

Innovative Data Security Framework for IoMT Using Lightweight Cryptography and RDWT Steganography

Swetha Pesaru¹, Naresh K. Mallenahalli², B. Vishnu Vardhan³

¹Research Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University of Hyderabad, Kukatpally, Telangana, India

²Engineer/Scientist, National Remote Sensing Center, Hyderabad, India

³Professor, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Hyderabad-UCESTH, Hyderabad, Telangana, India

Corresponding E-mail: swethapesaru2687@gmail.com

Abstract

The fusion of the Internet of Things (IoT) with medical systems, termed the Internet of Medical Things (IoMT), facilitates critical medical functions such as instant diagnosis, remote patient monitoring, and real-time prescription management. However, a significant challenge in healthcare services revolves around ensuring the security and privacy of medical data within IoMT platforms. This study focuses on integration of lightweight cryptography techniques with a steganography model to safeguard medical information. Initially, medical data undergoes segmentation into even and odd characters, with elliptic curve cryptography (ECC) applied to encrypt even characters and Feistel Block Cipher (FBC) to encrypt odd characters. Subsequently, a redundant discrete wavelet transforms (RDWT) based steganography technique conceals the encrypted data within a cover image. Simulation results demonstrate that the proposed method achieves superior resilience and imperceptibility in terms of metrics like Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Mean Square Error (MSE) compared to existing methods. Furthermore, the proposed approach also boasts reduced computational overhead compared to traditional techniques.

Keywords: Internet of Medical Things, real-time diagnosis, remote patient monitoring, real-time medicine prescriptions, medical information security, lightweight cryptography

1. Introduction

The IoT is transforming our lives in ways we could never have anticipated. In contrast to the previous paradigm, everything in the IoT world is seen as smart things that are linked to one another [1]. The IoT is a self-configuration model with physical and network connections, which are communicated each other using standard HTTP protocols [2]. The IoT has the potential capability to transmit message, audio, video over internet. However, securing IoT environment is a difficult task as it is exposed to vital attacks [3].

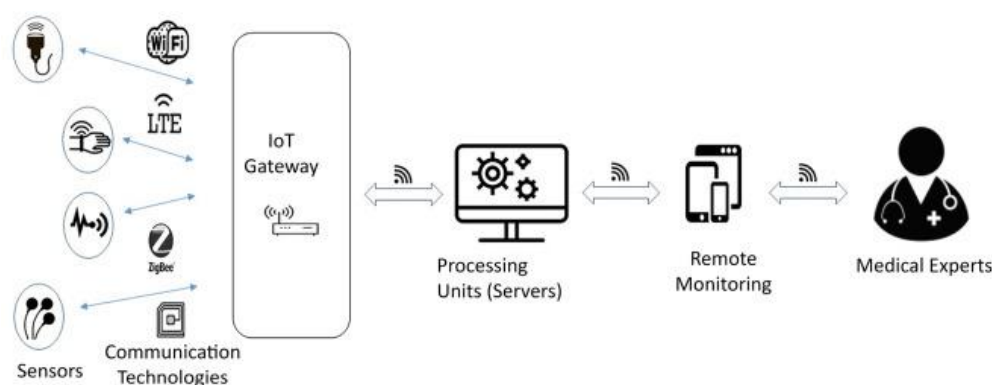


Figure 1. General architecture of internet of medical things.

Recently, the healthcare sector is expanded in excessive manner. The patients are contacting the doctors and hospitals over the IoT environment due to COVID-19 pandemic. Thus, the protection of individual patients' data over IoT environment is a challenging task, which caused to development of IoMT [4] with more secured properties. The IoMT provides tremendous advantages to people's well-being through improving life span and lowering medical costs [5]. As indicated in Figure 1, key features include wireless sensors that were utilized to remotely monitor a patient's health state and communication technology that can communicate the information to caregivers [6]. The IoMT is connectivity of not only various personal medical devices, but also gadgets and commercial corporations, medical researchers, hospitals-based health care providers. The emergence of IoMT is mostly due to a growth in the usage and development of connected and distributed medical devices, which brings with it both attractive prospective applications and various problems [7]. Most of the IoMT devices are wearable, so securing the data from wearable devices is essential. Because of the medical community's stringent ethical criteria, biomedical devices must handle the following issues:

- **Reliability:** A dependable system must always meet its functional objectives, which means it should not fail unexpectedly under typical operating settings [8]. Therefore,

the wearable medical equipment should satisfy their operation with maximum accuracy along with security standards.

- **Safety:** The wearable IoMT device should not affect the environment in which it operates. Specifically, the wearable medical devices must provide maximum safety to its users, they should not harm their users due to excessive radiation [9], heat and other physical problems.
- **Security:** The data generated from wearable medical devices must be secure because of the sensitive and confidential information they gather [10].

The wearable medical devices must satisfy above three properties to avoid the geometrical and non-geometrical attacks [11]. As a result, finding means to collect and send such personal data in this interventionist environment becomes a worry. Therefore, the hybrid cryptographic approaches help to providing security in the face of threats by combining several cryptography/encryption and steganography techniques [12]. Here, encryption provides the first degree of data security to data generated from wearable medical devices. An encryption technique often employs a pseudo-random encryption key [13] produced by an algorithm for technical reasons. The embedding process known as steganography provides the second degree of data security. When people think of the internet, the first thing that springs to mind is security. When it comes to the internet, one of the primary worries is security. Even though HTTPS is present in security situations [14], it is still a point of contention. As a result, it is critical to develop a safe way for transmitting medical data in the IoMT context. This was addressed by combining steganographic methods with encryption and decryption algorithms. Further, applying the steganography on encrypted outcomes resulted in more security and avoids different types of attacks generated in IoMT environment.

