History of Medicine, 2022, 8(1): 474-493
DOI: 10.17720/2409-5834.v8.1.2022.48

LIGHT WEIGHT BASED SECURED MEDICAL DATA TRANSMISSION FOR IOT POWERED COMMUNICATION SYSTEM

MD Reshma, P Ashwini, Jatavath Nagarjun Naik
Assistant professor, Assistant professor, Assistant professor

Department Of CSE
Sree dattha institute of engineering and science

ABSTRACT

In an era where data security is paramount, this research explores innovative approaches to fortify information protection by combining state-of-the-art techniques in encryption and steganography. The conventional system primarily relies on the widely adopted Advanced Encryption Standard with Rivest-Shamir-Adleman (AES-RSA) encryption scheme, which, despite its robustness, exhibits certain drawbacks. These drawbacks include potential vulnerabilities in the RSA algorithm and limitations in the overall efficiency of the system. To address these concerns, the proposed system introduces a novel encryption mechanism, AES-FBC (Advanced Encryption Standard with Feistel Block Cipher), known for its enhanced security features and improved performance. Moreover, the integration of Discrete Wavelet Transform (DWT) steganography into the proposed system adds an additional layer of concealment, making it more resilient against potential attacks. The comprehensive analysis of the conventional system and its drawbacks sets the stage for the introduction of the proposed system, shedding light on the limitations of the existing methodology and the necessity for an advanced and more secure approach. The ensuing discussion delves into the technical intricacies of both encryption and steganography components, providing a detailed understanding of their functionalities and how they synergistically contribute to bolstering data security. The research culminates in a thorough evaluation of the proposed system through simulations and experiments, demonstrating its effectiveness in comparison to the conventional approach. The findings will underscore the significant advancements achieved in terms of data confidentiality and integrity, thereby establishing the proposed system as a robust and innovative solution for securing sensitive information in various digital environments.

Keywords: Medical Data Transmission, IoT, Communication System, Encryption, Steganography, Advanced Encryption Standard, AES-RSA, AES-FBC, Feistel Block Cipher, Discrete Wavelet Transform, Data Security, Vulnerabilities, Efficiency, Robustness, Concealment, Attacks.

1.INTRODUCTION

Securing data is a critical aspect of modern information management, given the increasing reliance on digital systems and the proliferation of cyber threats. Data security encompasses a range of measures designed to protect information from unauthorized access, disclosure, alteration, or destruction. One fundamental aspect of securing data involves implementing robust authentication and access controls. This ensures that only authorized individuals or systems have the requisite permissions to access sensitive information, thereby reducing the risk of unauthorized breaches. The primary research in hiding data started with steganography, which refers to the science and art of hiding information within an image. The benefit of steganography is that it can be utilized to transmit classified messages without

the fact of the transmission being detected. The DWT has a tremendous spatial localization, frequency spread, and multi-resolution characteristics, which are matching with the theory of forms in the human visual system. This paper implements both 1-level and 2-level of DWT steganography techniques that operate on the frequency domain. It split up the image into high and low iteration parts. The high iteration part contains edge information, whereas the low iteration part is frequently divided into high and low iteration parts. Furthermore, there are still limited methods of concealing information for use with data transfer communication protocols, which can be unconventional but their future is promising. Aims to improve the security of medical data transmission based on the integration between a steganography technique and a hybrid encryption scheme to get a highly secured healthcare system. The increasing integration of Internet of Things (IoT) devices in healthcare has revolutionized the monitoring and transmission of medical data. However, this surge in connectivity has brought forth a critical challenge – the security of sensitive medical information during transmission. Current cryptographic methods, though effective, often prove cumbersome for the resource-constrained nature of many IoT devices commonly used in healthcare settings. This presents a pressing need for the development of lightweight cryptographic solutions tailored to the specific requirements of secure medical data transmission in IoT-powered communication systems. The successful development and implementation of such a solution will contribute significantly to advancing the secure transmission of medical data in the rapidly evolving landscape of healthcare IoT communication. The research objective of their proposed project is to develop a robust and lightweight cryptographic solution for ensuring the secure transmission of medical data in IoT-powered communication systems. The primary focus is on addressing the unique challenges posed by resource-constrained IoT devices, emphasizing efficient encryption algorithms like Advanced Encryption Standard (AES) or lightweight alternatives. The key objectives include implementing dynamic key generation mechanisms for enhanced security, establishing secure communication channels using protocols like Transport Layer Security (TLS), and integrating authentication measures to verify the identity of IoT devices. Additionally, the project aims to incorporate privacy-preserving techniques, such as data anonymization, to comply with healthcare regulations while maintaining the confidentiality, integrity, and authenticity of sensitive medical information throughout the transmission process.

2.LITERATURE SURVEY

2.1 Introduction

In an era dominated by digital advancements and widespread connectivity, the protection of sensitive information has become paramount. Secure data, referring to the safeguarding of digital information from unauthorized access, alteration, or destruction, has emerged as a critical concern for individuals, businesses, and governments alike. As organizations increasingly rely on digital platforms to store and manage vast amounts of data, ensuring its security has become a complex and multifaceted challenge.

The importance of secure data transcends mere privacy concerns; it is integral to maintaining trust and integrity in various sectors. Cyber threats, ranging from sophisticated hacking attempts to ransomware attacks, underscore the need for robust measures to safeguard data. Security protocols encompass encryption, access controls, firewalls, and other sophisticated technologies designed to fortify data against potential breaches. Beyond technological aspects, a comprehensive approach to secure data also involves educating users about best practices, implementing regular audits, and staying abreast of evolving cyber threats. As the digital landscape continues to evolve, the pursuit of secure data remains a dynamic and ongoing endeavor to fortify the foundations of our interconnected world.

2.2 Related Work

Suyel Namasudra, et.al [1] proposed a scheme that can establish a secure session between an authorized device and a gateway, and prevent unauthorized devices from getting access to healthcare systems. The security analysis and performance analysis assess they proposed authentication technique's effectiveness over existing well-known schemes.

Pesaru, et.al [2] survey mainly focuses on a lightweight cryptography-based data hiding (LWC-DH) system, which is developed by combining LWC approaches with a steganography model for securing medical data. Initially, medical data is divided into even and odd characters, where even characters are encrypted using elliptic curve cryptography (ECC) and odd characters are encrypted using Feistel block cipher (FBC) cryptography. Then, redundant discrete wavelet transforms (RDWT) based steganography is applied for hiding the encrypted message in the cover image. The simulation results show that the proposed LWC-DH system performs superior in terms of peak signal-to-noise ratio (PSNR), structural similarity (SSIM) index, and mean square error (MSE) as compared to state-of-the-art approaches. In addition, they proposed LWC-DH system also produces low computation time as compared to conventional cryptography approaches.

S.Emalda Roslin et.al [3] surveyed towards obtaining a tradeoff between security, cost and performance of IoT based application.

Almulhim, et.al [4] proposed a scheme with a feature of the group-based node will reduce distance and consumed energy, as well as leads to reduce communication cost. In addition, it will be resistant against hacks by using elliptic curve cryptography (ECC). this will provide many advantages like cost saving, transportation, and insurance costs and health care provider. Therefore, this will lead to achieve the goal of facilitating secure interactions among healthcare providers and patient, which leads to better quality of healthcare, and save the time of patients. E-health applications are an exhibition to hack data and increasing issues at issues in security aspects due to rising a number of access points and critical data through E-medical records as well as the growing of use wearable technology. So, one of the main issues of IoT is the high level of security that needed to keep all communications secured.

Tianhe Gong, Ning Ye, et.al [5] survey involves the HES groups of send-receive model scheme to realize key distribution and secure data transmission, the homomorphic encryption based on matrix scheme to ensure privacy, and an expert system able to analyze the scrambled medical data and feedback the results automatically. Theoretical and experimental evaluations are conducted to demonstrate the security, privacy, and improved performance of HES compared with current systems or schemes. Finally, the prototype implementation of HES is explored to verify its feasibility.

Chunming Tang,et.al[6] proposed a system that enables distributed access control of protected health information (PHI) among different medical domains. On the other hand, the accumulation of electronic health records (EHR) makes effective data retrieval a challenge task. Their scheme could provide efficient keyword search function on cross-domain PHI. For the resource limited devices in health IoT, it is an essential requirement to design lightweight algorithms in the secure data management system. They proposed system realizes lightweight data encryption, lightweight keyword trapdoor generation and lightweight data recovery, which leaves very few computations to user's terminal. The security of this system is reduced to the decisional bilinear Diffie-Hellman (DBDH) assumption. The comparison analysis is made between this scheme and other existing systems. The extensive experiments on both laptop and smart phone platforms show that their proposed scheme has greatly improved the computation efficiency and requires much less communication cost.

Senthil Murugan, et.al [7] proposed a scheme that is more secure against various known attacks, such as denial of service, router attack, and sensor attacks. This proposed system has better resistance protocols in analyzing the safety of patients.

