that the request meets predefined criteria without disclosing the criteria themselves.

(iv) Smart Contract Validation:

The request and ZKP are submitted to a smart contract on the Blockchain. Smart contract validates the ZKP and checks the user's Trust Score against the required threshold.

(v) Data Retrieval:

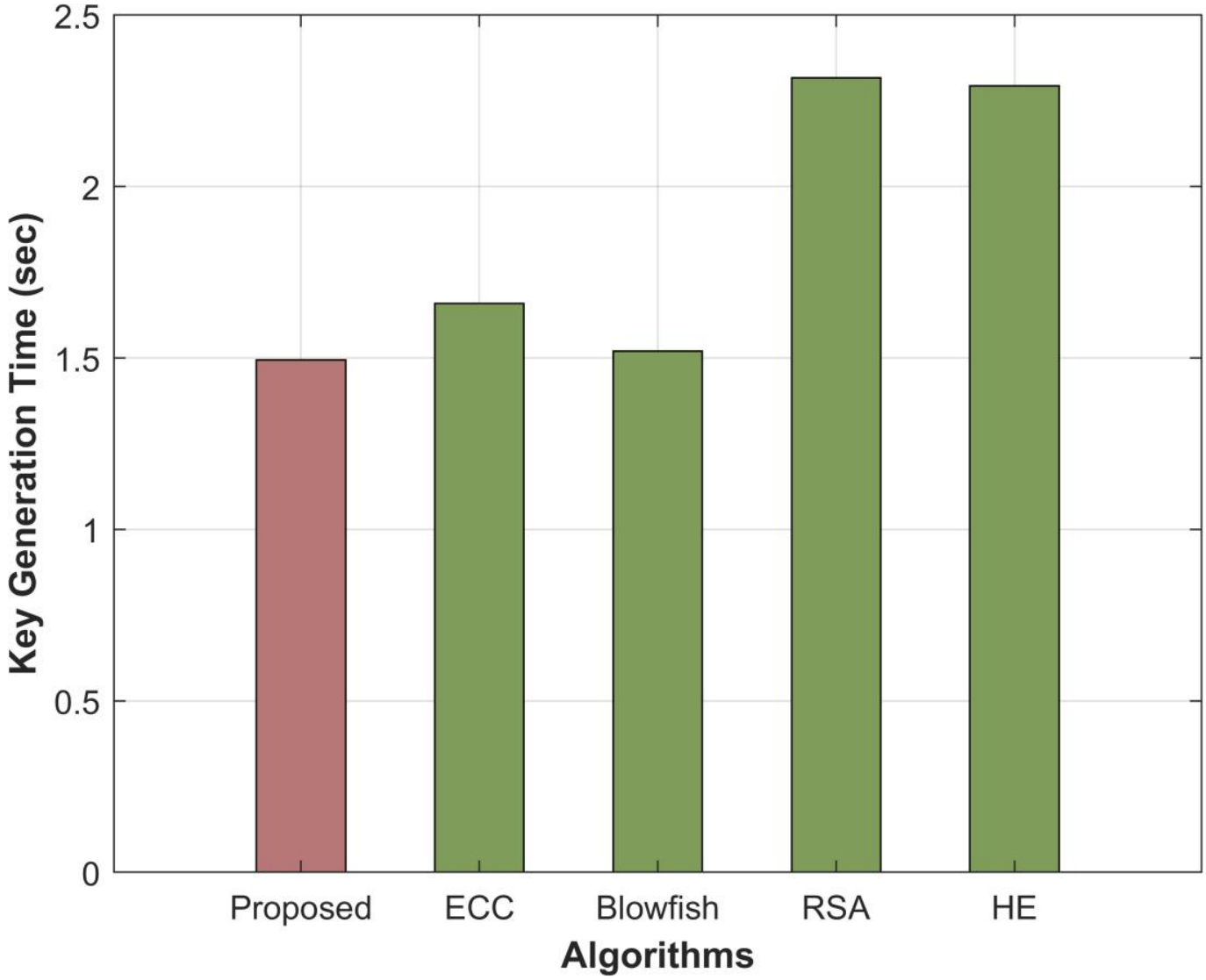
Upon successful validation, the authorized data is retrieved from the secure medical database. Retrieved data is encrypted and sent to the user, ensuring end-to-end confidentiality.

(vi) Trust Score Update:

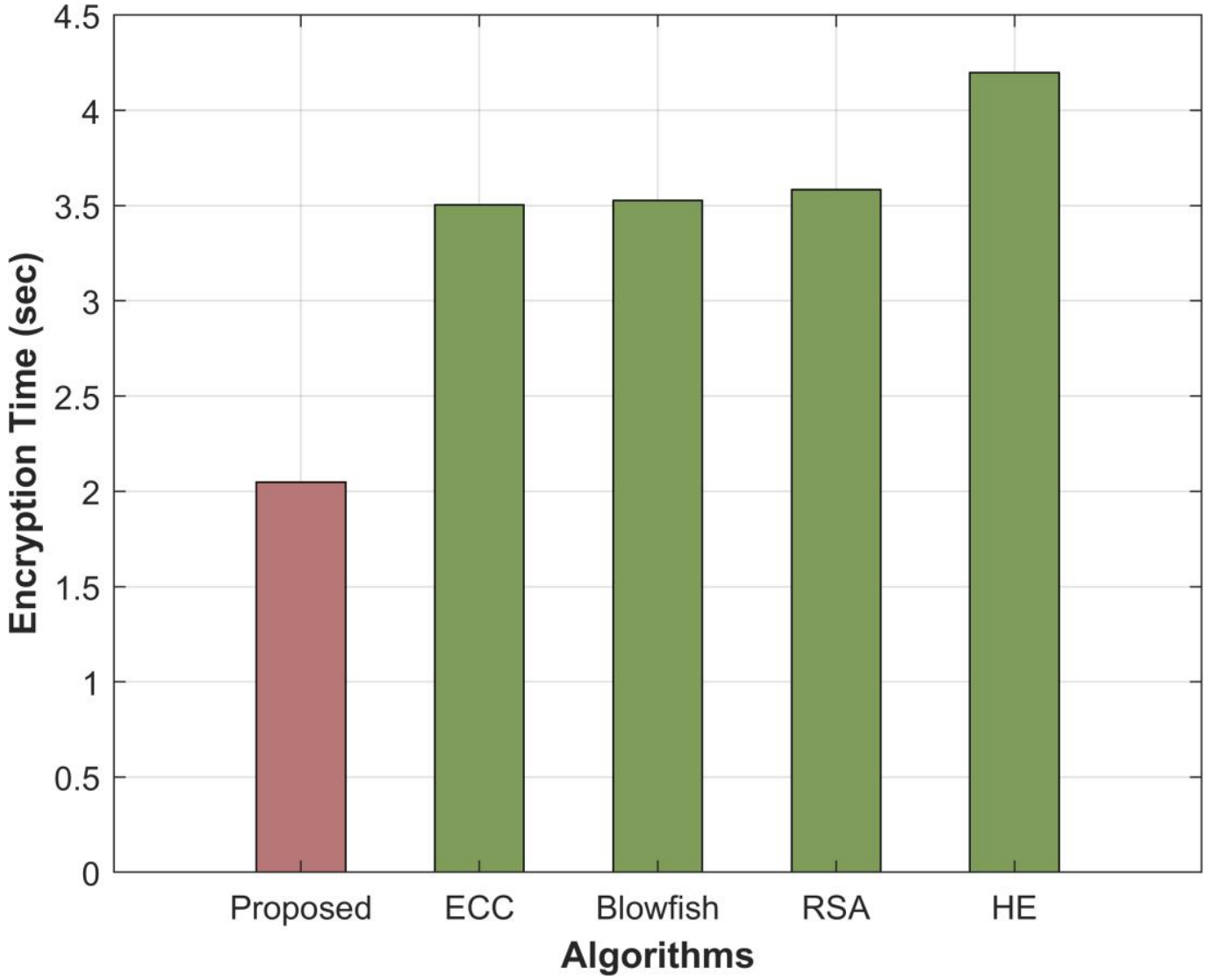
After successful data retrieval, the user's Trust Score is updated based on their adherence to protocol guidelines. Trust Scores are stored on the Blockchain, providing a transparent record of user behavior and reliability.

