Enhancing Data Security through Innovations in AES-FBC Encryption and DWT Steganography

A. Sneha[1], Y. Gowthami[2], SK. Shireen[2], Y. Soumya [2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science Engineering
[1,2]Malla Reddy Engineering College for Women, Maisammaguda, Dhulapally, Kompally, Secunderabad-500100, Telangana, India

ABSTRACT

The Internet of Medical Things (IoMT) refers to the interconnected network of medical devices and applications that collect, transmit, and exchange healthcare data over the internet. With the rapid advancement of technology, IoMT applications have become integral in modern healthcare, allowing for remote patient monitoring, real-time health data analysis, and improved medical services. However, the transmission of sensitive medical data over the internet raises significant security concerns. To address these concerns, lightweight cryptography (LWC) techniques are employed to secure medical data transmission in IoMT applications. LWC focuses on providing robust security with minimal computational and memory requirements. The need for secure medical data transmission in IoMT applications arises from the sensitive nature of healthcare information. Patient privacy, data integrity, and confidentiality must be ensured to maintain trust in healthcare systems. LWC addresses the need for efficient encryption and decryption processes, making it suitable for devices with limited processing power and memory. The problem lies in ensuring secure communication between medical devices and data repositories within IoMT applications. Traditional systems often rely on standard cryptographic algorithms, which, while secure, may be too resource intensive for IoMT devices. These devices, such as wearable sensors and implantable medical devices, have limited computational capabilities and battery life. As a result, implementing standard cryptographic protocols can lead to increased power consumption and latency issues. Therefore, this research aims to develop a system that employs LWC techniques to secure medical data transmission effectively while optimizing the use of resources. In addition, the proposed system adopts a hybrid security model for securing the diagnostic text data in medical images. The proposed model is developed through integrating Discrete Wavelet Transform (DWT)-based steganography technique with a hybrid LWC scheme. The proposed hybrid encryption schema is built using a combination of Advanced Encryption Standard (AES), and Feistel algorithms. It enables efficient, secure, and privacy-preserving communication, fostering the growth of innovative healthcare solutions in the era of digital transformation.

Keywords: DWT Steganography, AES-FBC Encryption, Enhancing Data Security.

1. INTRODUCTION

In recent years, the healthcare industry has shown rapid growth and has been a major contributor to revenue and employment. A few years ago, the diagnosis of diseases and abnormality in the human body was only being possible after having a physical analysis in the hospital. Most of the patients had to stay in the hospital throughout their treatment period. This resulted in an increased healthcare cost and also strained the healthcare facility at rural and remote locations. The technological advancement that has been achieved through these years has now allowed the diagnosis of various diseases and health monitoring using miniaturized devices like smartwatches. Moreover, technology has transformed a hospital-centric healthcare system into a patient-centric system. For example, several clinical analyses (such as measuring blood pressure, blood glucose level, pO_2, level, and so on) can be performed at home without the help of a healthcare professional. Further, the clinical data can be

communicated to healthcare centers from remote areas with the help of advanced telecommunication services. The use of such communication services in conjunction with the rapidly growing technologies (e.g., machine learning, big data analysis, Internet of things (IoT), wireless sensing, mobile computing, and cloud computing) has improved the accessibility of the healthcare facilities.

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.

IoT has not only enhanced the independence but also diversified the ability of the human to interact with the external environment. IoT, with help of futuristic protocol and algorithms, became a major contributor to global communication. It connects a large number of devices, wireless sensors, home appliances, and electronic devices to the Internet.The application of IoT can be found in the field of agriculture ,automobiles, home, and healthcare.

The growing popularity of the IoT is due to its advantage of showing higher accuracy, lower cost, and its ability to predict future events in a better way. Further, increased knowledge of software and applications, with the upgradation of mobile and computer technologies, easy availability of wireless technology, and the increased digital economy have added to the rapid IoT revolution.