This section focusses on intelligent, Secure and Energy-Efficient (ISEE) models [15] for securing the medical data in IoMT environment. In [16] authors implemented the modified LSB approach for medical image steganography. But this method not implemented on IoMT environment. In [17] authors implemented the hybrid encryption system using Bit-Plane Complexity Segmentation (BPCS), which is formed by incorporating the 8-level discrete wavelet transform (DWT). Further, this method also utilized the chaos encryption for encrypting the message. But this suffers with the high error rates. Therefore, Quantum chaos encryption (QCE) [18] is developed with the Quantum cryptography properties. Initially, quantum chaos is used for encryption, Huffman coding used for compression, and improved

least significant bit (LSB) is used for steganography process. But this method suffers with the lower pictorial quality of extracted cover image.

In [19], authors developed the hybrid cryptography approach, which is developed by combining the Steganography and encryption approaches. Initially, Bit Mask Oriented Genetic Algorithm (BMOGA) is used for sensitive encryption of patient medical data. Then, two level DWT (DWT2L) is used for embedding the encrypted data into a cover image. But this method suffers with lower robustness and imperceptibility properties. In [20], authors developed the hybrid encryption system using multiple models. Initially, even bits of patient medical data are encrypted by using advanced encryption standard (AES). Then, odd bits of patient medical data are encrypted by using blowfish standard (BFS). Then, hyperelliptic curve cryptography (HECC) is used for joint encryption of AES and BFS outcomes. In addition, 5-level DWT is used for embedding the encrypted message bits into region of interest-based cover image. Finally, lossy compression is applied on stego image to reduce the size for faster transmitting over IoMT channel. But this method suffers with the higher computational complexity.

In [21], authors developed the hybrid healthcare based IoMT system using cryptographic algorithms. Initially, even bits of patient medical data are encrypted by using Rivest-Shamir-Adleman (RSA) encryption. Then, odd bits of patient medical data are encrypted by using QCE. In addition, 8-level Improved BPCS (IBPCS) is used for embedding the encrypted message bits into region of interest-based cover image. But this method resulted in poor performance against the various geometrical attacks. Further, in [22] authors developed the hybrid medical data transmission system for IoMT environment using encryption, steganographic algorithms. Initially, even bits of patient medical data are encrypted by using RSA encryption. Then, odd bits of patient medical data are encrypted by using AES method. In addition, DWT2L is used for embedding the encrypted message bits into region of interest-based cover image. But this method resulted in poor performance against the various non-geometrical attacks.

The drawbacks of literature [22] is overcome by adopting the Adaptive Genetic Algorithm for Optimal Pixel Adjustment Process (AGA-OPAP) [23], which is natural inspired approach. The AGA-OPAP is mainly used to optimize the extraction coefficients of RSA-AES-DWT2L [22]. However, this method resulted in the poor embedding performance, where extracted message bits contain high error rates. Further, Homomorphic Encryption Based on Matrix (HEBM) [24] is implemented for medical image security for wireless systems. But this method has high synchronization issues in communication channel. Recently, basic LWC based block ciphers

[25] are introduced for medical image data transmission. Initially, SIMON cipher is used to encrypt the message, which is a LWC approach. Then, Chinese Remainder Theorem (CRT) is used for steganography process. Finally, Hybrid Teaching and Learning Based Optimization (HTLBO) based optimization approach is used for reduction computation cost and saving energy. It is observed from work [25] that the LWC approaches are reduced the computational time as compared to traditional encryption, cryptographic approaches.

From, the literature it is observed that the most of the works used RSA, AES, QCE, HECC, BFC, CRT and some other models. All these conventional models are basic cryptographic approaches, which resulted in high computation time and low robustness, imperceptibility performance. Thus, this work is focused on implementation of novel LWC approaches for better performance with reduced processing time.

The following are the significant contributions of this work:

- The proposed LWC-DH model contains ECC, FBC based LWC methods and RDWT based steganography method for data hiding.
- Here, ECC is used to encrypt the even characters and FBC is used to encrypt the odd characters of original medical data.

Apply RDWT on encrypted message, which hides the encrypted message into cover image and shows the better steganography performance.

- The simulation results shows that the proposed LWC-DH approach resulted in superior robustness and imperceptibility in terms of MSE, PSNR, SSIM, as compared to conventional approaches.

Rest of the article is summarized as follows: Section 2 deals with the detailed operation of related work with their drawbacks. Section 3 deals with the preliminary's operation such as ECC, FBC, RDWT. Section 4 deals with the detailed analysis of proposed LWC-DH model. Section 5 deals with the detailed analysis of results and discussions. Section 6 deals with the conclusion and future works.