Experimental Results and Analysis

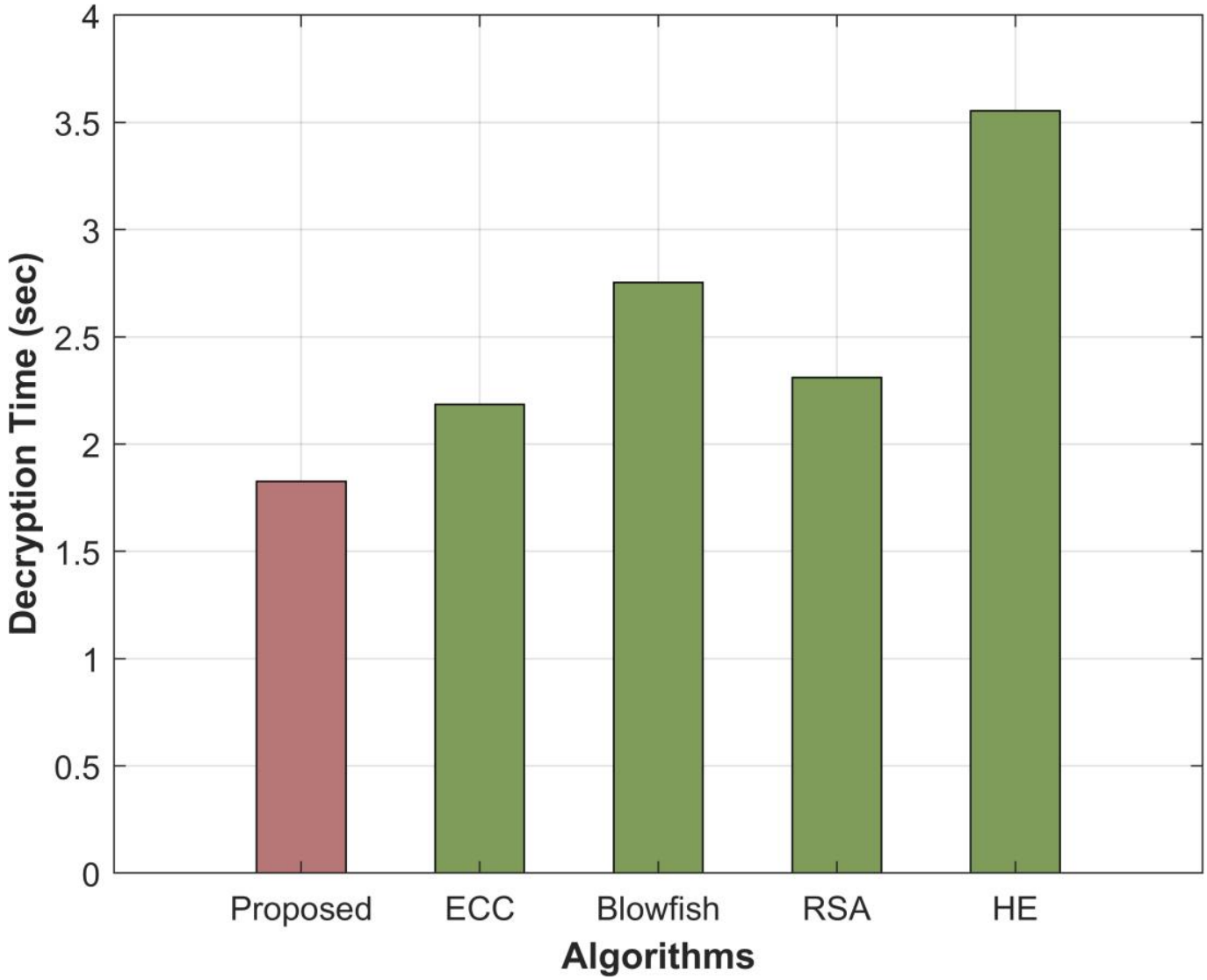
The proposed image algorithm is implemented using MATLAB R2010b on a personal computer equipped with an Intel Core™ i3 processor running at 2.27 GHz operating on Windows 10, and 8 GB RAM. The evaluations are made in terms of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER), Structural Similarity (SSIM), Structural Content (SC), and Correlation.


2.5
2
1.5
1
0.5
0
Key Generation Time (sec)
Proposed
ECC
Blowfish
RSA
HE
Algorithms

(a)


4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Encryption Time (sec)
Proposed
ECC
Blowfish
RSA
HE
Algorithms

(b)



(c)

Figure 3: Performance analysis (a) Key generation (b) Encryption time (c) Decryption time

Fig. 3 illustrates the performance analysis of the proposed method, focusing on key generation, encryption time, and decryption time. In Fig. 4 (a), the efficiency of key generation is showcased, indicating the rapid and precise key generation process of the I-AO integrated hybrid RSA and 3DES algorithm. Fig. 4 (b) and (c) present the encryption and decryption times, respectively. In terms of key generation, the approach yields a remarkable reduction in processing time, with values averaging at 1.494 sec, outperforming traditional methods such as RSA (2.317 sec), HE (2.294 sec), Blowfish (2.754 sec) and ECC (1.659 sec). The proposed method also demonstrates remarkable speed and efficiency in both encryption and decryption processes, outperforming existing methods such as Honey Encryption (HE) [29], RSA [30], Blowfish [31], and ECC [32]. This enhancement in encryption speed ensures rapid and secure data transmission.