The IoT devices (sensors, actuators, and so on) have been integrated with other physical devices to monitor and exchange information using different communication protocols such as Bluetooth, Zigbee, IEEE 802.11 (Wi-Fi), and so on. In healthcare applications, the sensors, either embedded or wearable on the human body, are used to collect physiological information such as temperature, pressure rate, electrocardiograph (ECG), electroencephalograph (EEG), and so on from the patient's body. Additionally, environmental information such as temperature, humidity, date, and time can also be recorded. These data help in making meaningful and precise inferences on the health conditions of the patients. Data storage and accessibility also play an important role in the IoT system as a large amount of data are acquired/recorded from a variety of sources (sensors, mobile phones, e-mail, software, and applications).

2. LITERATURE SURVEY

Related Work

Humayun, M., Jhanjhi, N. & Alamri, M. (2020). IoT-based Secure and Energy Efficient scheme for E-health applications. *Indian J Sci Technol*, *13*(28), 2833-2848.

Humayun, M., Jhanjhi, N., & Alamri,(2020)presented a secure and energy-efficient scheme of patient's data transmission from wearable IoT sensors (WIS) to base station (BS). IoT sensors are widely used in the healthcare domain for realtime data collection and transmission. However, these sensors are resource constrained in terms of computational power and storage due to which chances of security breaches and threats increase. Moreover, with time the energy level of IoT sensors also degrade that sometimes leads towards loss of sensitive patient data.

Almulhim, M., & Zaman, N. (2020, February). Proposing secure and lightweight authentication scheme for IoT based E-health applications. In *2018 20th International Conference on advanced communication technology (ICACT)* (pp. 481-487).

Almulhim, M., & Zaman, N.(2020) proposed a secure group-based lightweight authentication scheme for IoT based E-health applications, the proposed model will provide mutual authentication and

energy efficient, and computation for healthcare IoT based applications. Which will use elliptic curve cryptography (ECC) principles that provide mentioned featured of suggested model.

Mallikarjuna, B., Kiranmayee, D., Saritha, V., & Krishna, P. V. (2021, June). Development of efficient e-health records using iot and blockchain technology. In *ICC 2021-IEEE International Conference on Communications* (pp. 1-7). IEEE.

Mallikarjuna, B., Kiranmayee, D., Saritha, V., & Krishna, P. V.(2021) proposed the approach tested with the NodeJs software and ApacheJmeter open source JMeter Cloud Test environment and proved that the simulation-results of BEHR are an efficient approach in response time and file storage and transmission of EHR than the present conventional system.

Amare & Vuda (2021) proposed an improvement on the regular RSA algorithm such that two public keys are generated during the key generation process and these two public keys are used simultaneously instead of one as against the regular RSA cryptographic algorithm. In this scenario the public key is sent separately twice as against the traditional RSA algorithm where the public key is sent once. This makes the attacker ignorant about the key being used for encryption and thus is unable to decrypt the message. In some cases if the attacker with malicious intentions is able to intercept the sending process of both public keys, the attacker can use both public keys to decipher the encoded message.

Sarath Sabu, Swaraj Hegde et.al Global Transitions Proceedings 2 (2), 429-433, 2021

The secure and privacy aware E-Health record to propose a mechanism using blockchain and IPFS (InterPlanetary File System) which offers a solution to all these problems. It also includes limitations and safeguards on what can be done and cannot be done with your personal information in some cases. The IPFS data will be dispersed among the nodes. Use of IPFS (Interplanetary File System) to store health records, which has the benefit of being distributed which in turn makes record tamper-free.

Bairagi et al.(2019) proposed three color image steganography approaches for protecting information in an IoT infrastructure. The first and third approaches use three (red, green, and blue) channels, while the second approach uses two (green and blue) channels for carrying information. Dynamic positioning techniques have been used for hiding information in the deeper layer of the image channels with the help a shared secret key.