2. Prerequisites

2.1 ECC

This section contains some of the most basic principles in ECC that are important to this research. It has been shown that ECC is a more efficient cryptographic approach for security

when compared to earlier traditional cryptography techniques such as RSA, AES, QCE, BFC, CRT. When compared to other algorithms, ECC requires a much smaller key size to provide the same degree of security. The algorithm for ECC is shown in Table 1. For the mathematical operations, the elliptic curve equation $E_p(a, b): y^2 = x^3 + ax + b \pmod p$; is used to describe the operations when $a, b \in Z_p$ and $4a^3 + 27b^2 \pmod p \neq 0$, with p being a big prime integer. A point at infinity (x, y) is defined by the values of the variables a and b , and the points (x, y) that include that point are defined by the elliptic curve if and only if the preceding provided assertion is true. The repeated addition method is used to create what is commonly known as scalar multiplication, as in $tQ = Q + Q + Q + Q + \dots + Q$ (t times). Given Q as a point and $t \in F_p^*$ as an integer, the term "scalar multiplication" is defined as (t times). The domain parameters are members of the finite field F_p^* , which is defined as $F_p^* \text{ i.e. } (p, a, b, P, n, h) \in F_p^*$ is an abelian group, and the identity element of this group is the point that is at the limit of the domain.

Table 1. ECC algorithm

Key Generation
<p>Step 1: Develop elliptic curve equation $E_p(a, b): y^2 = x^3 + ax + b \pmod p$ with base point (G). The ECC points satisfies $(a * G) * b = (b * G) * a$ property.</p> <p>Step 2: Consider user A as sender and generate key for user A</p> <ul style="list-style-type: none"> • Select private key n_A; $n_A < n$. (Here, n is number of data bits generated by A) • Calculate public key, $P = n_A \times G$ <p>Step 3: Consider user B as receiver and generate key for user B.</p> <ul style="list-style-type: none"> • Select private key, n_B; $n_B < n$ • Calculate public key, $M = n_B \times G$ <p>Step 4: Equalize the resultant keys: $n_A \times M = n_A \times (n_B \times G) = n_B \times (n_A \times G) = n_B \times P$.</p>
ECC Encryption
<p>Step 5: Consider P_m as secret message generated from medical wearable device (user-A).</p> <p>Step 6: Calculate public key of user-A as mentioned in step-2, such as $P_A = n_A \times G$ with best elliptic curve point G as mentioned in step 1.</p> <p>Step 7: Finally, generate the cipher message (C_m) using user-A public keys.</p> $C_m = \{c_1, c_2\} = \{kG, P_m + kP_A\}$ <p>Here, k is an integer, which is randomly selected from range $[1 \text{ to } (n-1)]$ and c_1, c_2 are ECC points.</p>
ECC Decryption

Step 8: generate public key of user-B as mentioned in step-3, such as $P_B = n_B \times G$ with best elliptic curve point G as mentioned in step 1.

Step 9: Generate the extracted secret message (P_{med}) at user-B using following condition

$$P_{med} = c_2 - n_B * c_1$$

2.2 FBC

Luby and Rackoff were the first to propose the method of constructing a pseudo random permutation by employing the FBC network, which can achieve complete diffusion and confusion of encrypted data by alternately employing two basic operations of substitute and permutation and has a higher level of security and encryption efficiency than the previous methods proposed. Cryptographic structures that employ the FBC format are known as block cypher structures. Many classic block cyphers, such as FEAL, DES, and RC5, have adopted the FBC structure, among them RC5 and others. An iterative structure, the FBC structure is also a product form of cryptographic transformation, and it completely achieves the diffusion and scramble functions, resulting in a highly strong cryptosystem with a very long lifetime.

If the plaintext block P is divided into the left and right halves, $P = (L_0, R_0)$: for each round i of the encryption process, where round is defined as one of the integers $i = 1, 2, \dots, n$, a new left half part and new right half part are generated according to the rules as follows:

$$L_i = R_{i-1} \tag{1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \tag{2}$$

Here, round function indicated by F , sub-key is indicated by K_i , and i indicates round number. In this case, the sub-key is produced from the key K and is scheduled according to a specified key scheduling technique.

FBC Encryption process: Figure 2 (a) shows the FBC encryption process and it is illustrated as follows:

Step 1: The plain text is split into blocks of a set size, and only one block is treated at a time.

Step 2: The plain text is separated into blocks of a variable size, and only one block is processed at a time. As a result, the plain text block and the key K serve as the input to the encryption process.

In step two, the plain text block is separated into two equal halves, denoted by the letters RE_0 for the right half of the plain text block and LE_0 for the left half of the plain text block. Now,

LE_0 and RE_0 are subjected to several rounds of ciphering in order to generate the ciphertext block.

Each round, the encryption formulation was applied to the RE_i , together with K_i , to create an encrypted block. Afterwards, the output of this encryption formulation is XORed with the LE_i . This formulation output is the new right half for round RE_{i+1} , which replaces the result of the XOR function. Further, as seen in the picture above, the previous right half RE_i is transformed into the new left half LE_{i+1} for the next round. Each cycle involves the execution of the same function and generates the final encrypted message.

FBC decryption procedure: As seen in Figure 2 (b), the FBC structure does not use a various decryption technique than the other structures. The encryption and decryption functions suggested by FBC are the same as those offered by other organizations, with the exception of a few restrictions, which are as follows:

Step 1: the decryption algorithm is given the input of a cypher text block that was generated by the encryption process.