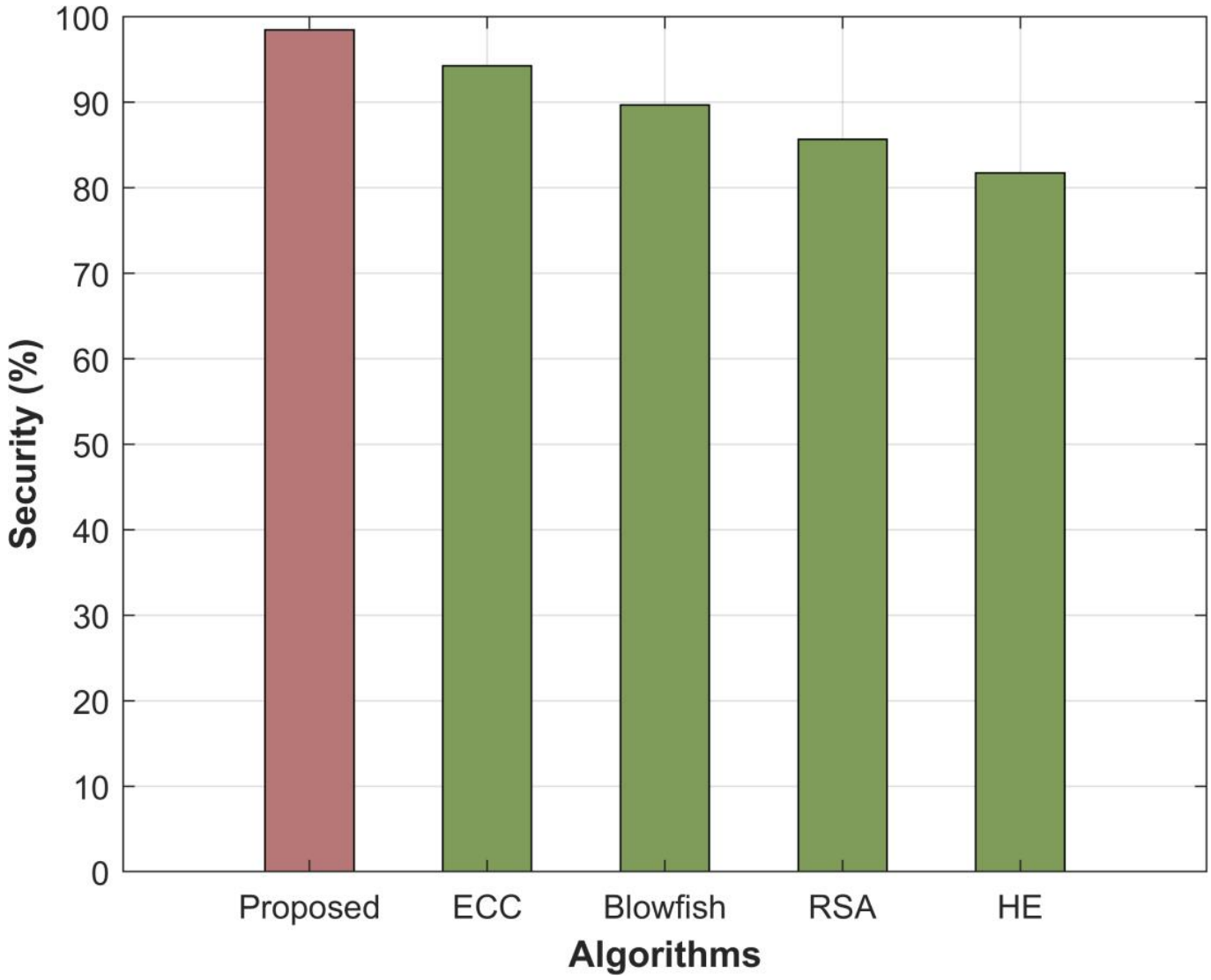


Figure 4: Security Analysis

The performance analysis for security metrics provided in Fig. 4 demonstrates the effectiveness of various encryption methods in ensuring data security. The proposed method achieved an outstanding security rate of 98.503%, indicating its robustness and ability to protect sensitive information effectively. In comparison, ECC exhibited a security rate of 94.281%, highlighting its strong security capabilities. Blowfish provided a security rate of 89.703%, indicating a good level of protection for encrypted data. RSA, with a security rate of 85.69%, demonstrated reliable security measures. HE, although secure, had a slightly lower security rate of 81.751% compared to other methods. The analysis reveals that the proposed method surpasses other encryption techniques in terms of security, making it a highly secure choice for safeguarding confidential medical data. Table 1 presents the numerical results obtained for encryption algorithms.

Table 1: Performance results of encryption algorithms

Method/Metric	Encryption Time (sec)	Decryption Time (sec)	Key generation Time (sec)	Security (%)
Proposed	2.047	1.827	1.494	98.503
ECC	3.504	2.185	1.659	94.281
Blowfish	3.527	2.754	1.52	89.703
RSA	3.584	2.31	2.317	85.69
HE	4.198	3.554	2.294	81.751