Anwar et al.(2020) developed a technique to secure any type of images especially medical images. They aimed to maintain the integrity of electronic medical information, ensuring

availability of that information, and authentication of that information to ensure that authorized people only can access the information. First, the AES encryption technique was applied on the first part. The ear print also embedded in this work, where seven values were extracted as feature vector from the ear image. The proposed technique improved the security of medical images through sending them via the internet and secured these images from being accessed via any unauthorized person.

Abdelaziz et al.(2019) proposed the analysis of the security vulnerabilities and the risk factors detected in mobile medical apps. According to risk factor standards, these apps can be categorized into remote monitoring, diagnostic support, treatment support, medical information, education and awareness, and communication and training for healthcare workers. Eight security vulnerabilities and ten risks factors detected by the World Health Organization (OWASP) mobile security project in 2014 have been analyzed.

Razzaq et al.(2021)proposed a fused security approach based on encryption, steganography, and watermarking techniques. It decomposed into three stages:

(1) encrypting the cover image using XOR operation

(2) embedding process done using least significant bits (LSBs) for generating the stego-image

(3) watermarking the stego-image in both spatial and frequency domains. Experimental results proved that proposed method was very much efficient and secured.

Jain et al.(2019) proposed a new technique for transferring the patient's medical information into the medical cover image by hiding the data using decision tree concept. The coding is done in the form of different blocks that evenly distributed. In concealment, secret code blocks are assigned to the cover image to insert the data by the mapping mechanism based on breadth-first search. RSA algorithm was used to encipher the data before embeddings.

Yehia et al. (2020) surveyed various healthcare applications based on wireless medical sensor network (WMSN) that can be implemented in IoT environment. Also, discussed the security

techniques that used for handling the security issues of healthcare systems especially hybrid security techniques.

Farahat, AS Tolba, Mohamed Elhoseny, Waleed Eladrosy Security in smart cities: models, applications, and challenges, 117-142, 2019

Proposed system first compresses data with run-length encoding technique then encrypt it using the AES method but with a rotated key then the source transfers the encoded and encrypted data to the destination where the data is decrypted then decoded to restore the original data then the original data is upload to the destination's website.

Zaw and Phyo, **(2019)** presented a algorithm based on dividing the original image to the group of blocks, where these blocks are arranged in the form of turns using a transformation algorithm. After that, the transformed image is encryption using the Blowfish algorithm. It was found that the correlation decreases and the entropy increase by increasing the number of blocks through using smaller block sizes.

Amine Rghioui, Sandra Sendra, Jaime Lloret, Abedlmajid Oumnad Network Protocols and Algorithms 8 (3), 15-28, 2016.

Internet of things (IoT) is a new paradigm that combines several technologies such as computers, Internet, sensor networks, radio frequency identification (RFID), communication technology and embedded systems to form a system that links the real world with digital world. Currently, a large number of smart objects and different type of devices are interconnected and more and more they are being used in Ambient Assisted Living (AAL) scenarios for improving the daily tasks of elderly and disabled people. Presented an IoT architecture and protocol for Ambient Assisted Living and e-health. It is designed for heterogeneous AAL and e-health scenarios where an IoT network is the most suitable option to interconnect all elements.

Sreekutty and Baiju (2020) proposed a medical integrity verification system to improve the security of medical image. The proposed system mainly decomposed into two stages: 1) the protection and 2) the verification. Through the protection stage, the binary form of the secret data is embedded in the high-frequency part (HH) within the cover image using 2D Haar DWT frequency domain technique. Through the verification stage, the extraction algorithm is applied to retrieve the original cover image and secret data.

V Kanchana, Surendra Nath, Mahesh K SinghMaterials Today: Proceedings 51, 961-964, 2022

Presented a combined image of the most significant function as well as services obtainable by Health Monitoring System method(HMS) for the detecting and monitoring human behavior. It is counting its processing techniques, approaches and concepts etc. Furthermore, it is provided a general, in detail study and assessment of the obtainable research conclusion in the field of e-health systems through IoT.