Mohammad Tabrez Quasim, et.al [8] proposed a secure framework, first, the task starts with the patient authentication, after that the sensors device linked to the patient is activated and the sensor values of the patient are transmitted to the cloud server. The patient's biometrics information has been added as a parameter in addition to the user name and password. The authentication scheme is coined with the SHA-512 algorithm that ensures integrity. To securely send the sensor information, the method follows two kinds of encryption: Substitution-Ceaser cipher and improved Elliptical Curve Cryptography (IECC). Whereas in improved ECC, an additional key (secret key) is generated to enhance the system's security. In this way, the intricacy of the two phases is augmented. The computational cost of the scheme in their proposed framework is 4H + Ec + Dc which is less than the existing schemes. The average correlation coefficient value is about 0.045 which is close to zero shows the strength of the algorithm. The obtained encryption and decryption time are 1.032 μs and 1.004μs respectively. The overall performance is analyzed by comparing their proposed improved ECC with existing Rivest-Shamir-Adleman (RSA)and ECC algorithms.

3.PROPOSED METHOD

Internet of Things (IoT) creates an integrated communication environment of interconnected devices and platforms by engaging both virtual and physical world together. With the advent of remote digital healthcare based IoT systems, the transmission of medical data becomes a daily routine. Therefore, it is necessary to develop an efficient model to ensure the security and integrity of the patient's diagnostic data transmitted and received from IoT environment. This goal is carried out using steganography techniques and system encryption algorithms together to hide digital information in an image. On the other hand, due to the significant advancement of the IoT in the healthcare sector, the security, and the integrity of the medical data became big challenges for healthcare services applications. Figure 1 shows the proposed block diagram. This work proposes a hybrid and lightweight security model for securing the diagnostic text data in medical images. The proposed model is developed through integrating 2-D discrete wavelet transform steganography technique with a proposed hybrid encryption scheme. The proposed hybrid encryption schema is built using a combination of Advanced Encryption Standard (AES), and Feistel encryption algorithms.

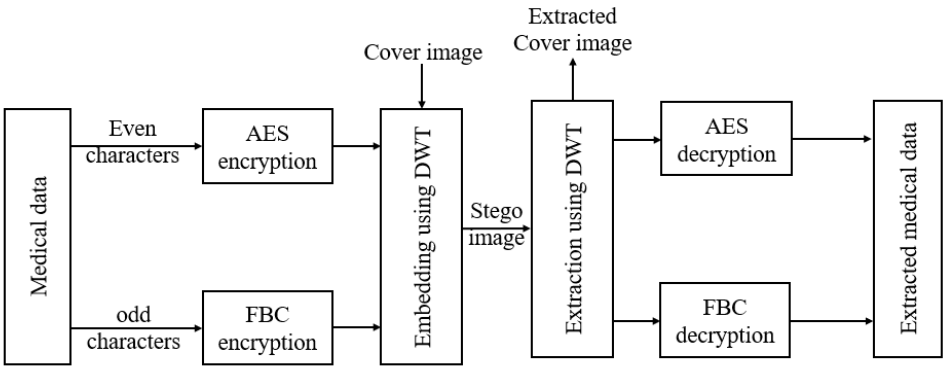


Figure 3.1.1. Proposed block diagram.

3.1 AES

The Advanced Encryption Standard (AES) is most popular and used across worldwide as encryption algorithm for data security. AES is a symmetric key algorithm from Rijndael family developed by Vincent Rijmen and Joan Daemen and established by U.S. National Institute of Standards and

Technology (NIST) in 2001. Symmetric algorithm means, it uses same key for both encryption and decryption. It is proposed to replace the encryption algorithm Data Encryption Standard (DES), which has small key length and more vulnerable to attacks. AES provides stronger encryption and faster in execution. AES encryption and decryption involves series of interlinked operations for N number of rounds with slight change in last, first round of encryption and decryption respectively. The number of rounds (N) is depends on the key length. AES ciphers uses block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. The number of rounds performed for 128 bit key is 10, for 192 bit key is 12 and for 256 bit key is 14. AES performs all its operations by considering the data as bytes, the data should be arranged in symmetrical matrix form. The encryption and decryption process of the AES is shown as a flow chart in figure.2.

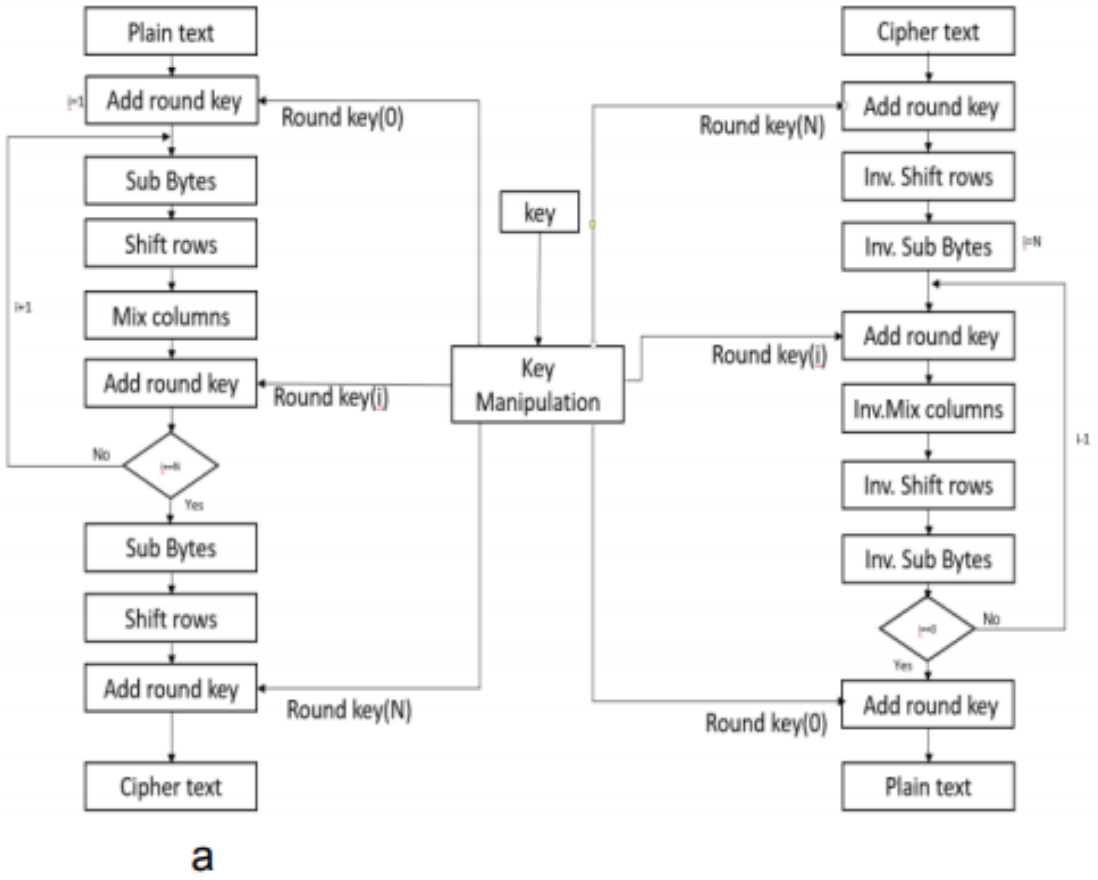


Fig 3.1.2. Flow diagram of AES Crypto Processor: a) Encryption b) Decryption

AES is based on a design principle known as a substitution-permutation network. It is fast in both software and hardware.[6] Unlike its predecessor, DES, AES does not use a Feistel network. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The blocksize has a maximum of 256 bits, but the keysize has no theoretical maximum. AES operates on a 4×4 column-major order matrix of bytes, termed the *state* (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field.