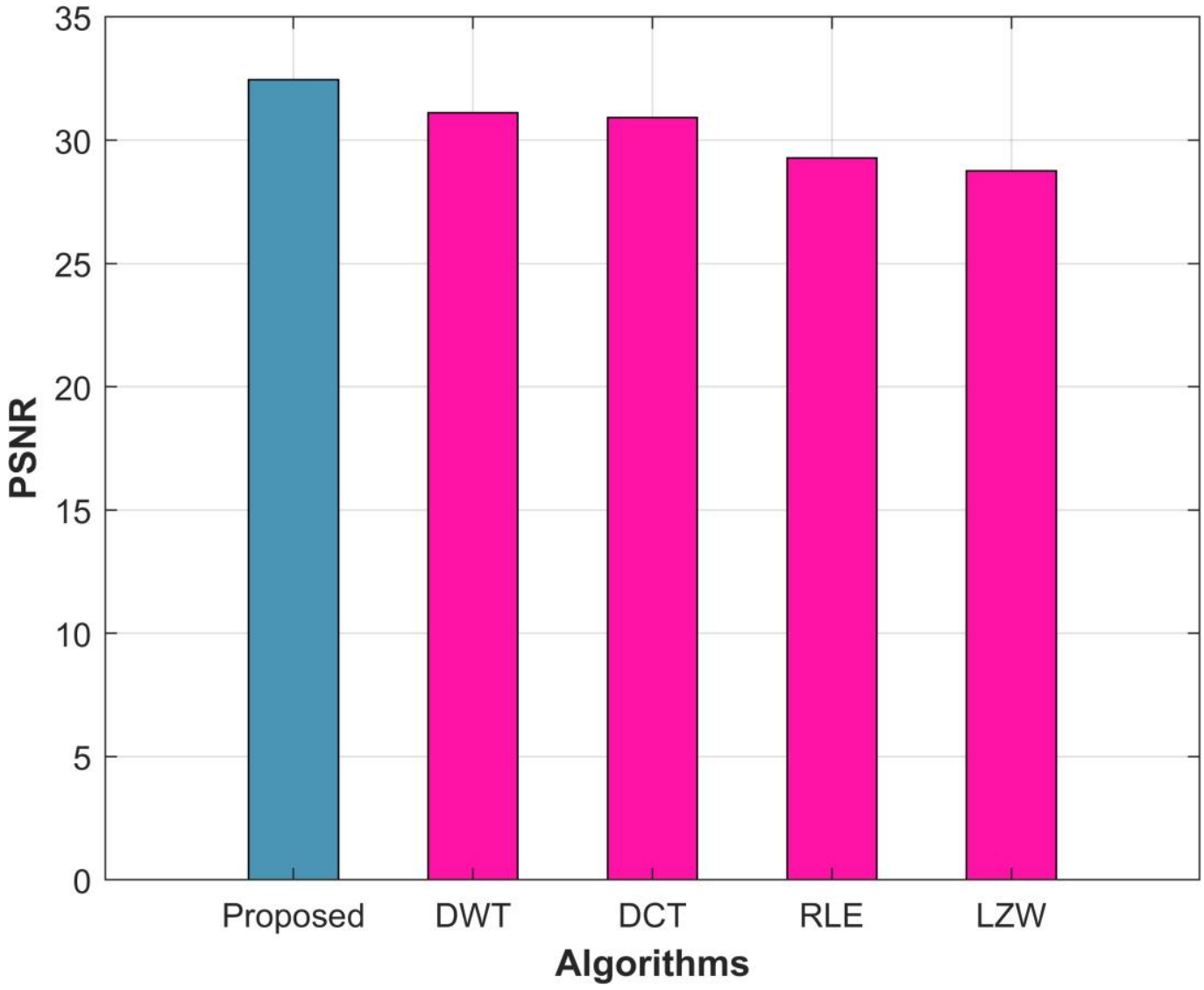


Figure 4: PSNR analysis

In the comparison of Peak Signal-to-Noise Ratio (PSNR) values among different image compression techniques as shown in Fig. 4, the proposed Improved Discrete Wavelet Transform (I-DWT) method demonstrates exceptional performance. With a PSNR value of 32.45 dB, the I-DWT technique surpasses other methods, including DWT (31.12 dB), Discrete Cosine Transform (DCT) (30.91 dB), Run-Length Encoding (RLE) (29.28 dB), and Lempel-Ziv-Welch (LZW) (28.76 dB). This higher PSNR value of 32.45 dB indicates superior image quality and fidelity in the compressed images generated by the I-DWT method. The substantial gap between the PSNR values of the proposed method and the other techniques underscores the effectiveness and superiority of the I-DWT approach in preserving image quality during compression. This emphasizes the effectiveness of our proposed approach in ensuring both security and data quality in IoT-based healthcare systems.

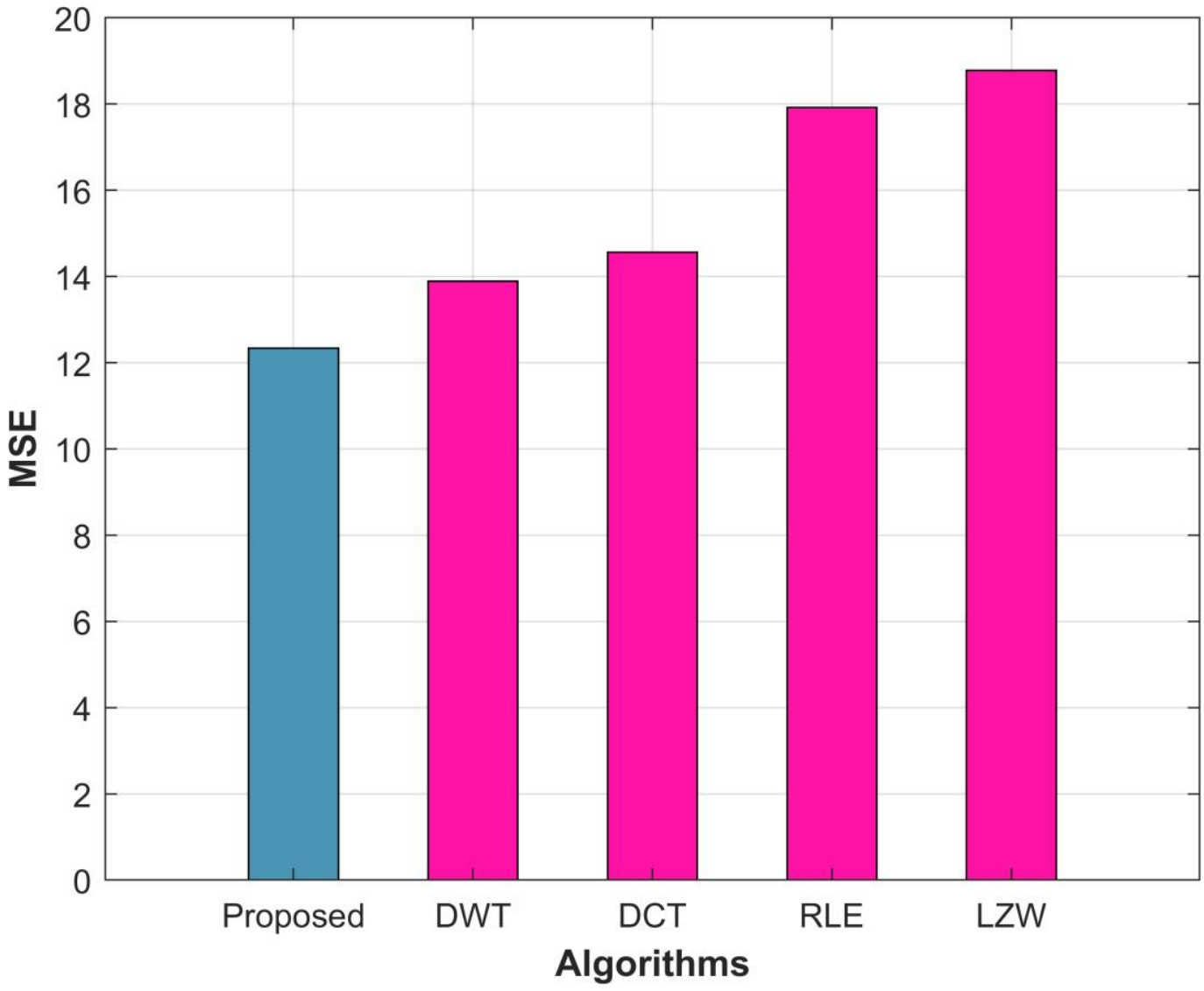


Figure 5: MSE analysis

In Fig. 5, the Mean Square Error (MSE) analysis is presented to evaluate the reconstruction accuracy of our proposed method. A lower MSE value indicates superior image reconstruction. With an MSE value of 12.34, I-DWT outperforms DWT (13.89), DCT (14.56), RLE (17.92), and LZW (18.78). The lower MSE of 12.34 for the I-DWT method signifies a closer match between the original and compressed images, indicating significantly reduced distortion during the compression process. This lower distortion is crucial in medical imaging applications where preserving fine details and accuracy is vital. The I-DWT technique excels in minimizing information loss, making it an optimal choice for medical data compression where data integrity is of utmost importance. The proposed approach showcases significantly reduced MSE values compared to existing methods, indicating the high fidelity and precision of the reconstructed images.