Step 2: The encryption sequence is reversed by reversing the order of subkeys utilized. The K_n is used in the first round of decryption, and then K_{n-1} used in the second round of decryption, and the iteration continues until the last round of decryption is performed, in which case the key K_1 is utilised.

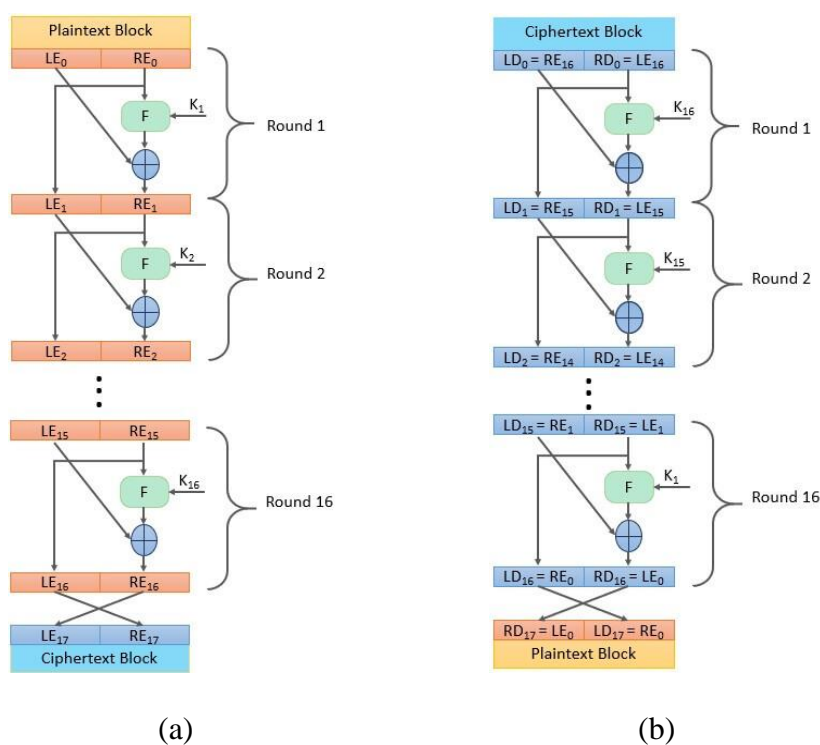


Figure 2. FBC process (a) encryption, (b) decryption

2.3 RDWT

Due to the down-sampling of its bands, DWT is one of the most widely used data hiding technologies, however one of its primary disadvantages is that it does not offer shift invariance. Even slight changes in the input image have a big impact on the image's wavelet coefficients. The shift variation of DWT causes incorrect extraction of the cover image, because data hiding needs the authors to know the exact areas where the data hidden information is placed. The RDWT has been offered as a solution to this problem by researchers. The RDWT is utilised to solve this problem since it eliminates down sampling and provides shift invariance.

Let $X(n)$ and $X'(n)$ represent the source and recovered signals. Here, LPF and HPF analysis filters are referred to as $a[-k]$ and $d[-k]$, while their synthesis filters are referred to as $a[k]$ and $d[k]$, respectively. Further, A_j and D_j are the output coefficients at the j th level. As previously stated, RDWT does not include the coefficients for up and down sampling. The RDWT filter bank analysis and synthesis are shown in Figure 3. Analysis and synthesis in DWT were stated as follows,

$$y[n] = (x * g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n - k] \quad (3)$$

$$A_j[k] = (A_{j+1}[k] * a_j[-k]) \alpha \quad (4)$$

and

$$D_j[k] = (A_{j+1}[k] * d_j[-k]) \alpha \quad (5)$$

Convolution is indicated by $*$ in Equations (3), (4) and (5), while down sampling is denoted by α . Further, synthesis was accomplished by using following equation,

$$A_{j+1}[k] = (A_j[k]\beta) * a[k] + (D_j[k]) * d[k] \quad (6)$$

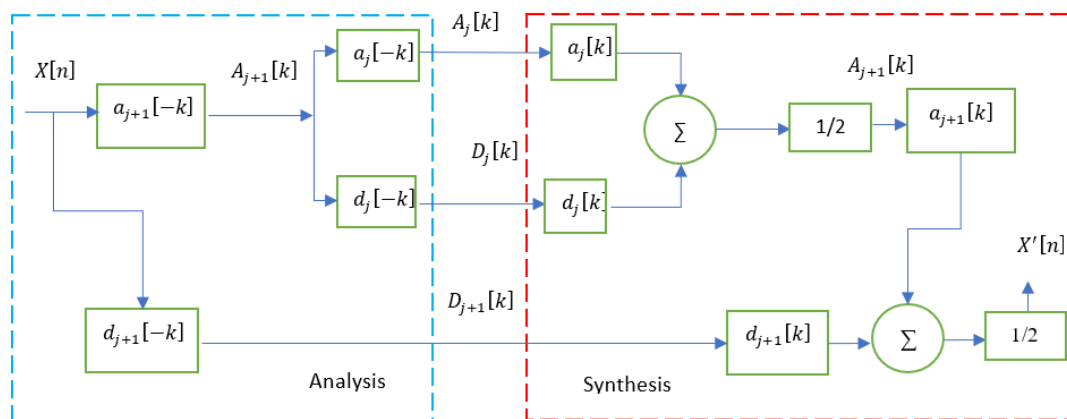


Figure 3: RDWT decomposition with filter bank structure.