The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including

one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

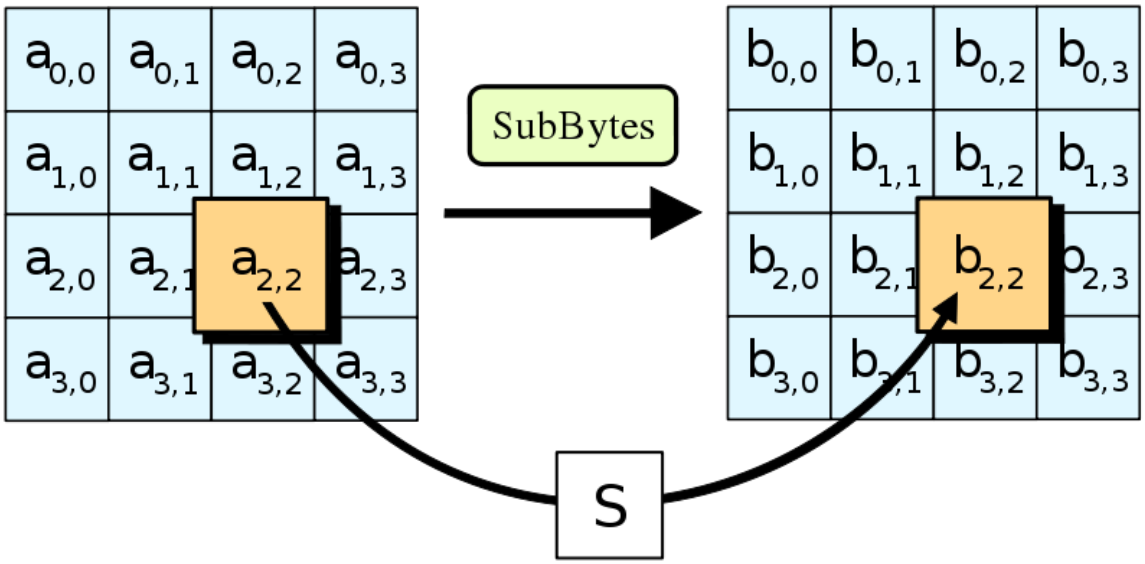
High-level description of the algorithm:

1. KeyExpansion—round keys are derived from the cipher key using Rijndael's key schedule
2. Initial Round
    1. AddRoundKey—each byte of the state is combined with the round key using bitwise xor
3. Rounds
    1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
    3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. AddRoundKey
4. Final Round (no MixColumns)
    1. SubBytes
    2. ShiftRows
    3. AddRoundKe

The Sub Bytes step:

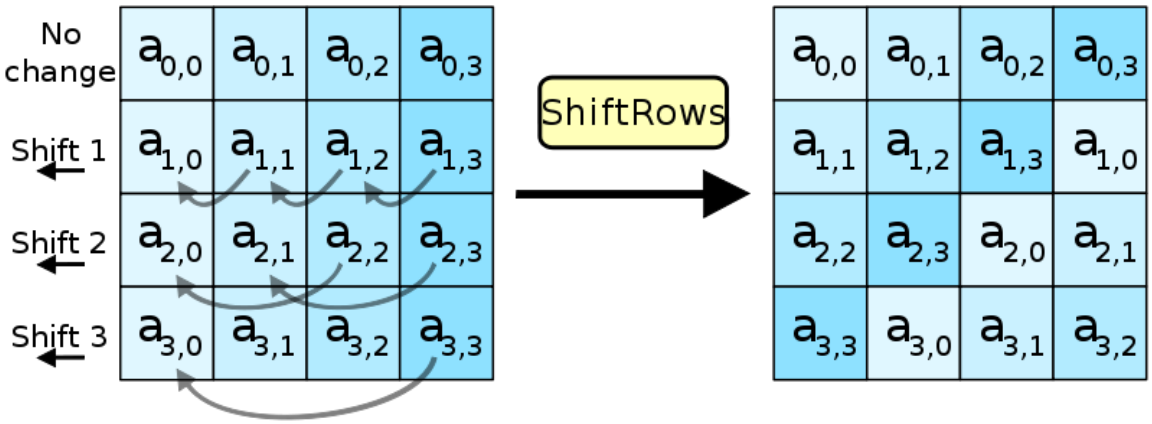
In the Sub Bytes step, each byte in the matrix is updated using an 8-bit substitution box, the Rijndael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over **GF**(2^8), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen The S-box is also chosen to avoid any

fixed points (and so is a derangement), and also any opposite fixed points.



ShiftRows step:

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first ro33w is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For the block of size 128 bits and 192 bits the shifting pattern is the same. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state. (Rijndael variants with a larger block size have slightly different offsets). In the case of the 256-bit block, the first row is unchanged and the shifting for second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively—this change only applies for the Rijndael cipher when used with a 256-bit block, as AES does not use 256-bit blocks.



Mix Columns step:

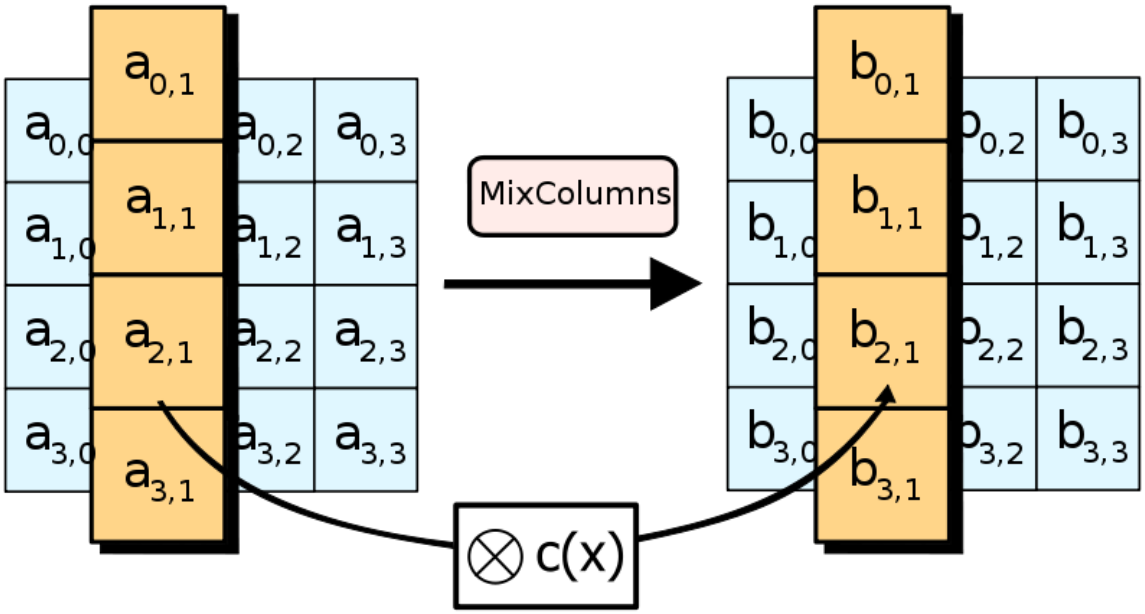
In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation. TheMixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together withShiftRows, MixColumns provides diffusion in the cipher.

During this operation, each column is multiplied by the known matrix that for the 128 bit key is

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}.$$

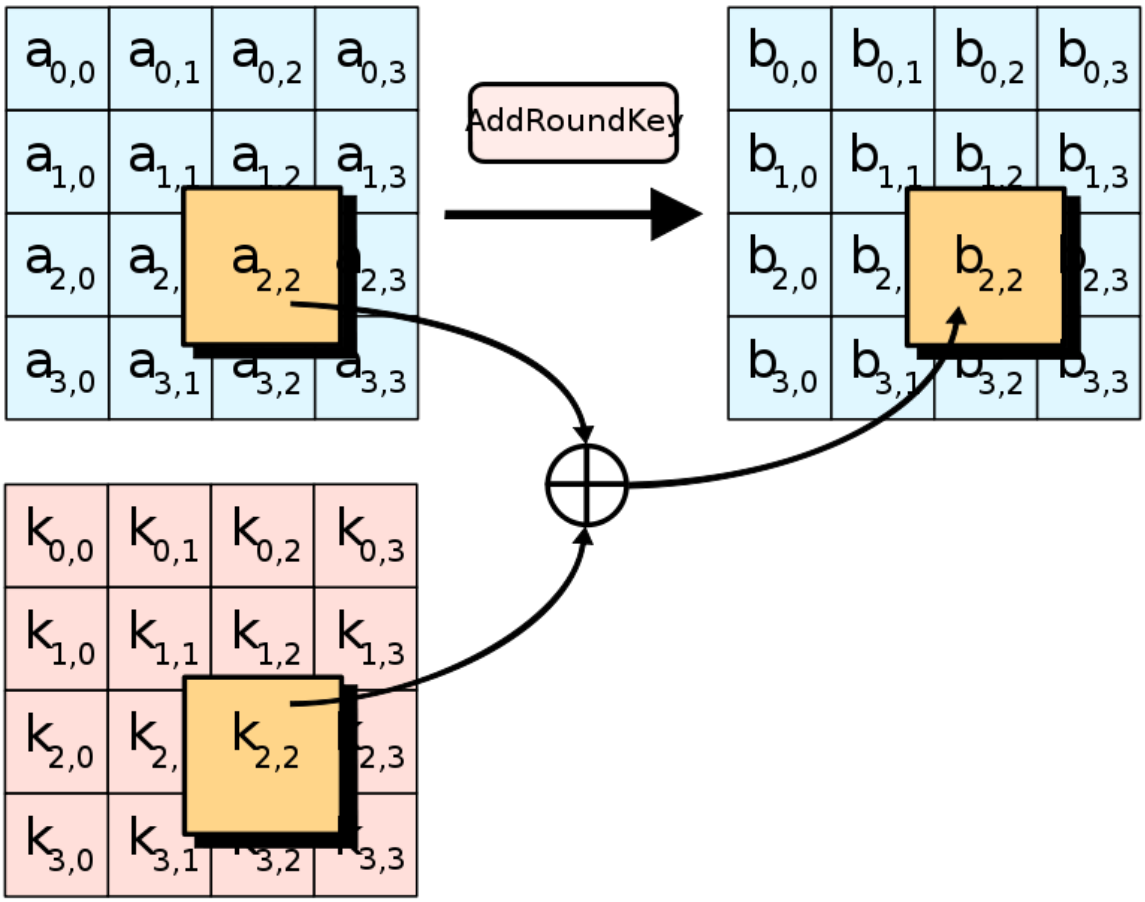
The multiplication operation is defined as: multiplication by 1 means leaving unchanged, multiplication by 2 means shifting byte to the left and multiplication by 3 means shifting to the left and then performing xor with the initial unshifted value. After shifting, a conditional xor with 0x1B should be performed if the shifted value is larger than 0xFF.