Bashir et al.(2019) proposed an image encryption technique based on the integration of shifted image blocks and the basic AES. The shifted algorithm technique is used to divide the image into blocks. Each block consists of many pixels, and these blocks are shuffled by utilizing a shift technique that moves the rows and columns of the original image in such a way to produce a shifted image. This shifted image is then used as an input image to the AES algorithm to encrypt the pixels of the shifted image.

Muhammad et al.(2021) proposed an efficient, secure method for RGB images based on gray level modification (GLM) and multi-level encryption (MLE). The secret key and the secret data are encrypted using MLE algorithm before mapping it to the gray-levels of the cover image. Then, a transposition function is applied to the cover image before data hiding. The usage of transpose, secret key, MLE, and GLM adds four different levels of security to the proposed algorithm, making it very difficult for a malicious user to extract the original secret information.

Rihab Boussada, Balkis Hamdane, Mohamed Elhoucine Elhdhili, Leila Azouz Saidane

2019 IEEE Wireless Communications and Networking Conference (WCNC), 1-6, 2019

Data Networking (NDN) represents a promising future networking paradigm fitting perfectly with the requirements of IoT applications and especially those related to security and privacy. In this paper, we leverage the basic feats of NDN vision for designing a robust privacy preserving NDN-based e-health IoT system (PP-NDNoT). It ensures security and fulfills content and contextual privacy requirements.

Yin et al.(2020)proposed an image steganography approach based on Inverted LSB (ILSB) technique for securing the transmitted face images from the IP camera as the IoT device to the home server in the LAN network. The local home server serves as a processing power node for the encryption of the stego images before transmitting them to the cloud and other devices for further processing.

N Deepa, Perumal Pandiaraja Journal of Ambient Intelligence and Humanized Computing 12, 4877-4887, 2021

Proposed protocol is secure against some attacks like Eavesdropping, masquerade, replay and man in the middle attack. Our performance analysis section describes that our ERFC mechanism is better with communication as well as computation complexity when related to the other existing protocols.

Abdel-Nabi, H., et al.(2021) proposed a cryptowatermarking approach based on AES standard encryption algorithm and reversible watermarking data hiding technique to secure medical images. The results proved that the proposed approach achieves both the authenticity and integrity of the images either in the spatial domain or the encrypted domain or both domains.

Iuliana Chiuchisan, Iulian Chiuchisan, Mihai Dimian 2015 International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM), 1-5, 2015

Proposed a secure Internet of Things (IoT) and its applications to e-Health is presented along with a case study using the K53 Tower System platform for e-Health. This platform offers a broad range of technologies for body area network (BAN) measurements and communications in healthcare and other medical applications**.**

Seyyedi et al.(2020) proposed a secure steganography method based on encrypting the confidential information using the symmetric RC4 encryption method and embedding it within the cover image based on the partitioning approach with minimal degrading of the quality. The cover image is partitioned into a predefined 8 × 8 blocks. Each block is manipulated using Integer Lifting Wavelet Transform (ILWT) method, then TSO (Tree Scan Order) is applied to each manipulated block to identify proper location of confidential information.

Khalil .al.(2021) proposed a method that studies the medical image quality degradation when hiding data in the frequency domain. The secret plaintext was encrypted using RC4 encryption before the embedding process. The Discrete Fourier Transform (DFT) was applied to transfer the cover image into the frequency domain by decomposing it into its sinusoidal (sine and cosine) fundamental components in different frequencies. The results indicated that the quality of the image is exceptionally degraded when embedding data close to the low-frequency bands (DC) and this effect decreases in the upper-frequency bands.

Gayathri Nagasubramanian, Rakesh Kumar Sakthivel, Rizwan Patan, Amir H Gandomi,

Neural Computing and Applications 32, 639-647, 2020

Proposed system for ensuring the secrecy of digital signatures also ensures aspects of authentication. Furthermore, data integrity is managed by the proposed blockchain technology. The performance of the proposed framework is evaluated by comparing the parameters like average time, size, and cost of data storage and retrieval of the blockchain technology with conventional data storage techniques.