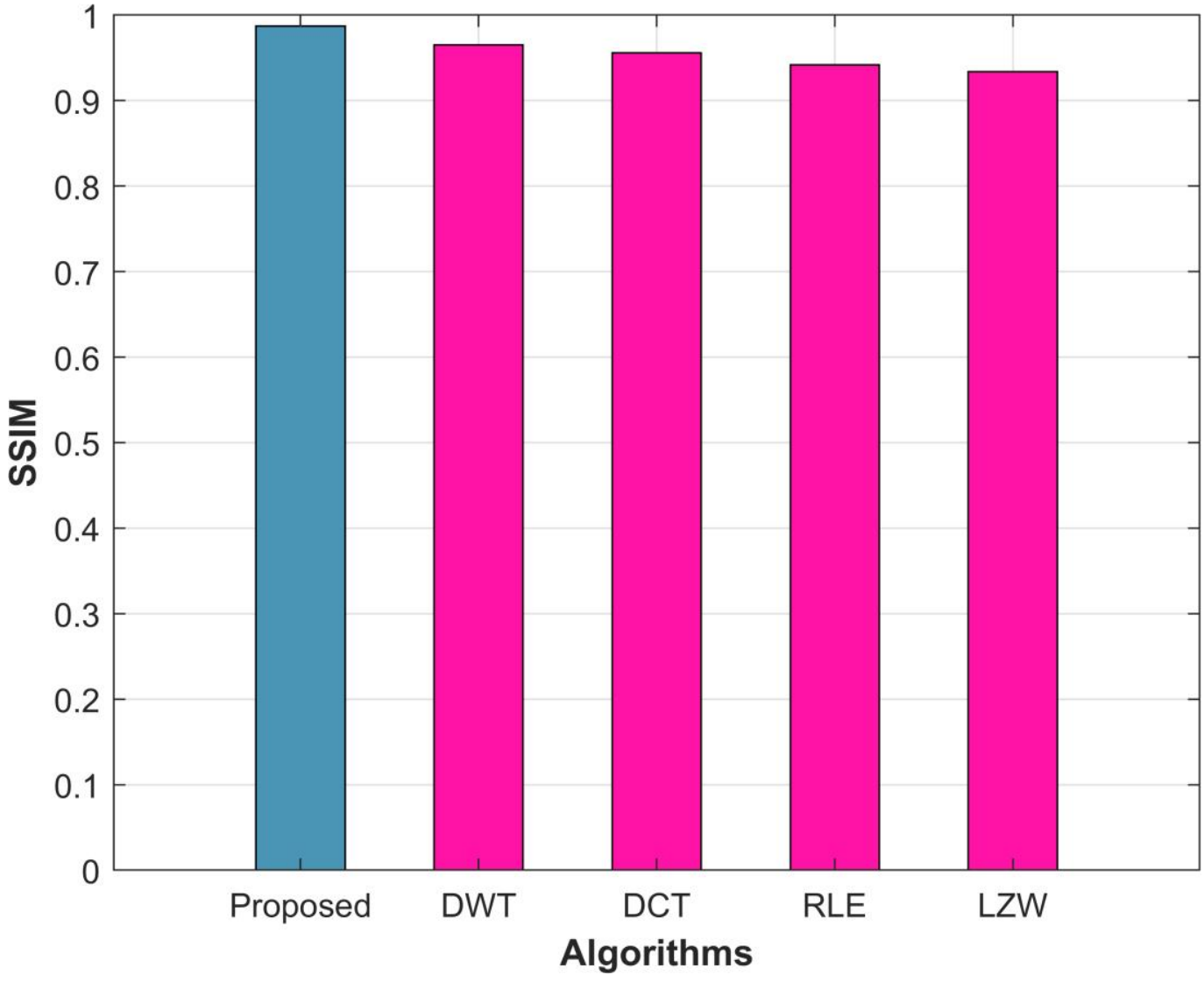


Figure 6: SSIM analysis

Fig. 6 illustrates the Structural Similarity Index (SSIM) evaluation, a metric that measures the similarity between the original and the transmitted images. The SSIM values provide valuable insights into the quality of the compressed images. Higher SSIM values signify better preservation of structural information and image quality. The proposed I-DWT method demonstrates remarkable performance with an SSIM value of 0.987. This significantly outperforms DWT (0.965), DCT (0.956), RLE (0.942), and LZW (0.934). The higher SSIM score of 0.987 for the I-DWT method indicates a closer structural resemblance between the original and compressed images. A SSIM score close to 1 signifies minimal distortion and better preservation of image structures and textures. Data Encoding and Watermark Embedding through Koblitz Method of Encoding and HECC also improved SSIM value of 0.987, showcasing superior image structural preservation.