In more general sense, each column is treated as a polynomial over **GF**(2^8) and is then multiplied modulo x^4+1 with a fixed polynomial $c(x) = 0x03 \cdot x^3 + x^2 + x + 0x02$. The coefficients are displayed in their hexadecimal equivalent of the binary representation of bit polynomials from **GF**(2)[x]. The MixColumns step can also be viewed as a multiplication by a particular MDS matrix in a finite field. This process is described further in the article Rijndael mix columns.



Add Round Key step:

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.



3.2 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 $i = 1, 2, \ldots, n$, a new left half part and new right half part are generated according to the rules as follows:

$$L_i = R_{i-1} \quad (1)$$

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

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.

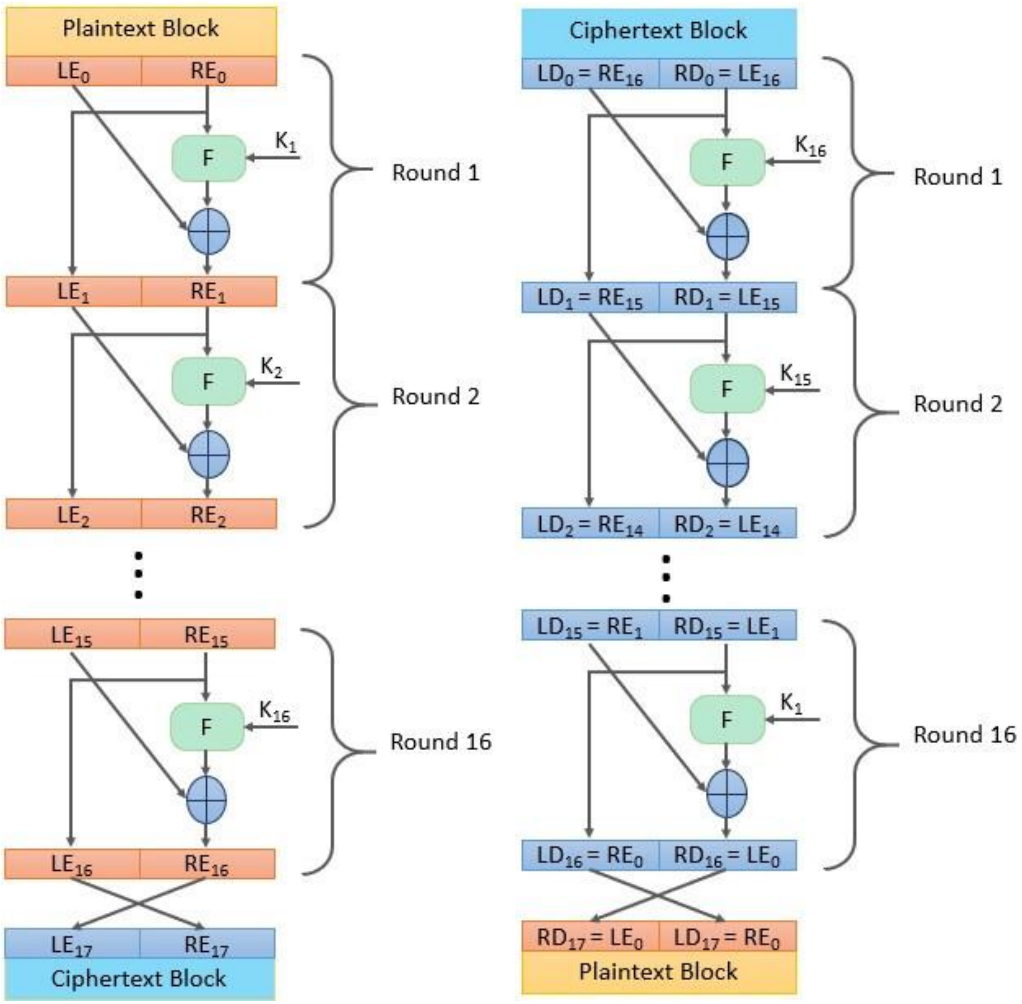
In step two, the plain text block is separated into two equal halves, denoted by the letters RE_0 for the right half of the plain text block and LE_0 for the left half of the plain text block. Now, LE_0 and RE_0 are subjected to a number of rounds of ciphering in order to generate the ciphertext block.

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. On the other hand, 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.



(a) (b)

Figure 3.2.1. FBC process (a) encryption, (b) decryption

3.3 DWT

A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time).

Definition:

One level of the transform

The DWT of a signal *x* is calculated by passing it through a series of filters. First the samples are passed through a low pass filter with impulse response*g* resulting in a convolution of the two:

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

The signal is also decomposed simultaneously using a high-pass filter*h*. the outputs giving the detail coefficients (from the high-pass filter) and approximation coefficients (from the low-pass). It is important that the two filters are related to each other and they are known as a quadrature mirror filter.

However, since half the frequencies of the signal have now been removed, half the samples can be discarded according to Nyquist's rule. The filter outputs are then sub sampled by 2 (Mallat's and the common notation is the opposite, g- high pass and h- low pass):

$$y_{\text{low}}[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n-k]$$

$$y_{\text{high}}[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n-k]$$

This decomposition has halved the time resolution since only half of each filter output characterizes the signal. However, each output has half the frequency band of the input so the frequency resolution has been doubled.

Examples:

Haar wavelets:

The first DWT was invented by the Hungarian mathematician Alfred Haar. For an input represented by a list of 2^n numbers, the Haar wavelet transform may be considered to simply pair up input values, storing the difference and passing the sum.

This process is repeated recursively, pairing up the sums to provide the next scale: finally resulting in $2^n - 1$ differences and one final sum.

Daubechies wavelets

The most commonly used set of discrete wavelet transforms was formulated by the Belgian mathematician Ingrid Daubechies in 1988. This formulation is based on the use of recurrence relations to generate progressively finer discrete samplings of an implicit mother wavelet function; each resolution is twice that of the previous scale. In her seminal paper, Daubechies derives a family of wavelets, the first of which is the Haar wavelet. Interest in this field has exploded since then, and many variations of Daubechies' original wavelets were developed.

Calculating wavelet coefficients at every possible scale is a fair amount of work, and it generates an awful lot of data. What if we choose only a subset of scales and positions at which to make our calculations?

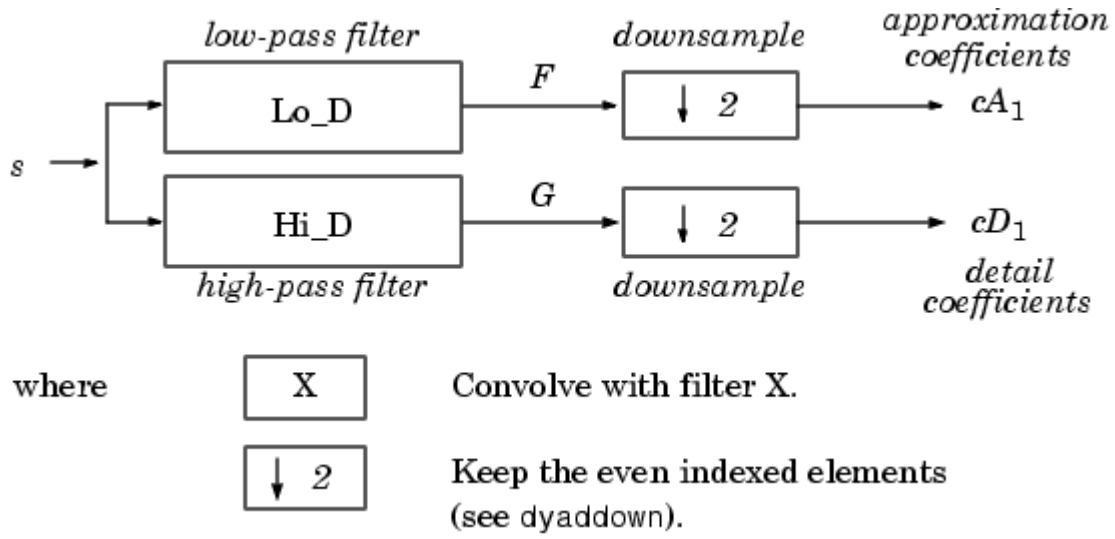
It turns out, rather remarkably, that if we choose scales and positions based on powers of two -- so-called dyadic scales and positions -- then our analysis will be much more efficient and just as accurate. We obtain such an analysis from the discrete wavelet transform (DWT).