Up sampling by a factor of two is denoted as β in Equation (6). As previously stated, RDWT does not take into account the up and down sampling operations that occur in DWT. As a result, the size of the input data is equal to the size of the decomposed data coefficients, which was expressed. RDWT analysis filter bank is formulated mathematically using Equation (7) and Equation (8) as follows:

$$a_j[K] = a_{j+1}[K]\beta \quad (7)$$

$$d_j[K] = d_{j+1}[K]\beta \quad (8)$$

Synthesis was stated using Equations (9) and (10).

$$A_j[k] = (A_{j+1}[k] * a_j[-k]) \quad (9)$$

$$D_j[k] = (A_{j+1}[k] * d_j[-k]) \quad (10)$$

$$A_{j+1}[k] = \frac{1}{2}(A_j[k] * a_j[k] + D_j[k] * d_j[k]) \quad (11)$$

In the temporal domain, RDWT maintains a constant sampling rate. The RDWT's redundancy fundamentally aids data hiding applications in increasing their embedding capacity.

3. Proposed methodology

Recently, the healthcare industry has grown at a shocking rate. Due to the COVID-19 epidemic, people are contacting physicians and hospitals through the IoT environment. As a result, protecting individual patients' data in an IoT context is a difficult problem, which has led to the creation of IoMT with more secure qualities. A reliable system must constantly satisfy its functional goals, which implies it should not fail abruptly under normal operating conditions. As a result, wearable medical equipment must operate with maximum precision while still meeting security regulations. The wearable IoMT device should have no negative impact on the environment in which it functions. Wearable medical gadgets must guarantee optimum safety to their users, and they must not injure their users due to high radiation, heat, or other physical concerns. The LWC methods can effectively solve these problems, as they consume very low power, which is not harmful to the users. Because wearable medical devices collect sensitive and personal information, thus the data created by them must be secure. Thus, the LWC-DH methods maintain the security standards, safter precautions with maximum reliability.

Figure 4 presents the process of proposed LWC-DH method with encryption and steganography schemes. The proposed LWC-DH system is created by combining LWC

techniques with a steganography model to secure medical data. Medical data is first separated into even and odd characters, with even characters encrypted using ECC and odd characters encrypted using FBC cryptography. The encrypted message is then hidden in the cover picture using RDWT-based steganography. Across the receiver side reverse operation is performed and generates original message.

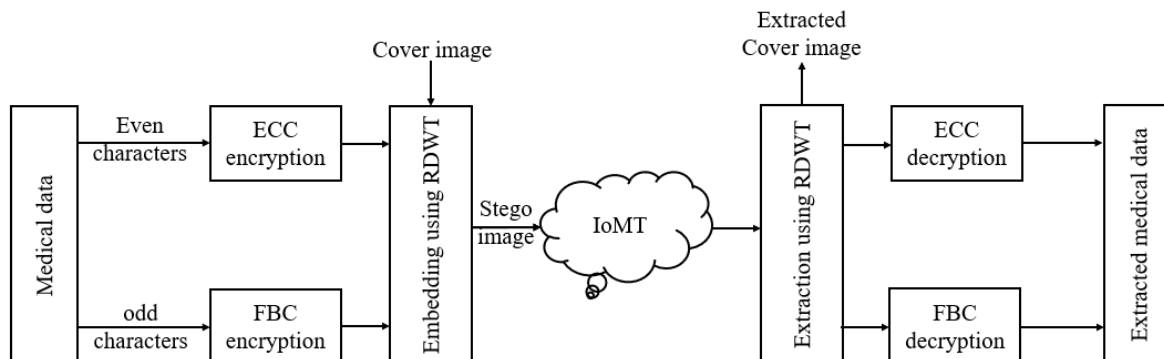


Figure 4. Proposed LWC-DH model for IoMT.

3.1 LWC-DH embedding

The proposed LWC-DH process contains two levels of security, where the first level of security contains the cryptographic methods, and second level of security is achieved by steganography method. The process of proposed hybrid embedding procedure is presented in following steps:

Step 1: Consider the patients' medical records as the input message and divide the message into even, odd characters separately. Here, the separation of message is used to encrypt individual bits more efficiently.

$$[M_{even}, M_{odd}] = even_odd_split (M) \quad (12)$$

Here, M is the original message, M_{even} is the even message data, and M_{odd} is the odd message data.

Step 2: Apply the even message characters to ECC, which is light weight cryptography method. The ECC method is presented in section 3.1, which provides the higher robustness to message.

$$M_{ECC} = ECC_encryption (M_{even}) \quad (13)$$

Step 3: Apply the odd message characters to FBC, which is a highspeed encryption method. The process of FBC method is presented in the section 3.2.

$$M_{FBC} = FBC_encryption (M_{odd}) \quad (14)$$

Step 4: Apply the RDWT embedding algorithm as presented in Table 2, which performs the steganography operation between M_{ECC} , M_{FBC} and cover medical image (C).

Step 5: Transmit the stego image into IoMT environment, so the patient medical records is securely transfer to the receiver.