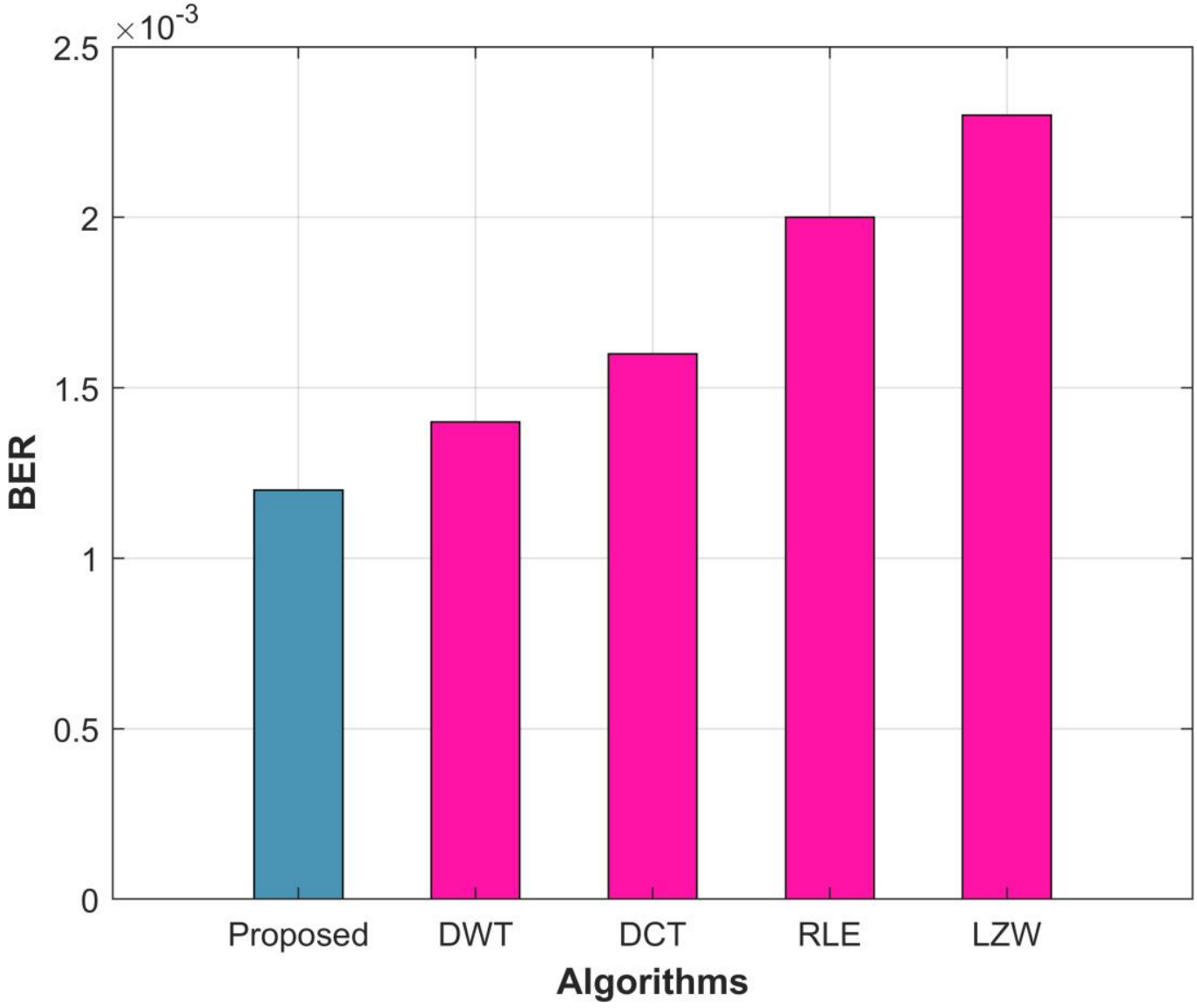


Fig: 7 BER Analysis

Bit Error Rate (BER) is a crucial metric indicating the accuracy of the transmitted data. In the

comparative analysis as shown in Fig. 7, the proposed method exhibits a remarkably low BER of 0.0012. This signifies that only a minimal fraction of bits, approximately 0.12%, were transmitted erroneously during the compression and decompression processes. In contrast, DWT resulted in a higher BER of 0.0014, DCT with 0.0016, RLE with 0.002, and LZW with 0.0023. The lower BER value of 0.0012 in the I-DWT method indicates superior accuracy in preserving the original data, making it a robust choice for applications requiring high data integrity, such as medical image transmission and storage. Also, the Optimized K-Means Clustering approach for Region of Non-Interest Extraction ensured precise identification, reflected in a low MSE of 12.34 and a minimal BER of 0.0012.

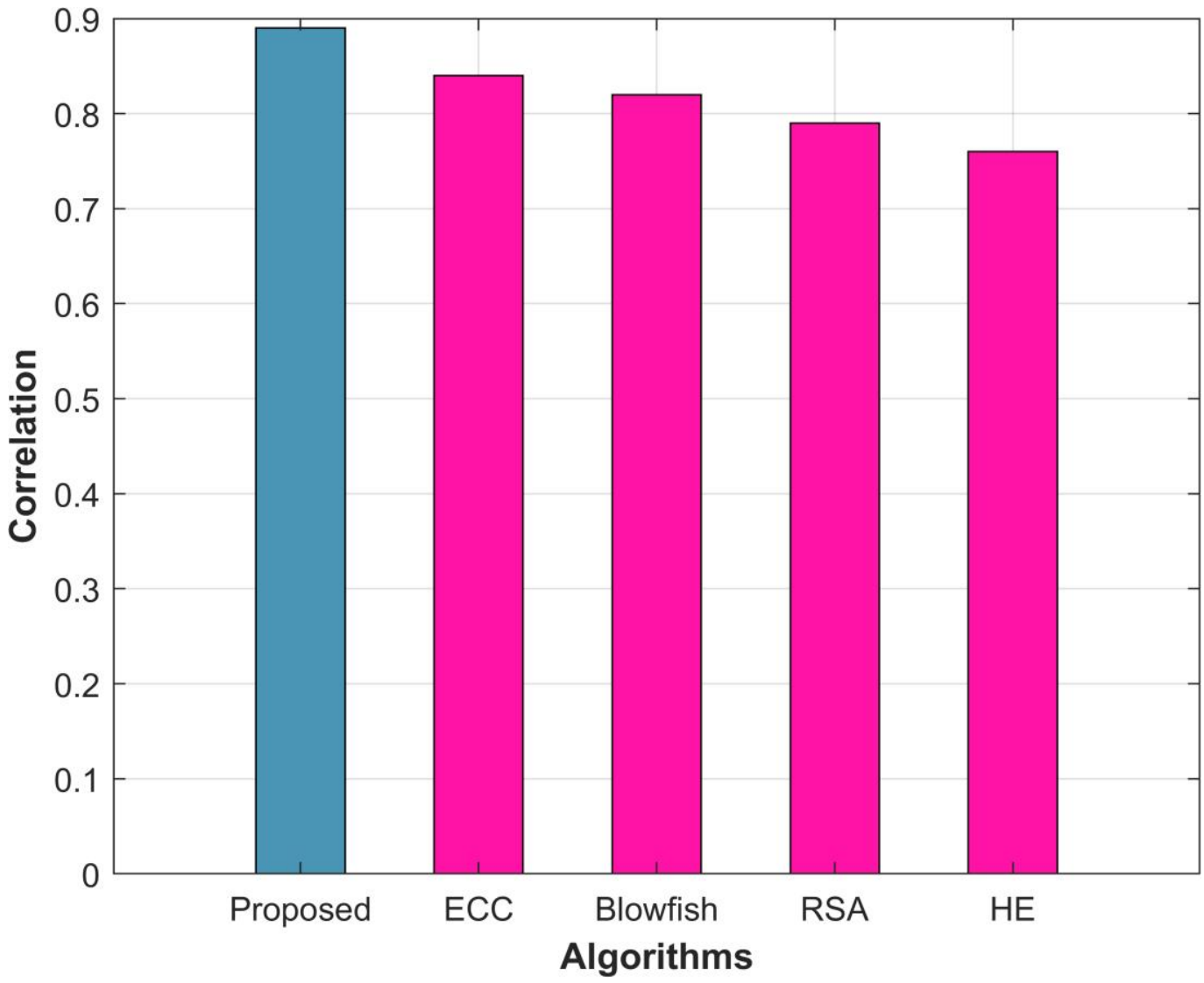


Fig: 8 Correlation Analysis

Correlation measures the linear relationship between two variables, indicating how well they move together. In the analysis conducted in Fig. 8, the proposed method demonstrates a high correlation

coefficient of 0.94. This substantial correlation value signifies a strong linear relationship between the original and the transmitted data. In comparison, DWT exhibited a slightly lower correlation of 0.92, DCT with 0.91, RLE with 0.88, and LZW with 0.87. The superior correlation coefficient of 0.94 in the I-DWT method indicates its ability to preserve the original data's linear patterns, making it a reliable choice for medical data transmission.