An efficient way to implement this scheme using filters was developed in 1988 by Mallat. The Mallat algorithm is in fact a classical scheme known in the signal processing community as a two-channel sub band coder. This very practical filtering algorithm yields a fast wavelet transform -- a box into which a signal passes, and out of which wavelet coefficients quickly emerge.

Given a signal s of length N, the DWT consists of log2N stages at most. Starting from s, the first step produces two sets of coefficients: approximation coefficients cA1, and detail coefficients cD1.

These vectors are obtained by convolving s with the low-pass filter Lo_ D for approximation, and with the high-pass filter Hi_ D for detail, followed by dyadic decimation.

More precisely, the first step is



The length of each filter is equal to 2N. If n = length (s), the signals F and G are of length

n + 2N - 1, and then the coefficients cA1 and cD1 are of length

$$\text{floor}\left(\frac{n-1}{2}\right)+N$$

The next step splits the approximation coefficients cA1 in two parts using the same scheme, replacing s by cA1 and producing cA2 and cD2, and so on.

Applications of discrete wavelet transform:

Generally, an approximation to DWT is used for data compression if signal is already sampled, and the CWT for signal analysis. Thus, DWT approximation is commonly used in engineering and computer science, and the CWT in scientific research.

Wavelet transforms are now being adopted for a vast number of applications, often replacing the conventional Fourier Transform. Many areas of physics have seen this paradigm shift, including molecular dynamics, astrophysics, density-matrix localization, seismology, optics, turbulence and quantum mechanics. This change has also occurred in image processing, blood-pressure, heart-rate and ECG analyses, DNA analysis, protein analysis, climatology, general signal processing, speech recognition, computer graphics and multi fractal analysis. In computer vision and image processing, the notion of scale-space representation and Gaussian derivative operators is regarded as a canonical multi-scale representation.

One use of wavelet approximation is in data compression. Like some other transforms, wavelet transforms can be used to transform data, then encode the transformed data, resulting in effective compression. For example, JPEG 2000 is an image compression standard that uses bi-orthogonal wavelets. This means that although the frame is over complete, it is a tight frame, and the same frame functions (except for conjugation in the case of complex wavelets) are used for both analysis and synthesis, i.e., in both the forward and inverse transform. For details see wavelet compression.

A related use is for smoothing/de-noising data based on wavelet coefficient thresholding, also called wavelet shrinkage. By adaptively thresholding the wavelet coefficients that correspond to undesired frequency components smoothing and/or de-noising operations can be performed.

4.SIMULATION RESULTS

The invisibility and robustness of the suggested technique are examined in this section. To begin, the best adaptive scaling factor for watermarks with different sizes is determined by analyzing the scaling factor across NC, PSNR, and SSIM. In the trials, the adaptive optimum scaling factors of watermarks with different sizes are employed. Subjective eye observation and objective quantitative analysis are used to detect the suggested method's invisibility and resilience. Furthermore, a variety of assaults with varying characteristics are employed to test the resilience. Finally, the suggested method's invisibility and robustness are compared to previous studies.

To run project double click on 'run.bat' file to get below screen

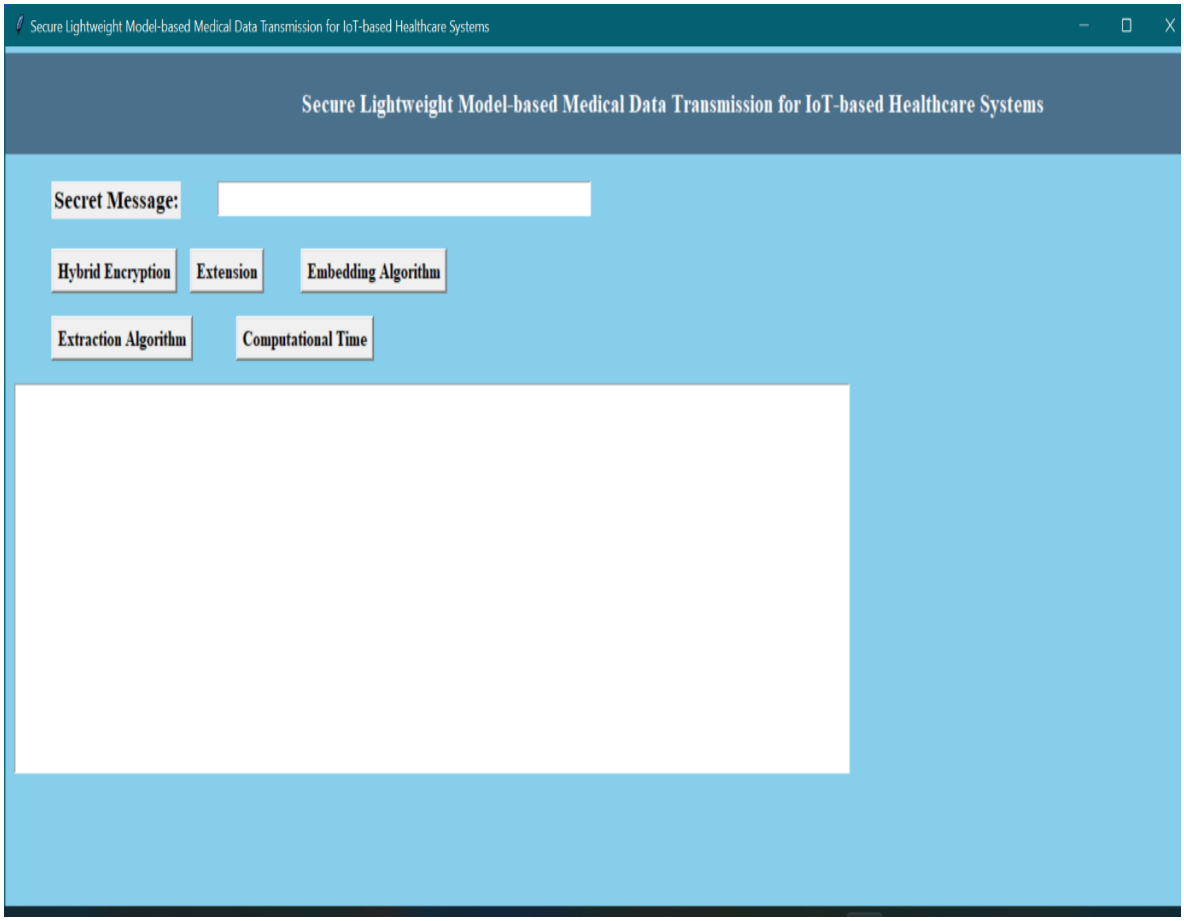


Fig 4.1: Secure Light Weight model based medical data Transmission for IOT based HealthCare System.

In above screen enter some message in 'Secret Message' field Ensuring secure transmission, a lightweight model safeguards medical data in IoT healthcare systems, prioritizing efficiency and privacy in information exchange.