Table 2. RDWT embedding algorithm.

<p>Inputs: C, M_{ECC}, M_{FBC}.</p> <p>Outputs: S</p>
<p>Step 1: Convert M_{ECC}, M_{FBC} into ASCII Code seperately, which generates $M_{ECC_{ASCII}}$, $M_{FBC_{ASCII}}$.</p>
<p>Step 2: Appply RDWT operation on cover image, which decomposes the image into low low (LL_C), low high (LH_C), high low (HL_C), and high high (HH_C) bands.</p> $[LL_C, LH_C, HL_C, HH_C] = RDWT(C).$
<p>Step 3: Hide $M_{ECC_{ASCII}}$ values in HL_C band, such as $HL_{new} = \{M_{ECC_{ASCII}}, HL_C\}$.</p>
<p>Step 4: Hide $M_{FBC_{ASCII}}$ values in HH_C band, such as $HH_{new} = \{M_{FBC_{ASCII}}, HH_C\}$.</p>
<p>Step 5: Perform Inverse RDWT (IRDWT) operation on LL_C, LH_C, HL_{new} and HH_{new} bands, which generates the stego imgae (S).</p> $[S] = IRDWT([LL_C, LH_C, HL_{new}, HH_{new},]).$

3.2 LWC-DH extraction

After incorporating the patient’s medical records into the cover image, the resultant stego image is exposed to insecure channel. At the receiver side all the processes are executed in reverse order to get back the secret information. The process of proposed hybrid extraction procedure is presented in following steps:

Step 1: Receive the stego image from IoMT and apply it to RDWT extraction algorithm as presented in Table 3, which generates the extracted cover image (C_{Ed}), even and odd extracted messages.

Step 2: Apply the even $M_{ECC_{ed}}$ characters to ECC decryption procedure, which generates the original even message characters ($M_{even_{ed}}$).

$$M_{even_{ed}} = ECC_decryption (M_{ECC_{ed}}) \tag{15}$$

Step 3: Apply the $M_{FBC_{ed}}$ characters to FBC decryption procedure, which generates the original odd message characters ($M_{odd_{ed}}$).

$$M_{odd_{ed}} = FBC_encryption(M_{odd}) \quad (16)$$

Step 4: Concatenate the even and odd sequenced extracted messages uniformly, which generates the final extracted message (M_{ed}).

Table 3. RDWT extraction algorithm.

Inputs: S
Outputs: $C_{Ed}, M_{ECC_{ed}}, M_{FBC_{ed}}$.
<p>Step 1: Apply RDWT operation on stego image, which decomposes the image into $LL_S, LH_S, HL_S,$ and HH_S.</p> $[LL_S, LH_S, HL_S, HH_S] = RDWT(S).$
Step 2: Sepertae the HL_S band into $M_{ECC_{ASCII}}$ message, HL_{S0} parts.
Step 3: Sepertae the HH_S band into $M_{FBC_{ASCII}}$ message, HH_{S0} parts.
<p>Step 4: Perform ASCII Code to binary conversion operation on $M_{ECC_{ASCII}}$, and $M_{FBC_{ASCII}}$ messages, which generates the extracted even message ($M_{ECC_{ed}}$) and extracted odd message ($M_{FBC_{ed}}$).</p>
<p>Step 5: Perform Inverse RDWT (IRDWT) operation on $LL, LH, HL_{S0},$ and HH_{S0} bands, which generates the extracted cover imgae (C_{ed}).</p> $[C_{ed}] = IRDWT([LL_S, LH_S, HL_{S0}, HH_{S0}]).$

4. Results and discussion

This section compares the performance of proposed models with existing encryption and cryptography models. The performance comparison is carried out using PSNR, SSIM, MSE performance metrics and objective performance of various approaches are also presented.

4.1 Subjective performance

This section deals with subjective evaluation of proposed methods on the three datasets. Figure 6 compares the performance of proposed LWC-DH method with conventional method using IDRiD cover images. Here, different medical messages like “diabetic retinopathy”, “diabetic macular edema”, “Diabetic retinopathy grade 1”, and “diabetic macular edema -2” are embedded into cover images and extracted perfectly as presented in fourth row. Here, the conventional RSA-AES-DWT2L [22] extracted images suffer with high contrast, whereas LWC-DH extracted images look similar like cover images.













Cover images				
Source message	Diabetic retinopathy	diabetic macular edema	Diabetic retinopathy grade 1	Diabetic macular edema 2
RSA-AES-DWT2L [22] extracted				
LWC-DH extracted images				
Proposed extracted messages	Diabetic retinopathy	diabetic macular edema	Diabetic retinopathy grade 1	Diabetic macular edema 2

Figure 6. Performance analysis of LWC-DH on IDRiD based cover images

4.2 Objective performance comparison

This section compares the objective performance of proposed methods with the conventional approaches and compares the computation time of various methods. Table 4 compares the performance of proposed LWC-DH method with the conventional BMOGA-DWT2L [19], AES-BFS-HECC [20], RSA-QCE-IBPCS [21], RSA-AES-DWT2L [22], and AGA-OPAP [23]. The proposed method improves the PSNR, SSIM and reduced the MSE as compared to conventional approaches, which shows the proposed LWC-DH approach resulted in better robustness and imperceptibility performance. Figure 7 presents the graphical representation of performance comparison.