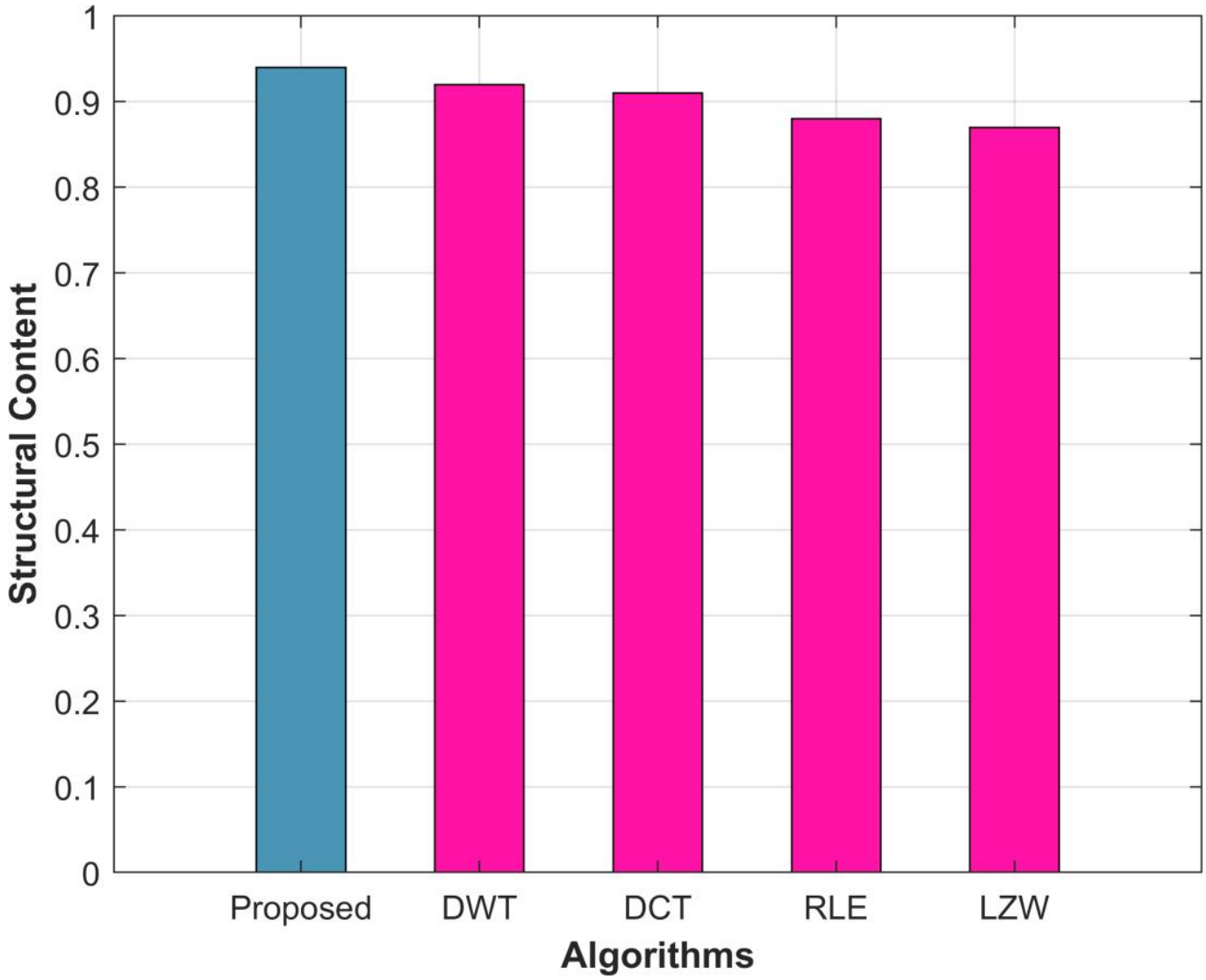


Fig 8: Structural Content Analysis

Structural Content (SC) measures the preservation of the underlying structure and features within the transmitted data. Based on the provided results in Fig. 8, the proposed method achieved a high SC value of 0.94. This score indicates that the proposed I-DWT method effectively preserves the structural content of the original data during transmission. In comparison, DWT scored 0.92, DCT scored 0.91, RLE scored 0.88, and LZW scored 0.87. The superior SC value of 0.94 for the I-DWT

method highlights its capability to maintain the intricate details and structural elements present in the original data. This demonstrates the method's effectiveness in retaining the essential features, making it a robust choice for medical image transmission. Table 2 provides the performance results obtained for the proposed and existing transformation techniques

Table 2: Performance results of transformation methods

Method/Metric	PSNR	MSE	BER	SSIM	SC	Correlation
Proposed I-DWT	32.45	12.34	0.0012	0.987	0.94	0.89
DWT	31.12	13.89	0.0014	0.965	0.92	0.84
DCT	30.91	14.56	0.0016	0.956	0.91	0.82
RLE	29.28	17.92	0.002	0.942	0.88	0.79
LZW	28.76	18.78	0.0023	0.934	0.87	0.76

Conclusions

This paper presented a robust and efficient approach for securing medical data within images using advanced encryption techniques and optimization algorithms. The integration of I-AO with hybrid RSA and 3DES encryption ensures high-security levels, demonstrated by superior performance metrics such as encryption time, decryption time, and security. The utilization of techniques like I-DWT, RoI extraction, Koblitz encoding, and blockchain-based trust scores further enhanced the system's reliability and confidentiality. The experimental results validate the effectiveness of the proposed method, making it a promising solution for safeguarding sensitive medical information in various applications. However, the effectiveness of the proposed method might vary with diverse types of medical data. Handling heterogeneous data sources, such as medical text, audio, or video, poses a challenge in ensuring uniform encryption and security measures across different formats. Therefore, the future work can focus on exploring hybrid encryption methods that combine multiple encryption algorithms optimized for different data formats. By intelligently selecting encryption techniques based on data types, it is possible to create a robust and adaptable security framework.