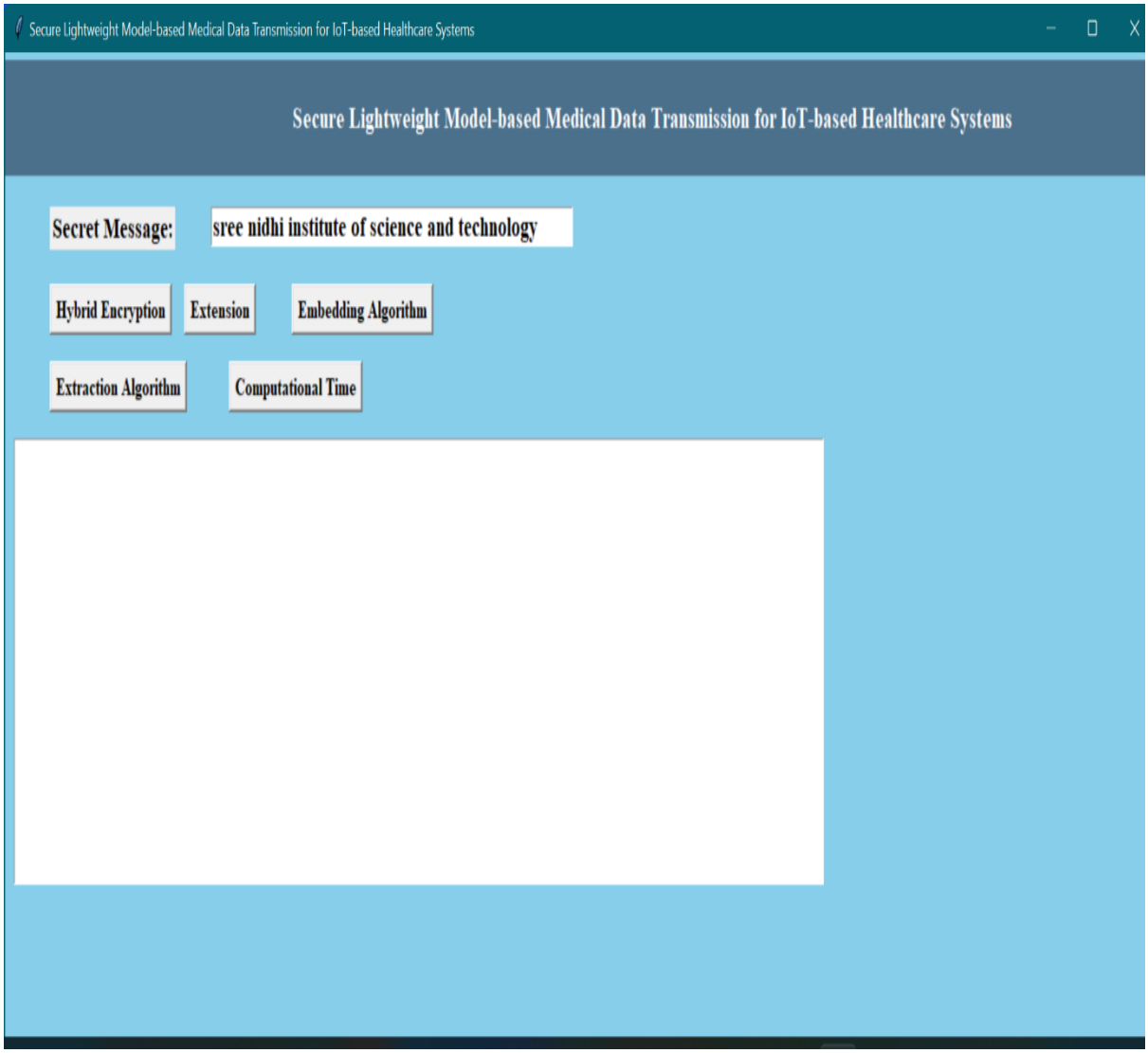


Fig 4.2: To check the process enter any message

In above screen, we have entered some message and then click on 'Hybrid Encryption' button to encrypt message using AES and RSA encryption. Hybrid encryption combines the efficiency of AES and the security of RSA. AES encrypts the message, and RSA encrypts the AES key, providing a robust dual-layer protection for secure communication.

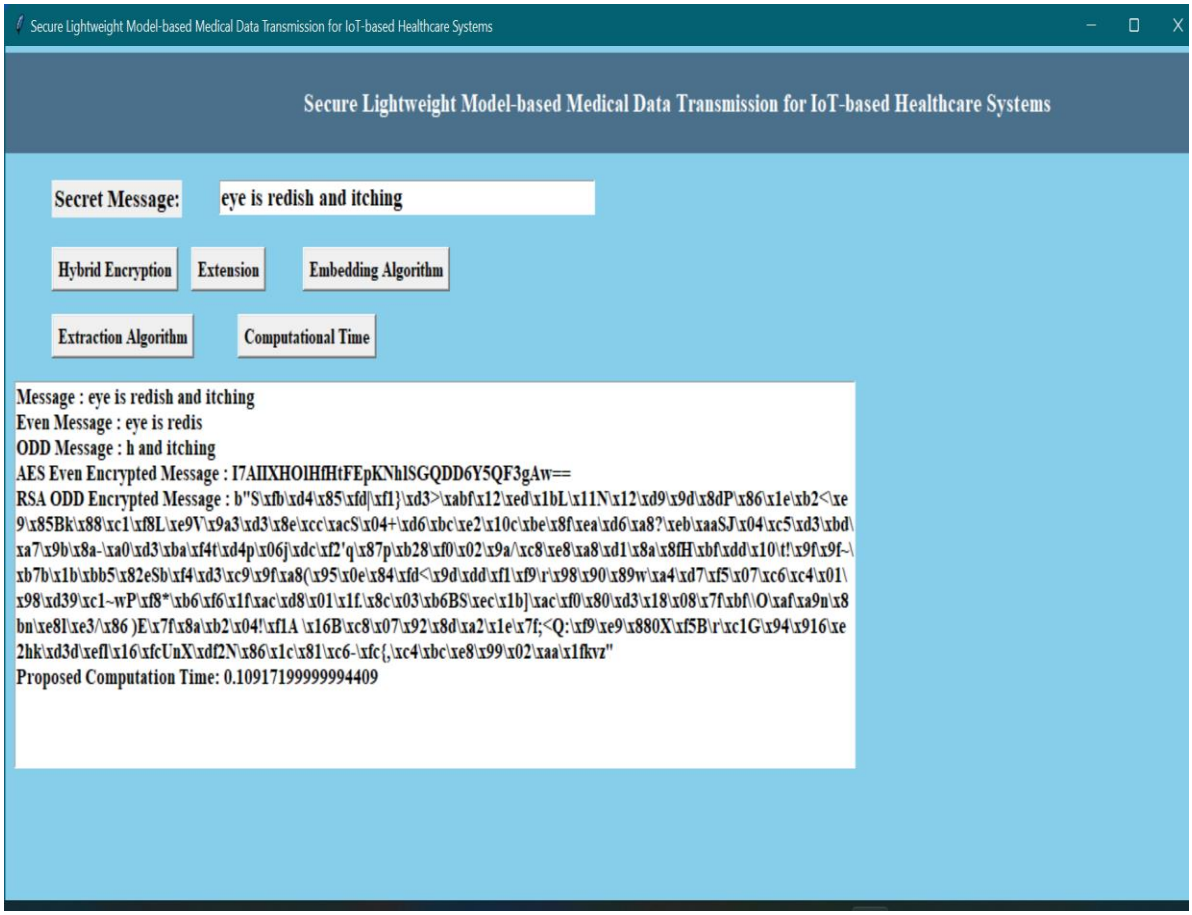


Fig 4.3: Hybrid Encryption of the message using AES and RSA encryption

In above screen, we can see the encrypted odd and even messages using hybrid encryption AES-RSA algorithm. Now click on 'Extension' button to encrypt message using AES and Feistel encryption. Extending the encrypted message involves utilizing AES for data encryption and the Fiestel network for further cryptographic processing. This combination enhances security by employing a multi-round structure for robust and efficient encryption in communication systems.