Table 5 compares the computation time computation of proposed LWC-DH approach with conventional methods such as BMOGA-DWT2L [19], RSA-QCE-IBPCS [21], RSA-AES-DWT2L [22], AGA-OPAP [23], HEBM [24], and HTLBO [25]. The proposed method resulted in low computation time as compared to traditional encryption methods as proposed method adapted the LWC methods for dual stage encryption.

Table 4. Performance comparison of LWC-DH model with conventional methods

Method	PSNR (dB)	SSIM	MSE
BMOGA-DWT2L [19]	47.82	0.8937	1.0736
AES-BFS-HECC [20]	52.39	0.9173	0.396
RSA-QCE-IBPCS [21]	57.69	0.9545	0.136
RSA-AES-DWT2L [22]	68.26	0.9836	0.009736
AGA-OPAP [23]	74.38	0.9892	0.00237
Proposed LWC-DH method	82.25	0.9980	0.0002869

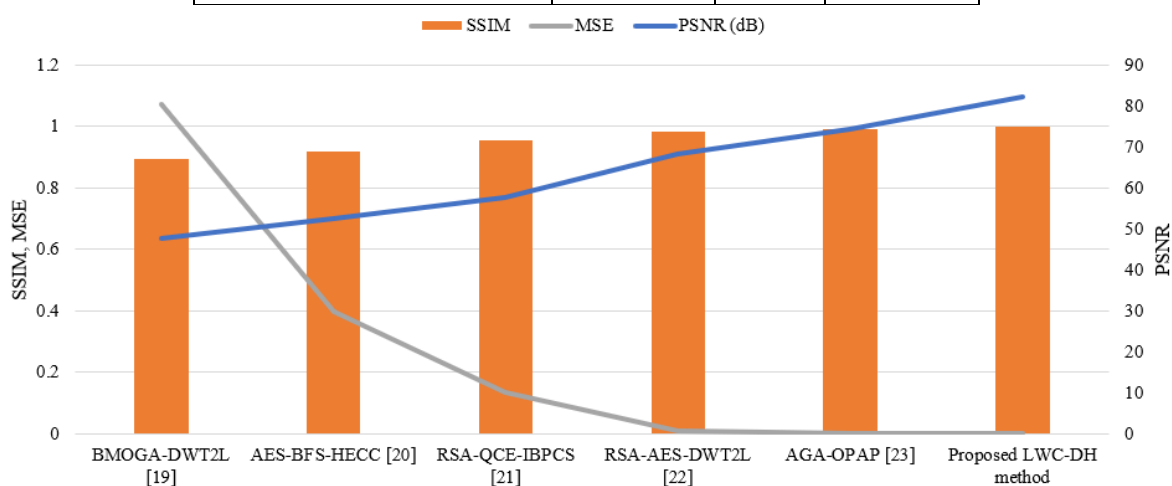


Figure 7. Graphical representation of performance comparison

Table 5. Computation time (in seconds) comparison of LWC-DH model with conventional methods

BMOGA-DWT2L [19]	RSA-QCE-IBPCS [21]	RSA-AES-DWT2L [22]	AGA-OPAP [23]	HEBM [24]	HTLBO [25]	Proposed LWC-DH
0.192	0.174	0.142	0.1038	0.0947	0.05237	0.0238

5. Conclusion

In conclusion, the integration of lightweight cryptography and steganography within the IoMT presents a promising approach to addressing the critical challenges of securing medical data.

The proposed LWC-DH system, combining ECC and FBC for encryption, along with RDWT for steganography, has demonstrated superior robustness, imperceptibility, and computational efficiency compared to conventional methods. Through simulations, this work achieved significant improvements in metrics such as PSNR, SSIM, and MSE, indicating the effectiveness of our approach in safeguarding medical information while embedding it into cover images seamlessly. These results underscore the viability of our method for enhancing confidentiality and integrity in IoMT environments, crucial for real-time diagnosis, remote patient monitoring, and secure medicine prescription management. Looking ahead, there are several avenues for future research and development in this domain. Firstly, exploring further advancements in lightweight cryptography algorithms tailored specifically for IoMT applications could enhance both security and computational efficiency. Additionally, investigating novel steganography techniques beyond RDWT to improve data hiding capacity without compromising image quality can be beneficial. Moreover, addressing the scalability and interoperability challenges of IoMT systems remains pivotal. Future studies could focus on developing standardized protocols and frameworks that ensure seamless integration and secure communication among heterogeneous medical devices and platforms. Furthermore, investigating the impact of emerging technologies such as blockchain for enhancing data integrity and traceability in IoMT could open new possibilities for secure medical data management.

References

- [1]. Yaacoub, Jean-Paul A., et al. "Securing internet of medical things systems: Limitations, issues and recommendations." *Future Generation Computer Systems* 105 (2020): 581-606.
- [2]. Ullah, Ata, et al. "Secure healthcare data aggregation and transmission in IoT—A survey." *IEEE Access* 9 (2021): 16849-16865.
- [3]. Kaabi, Rana, Hassan Fakhruddin, and Karrar Alhamami. "The Status, Challenges, and Future Trends of Advanced Crypto Algorithms for Wireless Network Security: an Overview." (2021).
- [4]. Qiu, Han, et al. "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0." *IEEE journal of biomedical and health informatics* 24.9 (2020): 2499-2505.
- [5]. Papaioannou, Maria, et al. "A survey on security threats and countermeasures in internet of medical things (IoMT)." *Transactions on Emerging Telecommunications Technologies* (2020): e4049.