D Singh Rajput, Rakesh Gour International Journal of Computer Science and Information Security 14 (5), 2016

Proposed a E-Health Monitoring (EHM). This paper presents an architectural framework to describe the entire monitoring life cycle and highlights essential service components. It serves as a fundamental basis for achieving robust, efficient, and secure health monitoring.

Pushkar Kishore, Swadhin Kumar Barisal, Kulamala Vinod Kumar, Durga Prasad Mohapatra ICC 2021-IEEE International Conference on Communications, 1-6, 2021

Proposed a new technique is proposed utilising timestamp for handling a replay attack. We ensure strong forward security using the Elliptic Curve Discrete Logarithm Problem (ECDLP), making it challenging for an adversary to decode the security parameters. Finally, it is ensured that the hash function's bits maintain the entropy of the key involved in the security model. Thus, the proposed model preserves privacy as well as improves the security of the E-Health model.

Marlon Cordeiro Domenech, Eros Comunello, Michelle Silva Wangham 2014 IEEE 16th International Conference on e-Health Networking,Applications and Services (Healthcom), 219-224, 2014

Providing identity management (IdM) in the scene of Web of Things (WoT) is an important requirement to ensure protection of user data made available or consumed by the medical devices in WoT. This work aims to purpose the use of a user-centric IdM system in an ambient assisted living (AAL) environment in the WoT scenario. The IdM system is based on OpenID Connect that attends some of the main security requirements of an AAL environment.

Alkhabet, M.M., Ismail, M. Security algorithms for distributed storage system for E-health application over wireless body area network. *J Ambient Intell Human Comput* (2021).

Proposed, enhanced security and privacy of patient information and E-health systems based on distributed storage systems (DSSs) are developed using public-key cryptography to store patient

information. The storage of data and the security requirements (such as confidentiality, reliability, authentication, and dynamic integrity) are simultaneously distributed among individual nodes throughout the network. The patient data are encrypted using the redundant residue number system (RRNS) technique, which depends on a library of moduli in the encrypting process to generate residues.

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.

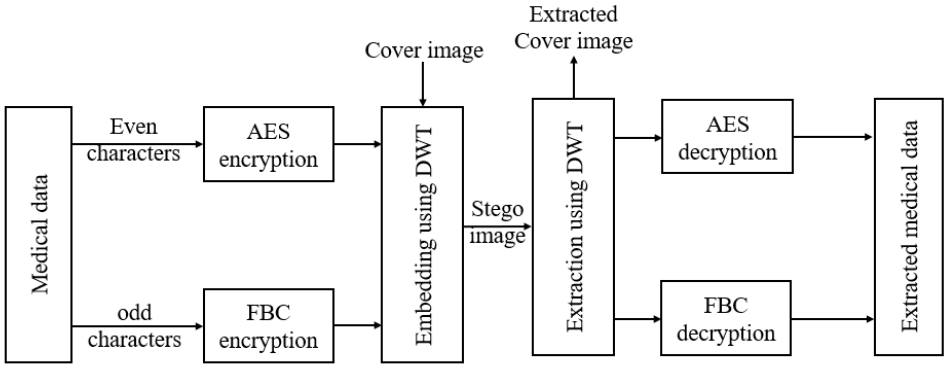

Figure 1. Proposed block diagram.

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.

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.