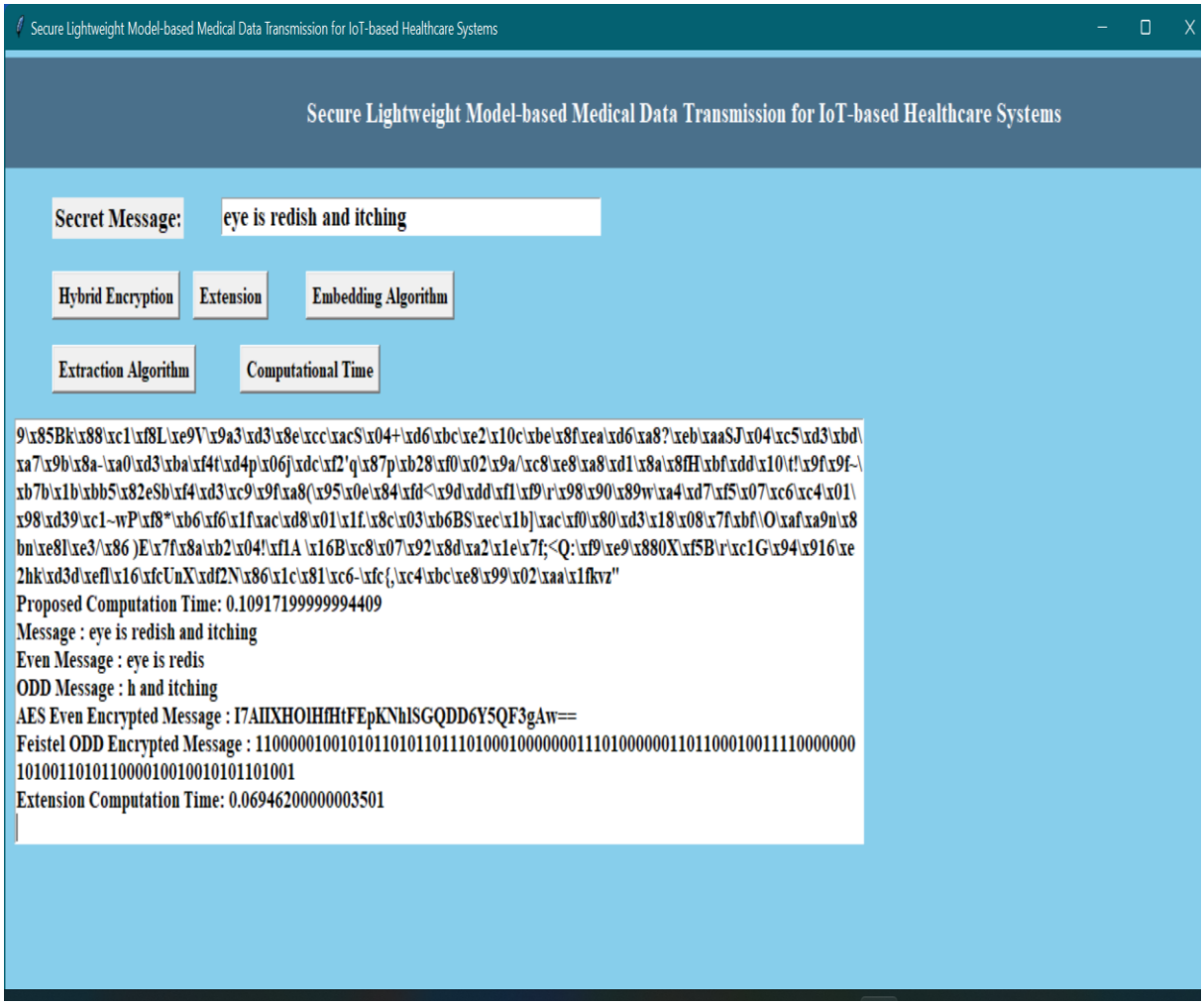


Fig 4.4: Extension of the encrypted message using AES and Fiestel encryption

In above screen displaying complete message with ODD and EVEN parts and then encrypting both parts with AES and Feistel encryption. Now message is ready and now click on 'Embedding Algorithm' button to upload image and then hide that encrypted message. This process involves strategically altering the pixel values or color channels in the image to conceal the encrypted data without visibly affecting the overall appearance. The hidden message can be extracted later using a corresponding extraction algorithm and the appropriate decryption key.

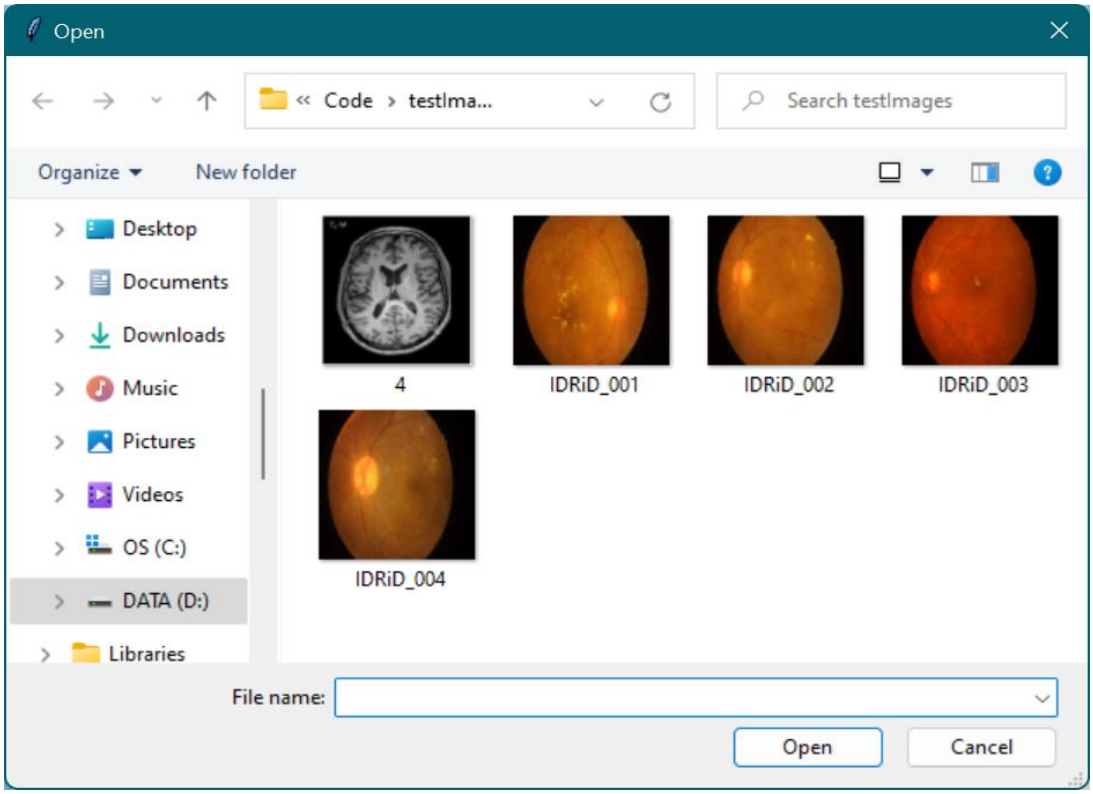


Fig 4.5: Embedding Algorithm to upload image and to hide encryption message

In above screen I am selecting one image and it has both colour and grey images and now click on 'Open' button to get below output.

Fig 4.6: Original Image

Fig 4.7: Stego Image

In above screen first image is the original image and second image contains steganography hidden message and both messages look similar in visual quality. Now close the both images to get below histogram graph of both images.

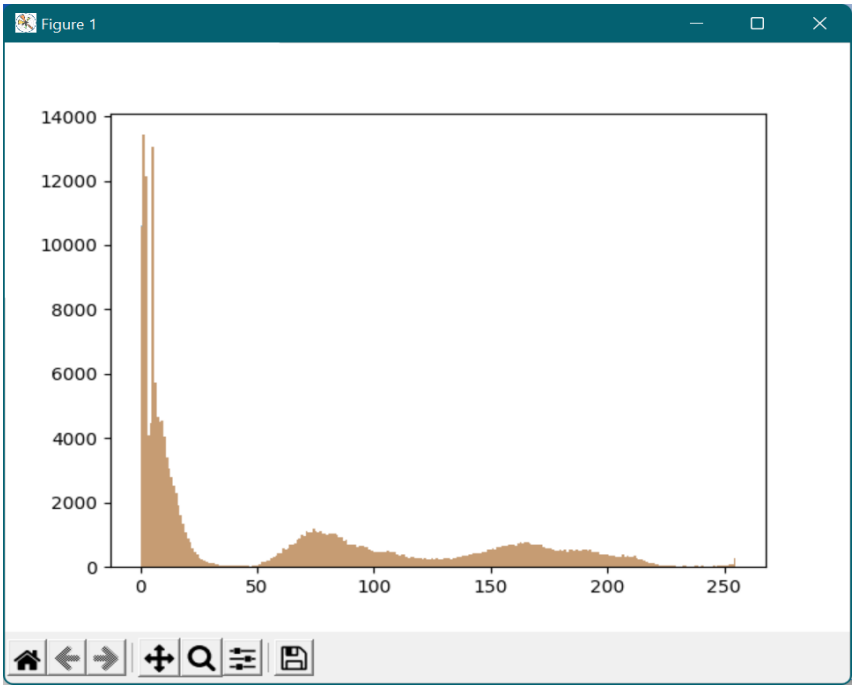


Fig 4.8: Histogram graph

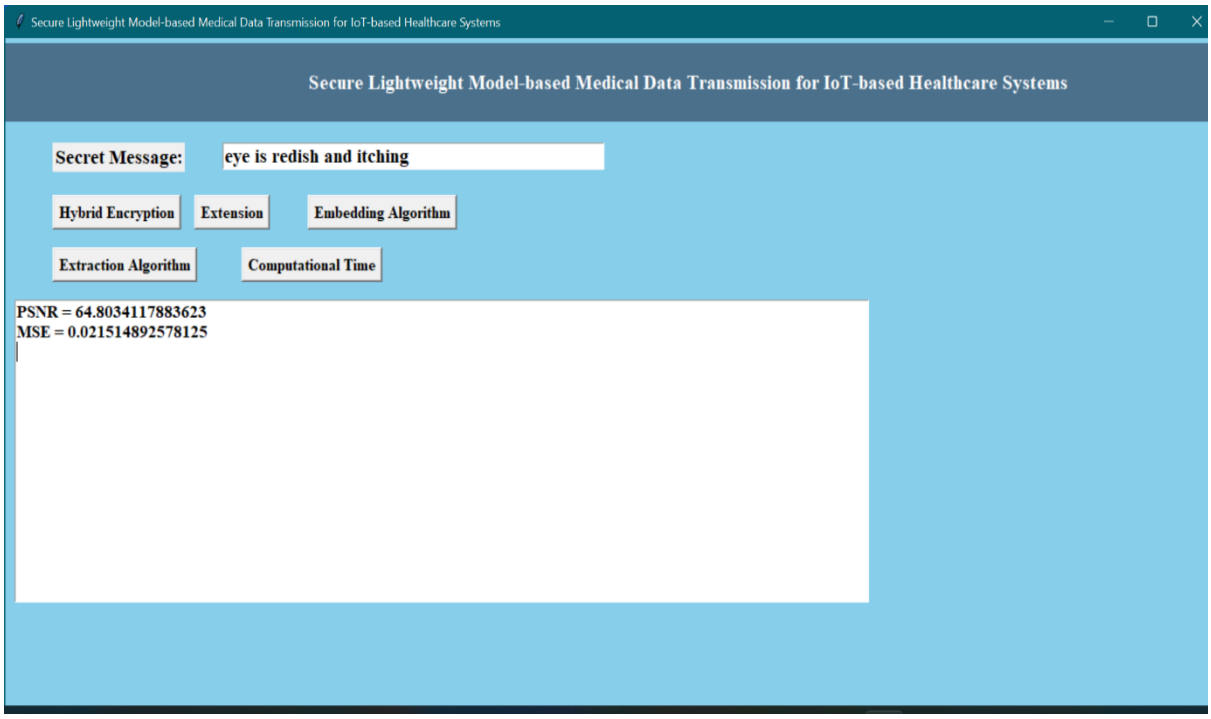


Fig 4.9: Extraction algorithm to extract and decrypt message from image.