- [6]. Sun, Yingnan, Frank P-W. Lo, and Benny Lo. "Security and privacy for the internet of medical things enabled healthcare systems: A survey." *IEEE Access* 7 (2019): 183339-183355.
- [7]. Kagita, Mohan Krishna, et al. "A review on security and privacy of internet of medical things." *Intelligent Internet of Things for Healthcare and Industry*. Springer, Cham, 2022. 171-187.
- [8]. Ray, Partha Pratim, Dinesh Dash, and Neeraj Kumar. "Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions." *Computer Communications* 160 (2020): 111-131.
- [9]. Thamilarasu, Geethapriya, Adedayo Odesile, and Andrew Hoang. "An intrusion detection system for internet of medical things." *IEEE Access* 8 (2020): 181560-181576.
- [10]. Parah, S. A., Kaw, J. A., Bellavista, P., Loan, N. A., Bhat, G. M., Muhammad, K., & de Albuquerque, V. H. C. (2020). Efficient security and authentication for edge-based internet of medical things. *IEEE Internet of Things Journal*, 8(21), 15652-15662.
- [11]. Huang, Xucheng, and Shah Nazir. "Evaluating security of internet of medical things using the analytic network process method." *Security and Communication Networks* 2020 (2020).
- [12]. Kumar, Randhir, and Rakesh Tripathi. "Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology." *The Journal of Supercomputing* 77.8 (2021): 7916-7955.
- [13]. Manimurugan, S., Al-Mutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access*, 8, 77396-77404.
- [14]. Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of medical things security assessment framework. *Internet of Things*, 8, 100123.
- [15]. Allahham, M. S., Abdellatif, A. A., Mohamed, A., Erbad, A., Yaacoub, E., & Guizani, M. (2020). I-SEE: Intelligent, Secure, and Energy-Efficient Techniques for Medical Data Transmission Using Deep Reinforcement Learning. *IEEE Internet of Things Journal*, 8(8), 6454-6468.
- [16]. Stoyanov, Bozhidar, and Borislav Stoyanov. "BOOST: Medical image steganography using nuclear spin generator." *Entropy* 22.5 (2020): 501.

- [17]. Bansal, Ritesh, Chander Kumar Nagpal, and Shailender Gupta. "An efficient hybrid security mechanism based on chaos and improved BPCS." *Multimedia Tools and Applications* 77.6 (2018): 6799-6835.
- [18]. Dhall, Sangeeta, Rinku Sharma, and Shailender Gupta. "A multi-level steganography mechanism using quantum chaos encryption." *Multimedia Tools and Applications* 79.3 (2020): 1987-2012.
- [19]. Pandey, Hari Mohan. "Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography." *Future Generation Computer Systems* 111 (2020): 213-225.
- [20]. Prasanalakshmi, B., et al. "Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography." *The Journal of Supercomputing* 78.1 (2022): 361-378.
- [21]. Panwar, Priya, Sangeeta Dhall, and Shailender Gupta. "A multilevel secure information communication model for healthcare systems." *Multimedia Tools and Applications* 80.5 (2021): 8039-8062.
- [22]. Elhoseny, Mohamed, et al. "Secure medical data transmission model for IoT-based healthcare systems." *Ieee Access* 6 (2018): 20596-20608.
- [23]. Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. *Multimedia Tools and Applications*, 80(14), 21165-21202.
- [24]. Huang, Haiping, et al. "Private and secured medical data transmission and analysis for wireless sensing healthcare system." *IEEE Transactions on Industrial Informatics* 13.3 (2017): 1227-1237.
- [25]. Rani, S. Sheeba, et al. "Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers." *Multimedia Tools and Applications* 79.47 (2020): 35405-35424.
- [26]. Reddy, V. P. C., & Gurralla, K. K. (2022). Joint DR-DME classification using deep learning-CNN based modified grey-wolf optimizer with variable weights. *Biomedical Signal Processing and Control*, 73, 103439.

- [27]. Oh, Yujin, Sangjoon Park, and Jong Chul Ye. "Deep learning COVID-19 features on CXR using limited training data sets." *IEEE transactions on medical imaging* 39.8 (2020): 2688-2700.
- [28]. Tabik, Siham, et al. "COVIDGR dataset and COVID-SDNet methodology for predicting COVID-19 based on chest X-ray images." *IEEE journal of biomedical and health informatics* 24.12 (2020): 3595-3605.
- [29]. Varma, P. B. S., Paturu, S., Mishra, S., Rao, B. S., Kumar, P. M., & Krishna, N. V. SLDCNet: Skin lesion detection and classification using full resolution convolutional network-based deep learning CNN with transfer learning. *Expert Systems*, e12944.
- [30]. Gottumukkala, VSSP Raju, N. Kumaran, and V. Chandra Sekhar. "BLSNet: Skin lesion detection and classification using broad learning system with incremental learning algorithm." *Expert Systems*: e12938.