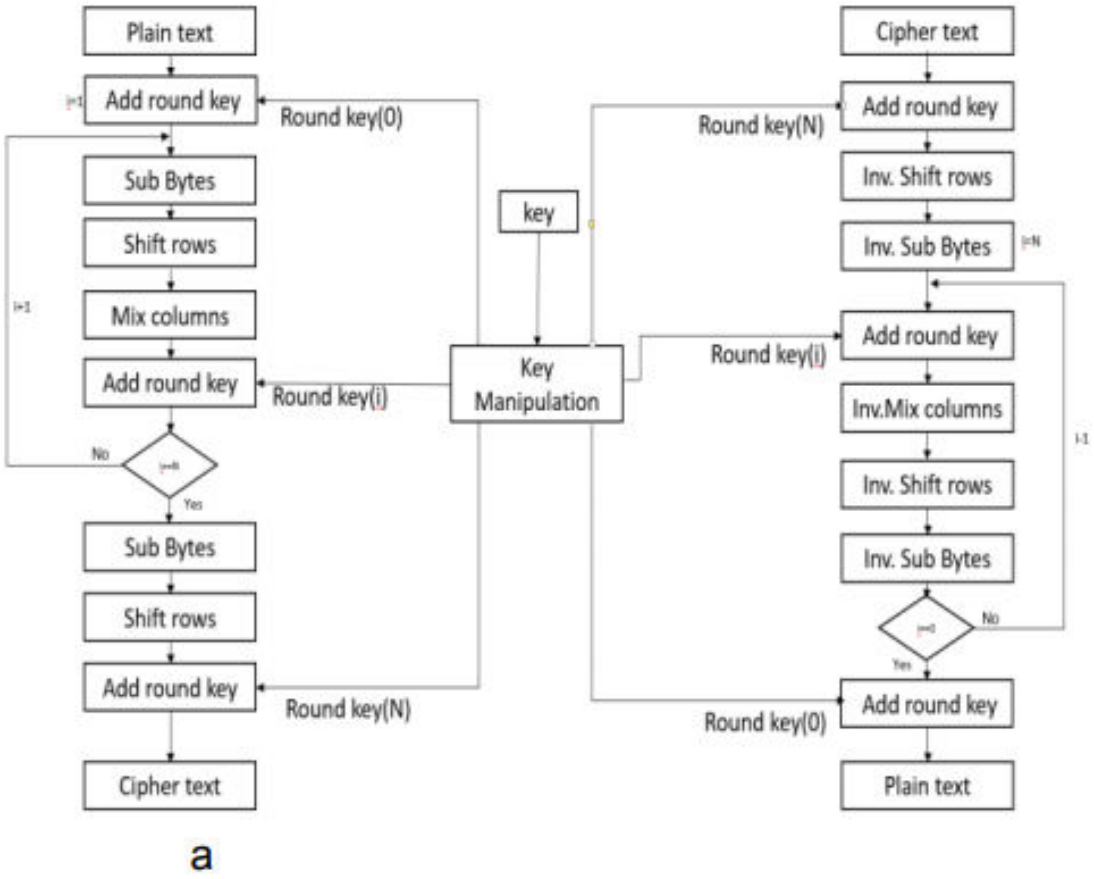

Fig.2. Flow diagram of AES Crypto Processor: a) Encryption b) Decryption

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.

5. RESULTS AND DISCUSSION

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 figure 1.

— In figure 3 screen enter some message in 'Secret Message' field.
— In figure 4 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

Figure 3: Displays the gui of the enhancing data security through innovations in aes-fbc encryption and dwt steganography.