In above histogram we can see both images are showing equal size bars show after hiding message not much change we can see in Steg image and in above screen in text area we got PSNR as 64.8% and MSE 0.027. Similarly, you can upload other images and test. Now click on 'Extraction Algorithm' button to extract and decrypt message from image.

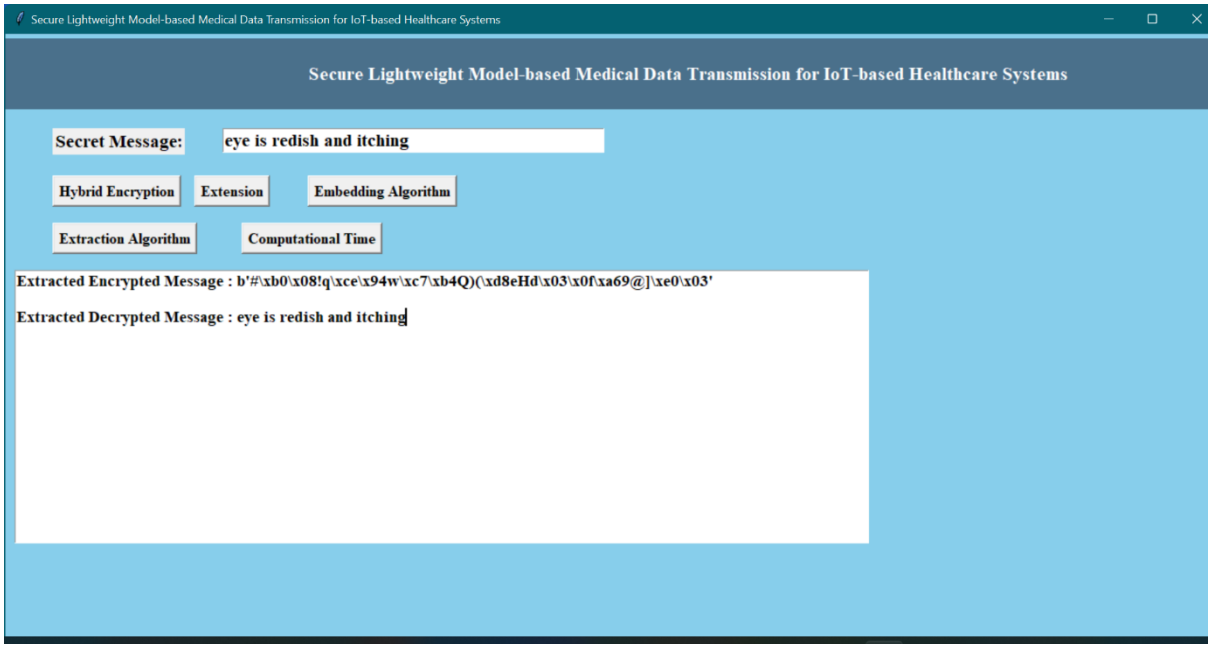


Fig 4.10. To get original data extracted decrypted message

In above screen in text area, To recover the original image from the encrypted message, one needs the correct decryption key and algorithm to reverse the encoding process, unveiling the concealed content. This cryptographic technique ensures the confidentiality and integrity of sensitive information during transmission or storage.

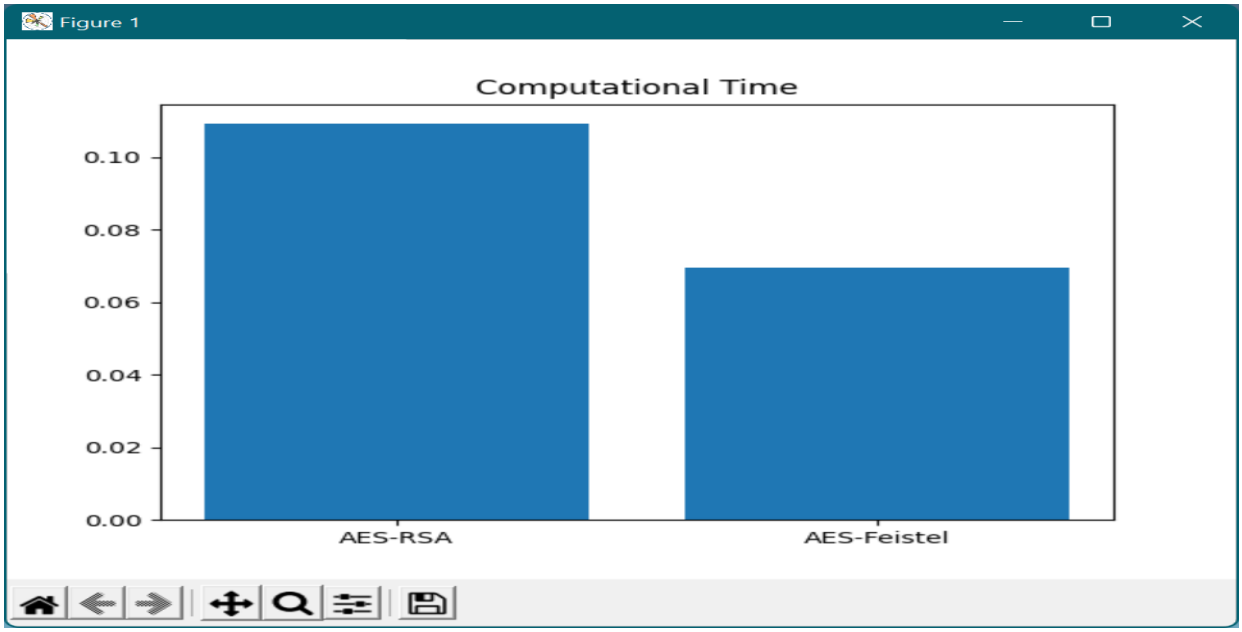


Fig 4.11: Computational Time by using bar graph

5.CONCLUSION

For a healthcare-based IoT context, a secure patient diagnostic data transfer model employing both colour and gray-scale pictures as a cover carrier has been proposed. The suggested model used DWT steganography, as well as a mix of AES and FBC cryptography. In future research, the suggested steganography approach may need to pay more attention to repelling additional attacks, such as rotation

and cropping attacks. Furthermore, if the enhanced FOA method is used, the steganography performance may be increased even further.

REFERENCES

[1] Das, Sangjukta, and Suyel Namasudra. "Lightweight and efficient privacy-preserving mutual authentication scheme to secure internet of things-based smart healthcare." Transactions on Emerging Telecommunications Technologies (2023): e4716.

[2] Pesaru, Swetha, Naresh K. Mallenahalli, and B. Vishnu Vardhan. "Light weight cryptography-based data hiding system for Internet of Medical Things." International Journal of Healthcare Management (2022): 1-14.

[3] Rani, D. Jamuna, and S. Emalda Roslin. "Light weight cryptographic algorithms for medical internet of things (IoT)-a review." In 2016 Online international conference on green engineering and technologies (IC-GET), pp. 1-6. IEEE, 2016.

[4] Almulhim, Maria, Nazurl Islam, and Noor Zaman. "A lightweight and secure authentication scheme for IoT based e-health applications." International Journal of Computer Science and Network Security 19, no. 1 (2019): 107-120.

[5] Huang, Haiping, Tianhe Gong, Ning Ye, Ruchuan Wang, and Yi Dou. "Private and secured medical data transmission and analysis for wireless sensing healthcare system." IEEE Transactions on Industrial Informatics 13, no. 3 (2017): 1227-1237.

[6] Yang, Yang, Xianghan Zheng, and Chunming Tang. "Lightweight distributed secure data management system for health internet of things." Journal of Network and Computer Applications 89 (2017): 26-37.

[7] Nagarajan, Senthil Murugan, Ganesh Gopal Deverajan, U. Kumaran, M. Thirunavukkarasan, Mohammad Dahman Alshehri, and Salem Alkhalaf. "Secure data transmission in internet of medical things using RES-256 algorithm." IEEE Transactions on Industrial Informatics 18, no. 12 (2021): 8876-8884.

[8] Khan, Mohammad Ayoub, Mohammad Tabrez Quasim, Norah Saleh Alghamdi, and Mohammad Yahiya Khan. "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data." IEEE Access 8 (2020): 52018-52027.