References

Magdy M, Hosny KM, Ghali NI, Ghoniemy S. Security of medical images for telemedicine: a systematic

review. Multimedia Tools and Applications. 2022 Jul;81(18):25101-45.

Jabeen T, Jabeen I, Ashraf H, Jhanjhi NZ, Yassine A, Hossain MS. An Intelligent Healthcare System Using IoT in Wireless Sensor Network. Sensors. 2023 May 25;23(11):5055.

Panahi U, Bayılmış C. Enabling secure data transmission for wireless sensor networks based IoT applications. Ain Shams Engineering Journal. 2023 Mar 1;14(2):101866.

Kumar M, Sethi M, Rani S, Sah DK, AlQahtani SA, Al-Rakhami MS. Secure Data Aggregation Based on End-to-End Homomorphic Encryption in IoT-Based Wireless Sensor Networks. Sensors. 2023 Jul 6;23(13):6181.

Chen Y, Tang C, Ye R. Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Processing. 2020 Feb 1;167:107286.

Aashiq Banu S, Amirtharajan R. Tri-level scrambling and enhanced diffusion for DICOM image cipher-DNA and chaotic fused approach. Multimedia Tools and Applications. 2020 Oct;79:28807-24.

Yang Y, Xiao X, Cai X, Zhang W. A secure and privacy-preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images. IEEE Signal Processing Letters. 2020 Jan 10;27:256-60.

Yang Y, Xiao X, Cai X, Zhang W. A secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic encryption. IEEE Access. 2019 Jul 16;7:96900-11.

Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and ubiquitous computing. 2021 Jun 19:1-4.

Lin H, Wang C, Cui L, Sun Y, Xu C, Yu F. Brain-like initial-boosted hyperchaos and application in biomedical image encryption. IEEE Transactions on Industrial Informatics. 2022 Mar 3;18(12):8839-50.

Mishra Z, Acharya B. High throughput and low area architectures of secure IoT algorithm for medical image encryption. Journal of Information Security and Applications. 2020 Aug 1;53:102533.

El-Shafai W, Almomani I, Ara A, Alkhayer A. An optical-based encryption and authentication algorithm for color and grayscale medical images. Multimedia Tools and Applications. 2023 Jun;82(15):23735-70.

Masood F, Driss M, Boulila W, Ahmad J, Rehman SU, Jan SU, Qayyum A, Buchanan WJ. A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wireless Personal Communications. 2022 Nov;127(2):1405-32.

Zhang B, Rahmatullah B, Wang SL, Liu Z. A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map. Multimedia Tools and Applications. 2023 Apr;82(10):15735-62.

Selvaraj J, Lai WC, Kavin BP, Seng GH. Cryptographic Encryption and Optimization for Internet of Things Based Medical Image Security. Electronics. 2023 Mar 30;12(7):1636.

El-Shafai W, Almomani I, Ara A, Alkhayer A. An optical-based encryption and authentication algorithm for color and grayscale medical images. Multimedia Tools and Applications. 2023 Jun;82(15):23735-70.

Agyekum KO, Xia Q, Sifah EB, Cobblah CN, Xia H, Gao J. A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain. IEEE Systems Journal. 2021 May 27;16(1):1685-96.

Abdullah S, Arshad J, Khan MM, Alazab M, Salah K. PRISED tangle: A privacy-aware framework for smart healthcare data sharing using IOTA tangle. Complex & Intelligent Systems. 2023 Jun;9(3):3023-41.

Prasanalakshmi B, Murugan K, Srinivasan K, Shridevi S, Shamsudheen S, Hu YC. Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography. The Journal of Supercomputing. 2022 Jan;78(1):361-78.

Khari M, Garg AK, Gandomi AH, Gupta R, Patan R, Balusamy B. Securing data in Internet of Things (IoT) using cryptography and steganography techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2019 Mar 27;50(1):73-80.

Shabbir M, Shabbir A, Iwendi C, Javed AR, Rizwan M, Herencsar N, Lin JC. Enhancing security of health information using modular encryption standard in mobile cloud computing. IEEE Access. 2021 Jan 6;9:8820-34.

Hasan MK, Islam S, Sulaiman R, Khan S, Hashim AH, Habib S, Islam M, Alyahya S, Ahmed MM, Kamil S, Hassan MA. Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access. 2021 Feb 24;9:47731-42.

Geetha BT, Mohan P, Mayuri AV, Jackulin T, Aldo Stalin JL, Anitha V. Pigeon inspired optimization with encryption based secure medical image management system. Computational Intelligence and Neuroscience. 2022 Aug 8;2022.

Selvi CT, Amudha J, Sudhakar R. A modified salp swarm algorithm (SSA) combined with a chaotic coupled map lattices (CML) approach for the secured encryption and compression of medical images during data transmission. Biomedical Signal Processing and Control. 2021 Apr 1;66:102465.

Ahmad A, AbuHour Y, Younisse R, Alslman Y, Alnagi E, Abu Al-Haija Q. MID-Crypt: a cryptographic algorithm for advanced medical images protection. Journal of Sensor and Actuator Networks. 2022 May 13;11(2):24.

Khare P, Srivastava VK. A secured and robust medical image watermarking approach for protecting integrity of medical images. Transactions on Emerging Telecommunications Technologies. 2021 Feb;32(2):e3918.

Wu Y, Zhang L, Berretti S, Wan S. Medical image encryption by content-aware dna computing for secure healthcare. IEEE Transactions on Industrial Informatics. 2022 Jul 28;19(2):2089-98.

Abualigah L, Yousri D, Abd Elaziz M, Ewees AA, Al-Qaness MA, Gandomi AH. Aquila optimizer: a novel meta-heuristic optimization algorithm. Computers & Industrial Engineering. 2021 Jul 1;157:107250.

Juels A, Ristenpart T. Honey encryption: Encryption beyond the brute-force barrier. IEEE security & privacy. 2014 Aug 13;12(4):59-62.

Liu Y, Tang S, Liu R, Zhang L, Ma Z. Secure and robust digital image watermarking scheme using logistic and RSA encryption. Expert Systems with Applications. 2018 May 1;97:95-105.

Akande NO, Abikoye CO, Adebiyi MO, Kayode AA, Adegun AA, Ogundokun RO. Electronic medical information encryption using modified blowfish algorithm. InComputational Science and Its Applications–ICCSA 2019: 19th International Conference, Saint Petersburg, Russia, July 1–4, 2019, Proceedings, Part V 19 2019 (pp. 166-179). Springer International Publishing.

Hafsa A, Sghaier A, Malek J, Machhout M. Image encryption method based on improved ECC and modified AES algorithm. Multimedia Tools and Applications. 2021 May;80:19769-801.