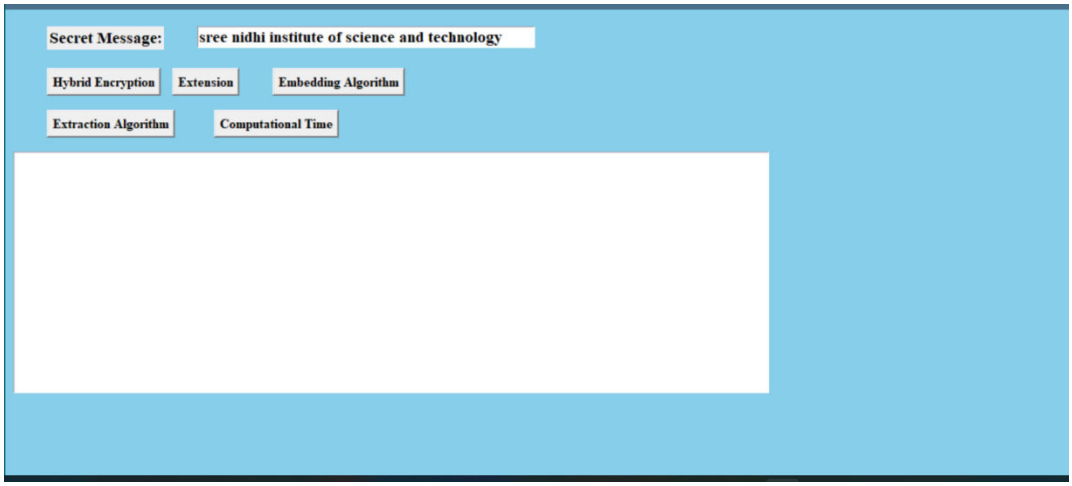

Figure 4: Represents the entered secret message in the gui.

In above screen, we have entered some message and then click on 'Hybrid Encryption' button to encrypt message using AES and RSA encryption.

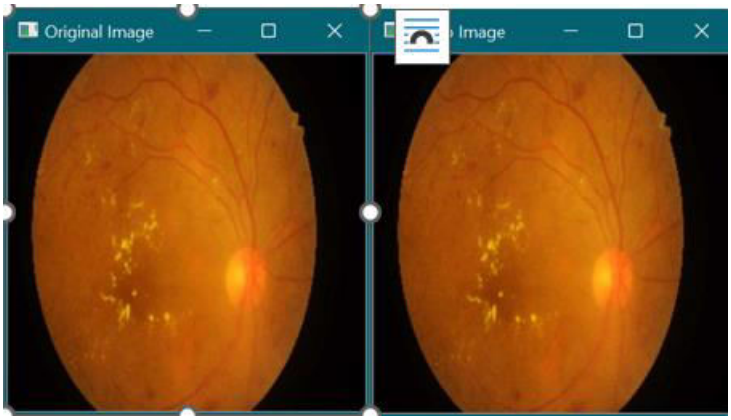

Figure 5: Shows the comparison of original and stego image.

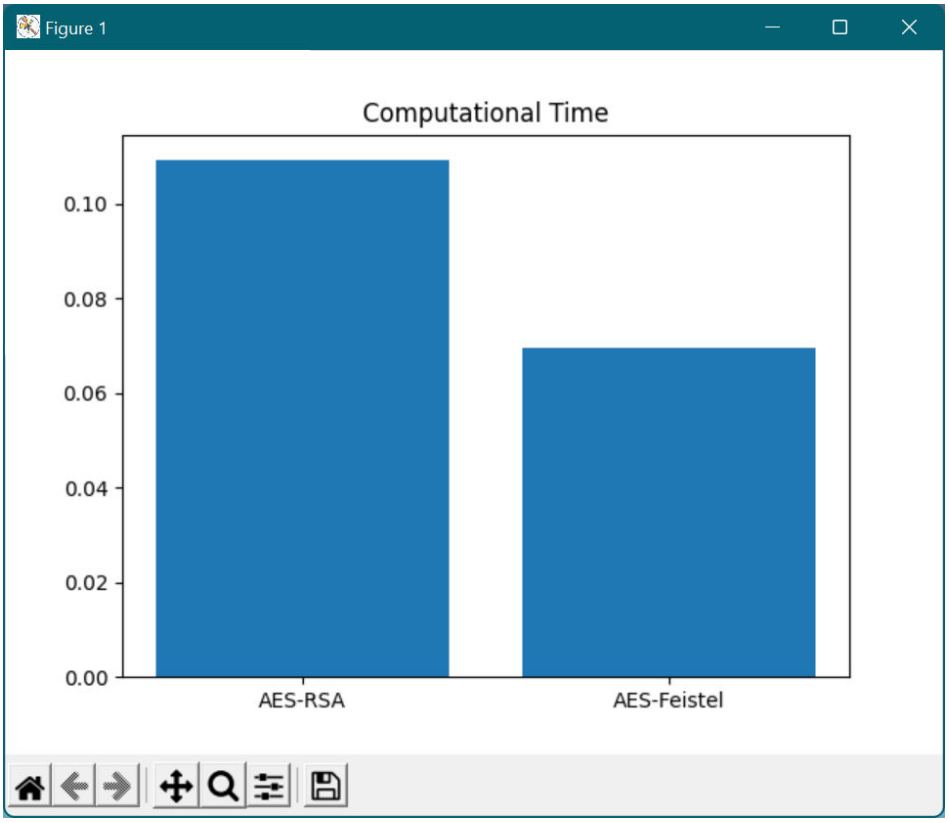

Figure 6: Displays the computation time comparison of two models.

5. CONCLUSION

For a healthcare-based IoT context, a secure patient diagnostic data transfer model employing both color 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]. Humayun, M., Jhanjhi, N. & Alamri, M. (2020). IoT-based Secure and Energy Efficient scheme for E-health applications. Indian J Sci Technol, 13(28), 2833-2848.

[2]. Almulhim, M., & Zaman, N. (2020, February). Proposing secure and lightweight authentication scheme for IoT based E-health applications. In 2018 20th International Conference on advanced communication technology (ICACT) (pp. 481-487).

[3]. Mallikarjuna, B., Kiranmayee, D., Saritha, V., & Krishna, P. V. (2021, June). Development of efficient e-health records using iot and blockchain technology. In ICC 2021-IEEE International Conference on Communications (pp. 1-7). IEEE.

[4]. Amare & Vuda (2021) .Edge Devices for Internet of Medical Thing Technologies, Techniques, and Implementation, eddah 22246-48.

[5]. Sarath Sabu, Swaraj Hegde et.al Global Transitions Proceedings 2 (2), 429-433, 2021

[6]. Bairagi et al.(2019), IoT-Based Healthcare-Monitoring System towards Improving Quality of Life. hulna 9208, Bangladesh

[7]. Shahzadi, R., Niaz, A., Ali, M., Naeem, M., Rodrigues, J. J., Qamar, F., & Anwar, S. M. (2019). Three tier fog networks: Enabling IoT/5G for latency sensitive applications. China Communications, 16(3), 1-11.

[8]. Hussain, A., Ali, T., Adeelaziz, F., Draz, U., Irfan, M., Yasin, S., ... & Alqhtani, S. (2021). Security framework for IoT based real-time health applications. Electronics, 10(6), 719.

[9]. Karolak, M., Razzaque, A., & Al-Sartawi, A. (2021). E-services and M-services using IoT: an assessment of the Kingdom of Bahrain. In Artificial Intelligence Systems and the Internet of Things in the Digital Era: Proceedings of EAMMIS 2021 (pp. 523-533). Cham: Springer International Publishing.

[10]. Dhatterwal, Jagjit Singh, Kuldeep Singh Kaswan, Anupam Baliyan, and Vishal Jain. "Integration of Cloud and IoT for Smart e-Healthcare." In Connected e-Health: Integrated IoT and Cloud Computing, pp. 1-31. Cham: Springer International Publishing, 2022.

[11]. Ould-Yahia, Youcef, Soumya Banerjee, Samia Bouzefrane, and Hanifa Boucheneb. "Exploring formal strategy framework for the security in iot towards e-health context using computational intelligence." Internet of things and Big data technologies for next generation healthcare (2017): 63-90.

[12]. Farahat, AS Tolba, Mohamed Elhoseny, Waleed Eladrosy Security in smart cities: models, applications, and challenges, 117-142, 2019