Enhancing Data Security through Novel AES-FBC Encryption and DWT Steganography Integration for IoT Communication Systems

Kamepalli Dharani, Assistant Professor, Department of ECE, St. Martin's Engineering College, Secunderabad , Telangana, Email: dharanikamepalli7596@gmail.com

ABSTRACT

In an era of data security, this research examines creative ways to protect information using cutting-edge encryption and steganography. The typical method uses the widely used Advanced Encryption Standard with Rivest-Shamir-Adleman (AES-RSA) encryption technique, which has some limitations. RSA algorithm flaws and system performance issues are among these downsides. The suggested system uses AES-FBC, a new encryption method with increased security and performance, to overcome these challenges. Discrete Wavelet Transform (DWT) steganography adds another layer of concealment, making the suggested method more resistant to attacks. The complete examination of the conventional system and its disadvantages prepares for the adoption of the suggested system by highlighting the limitations of the existing technique and the need for a more secure approach. The following explanation explains the technical details of encryption and steganography components and how they work together to improve data security. After simulations and experiments, the proposed system is shown to be more effective than the standard approach. The findings will demonstrate considerable data confidentiality and integrity improvements, proving the suggested system as a solid and novel method for securing sensitive data in digital contexts.

Keywords: IoT, Advanced Encryption Standard, Feistel Block Cipher, Data Security.

1. INTRODUCTION

Given the rise of cyberattacks and digital dependence, data security is essential to modern information management. Data security includes procedures to prevent unauthorized access, disclosure, alteration, and destruction. Strong authentication and access controls are essential to data security. This reduces the danger of unauthorized breaches by restricting sensitive data access to approved users or systems. Research on hiding data began with steganography, the science and art of hiding information in images. Steganography allows classified messages to be sent undetected. With its high spatial localization, frequency spread, and multi-resolution, the DWT matches the human visual system's theory of forms. This work implements frequency-domain 1-level and 2-level DWT steganography. The image was divided into high and low iterations. The high iteration section provides edge information, while the low part is often split into high and low parts. The future of unorthodox data transfer communication protocols is bright, yet there are still few ways to hide information. Improves medical data transmission security by using steganography and hybrid encryption to create a safe healthcare system. The growing use of IoT devices in healthcare has transformed medical data monitoring and transmission. A major issue with this increased connectedness is the protection of sensitive medical data during transmission. Though effective, current encryption approaches might be onerous for resource-constrained IoT devices used in healthcare. The demand for lightweight cryptographic solutions for safe medical data transfer in IoT-powered communication systems is urgent. A successful solution will improve medical data security in the fast-changing healthcare IoT connectivity ecosystem. Their project aims to provide a strong and lightweight cryptographic solution for safe medical data transmission in IoT-powered communication networks. Resource-constrained IoT devices present particular issues, so efficient encryption methods like AES or lightweight alternatives are prioritized. Dynamic key generation,

secure communication channels employing protocols like Transport Layer Security (TLS), and IoT device authentication are the main goals. The initiative also uses data anonymization to comply with healthcare rules and protect sensitive medical data during transmission.

2. LITERATURE SURVEY

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 METHODOLOGY

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.

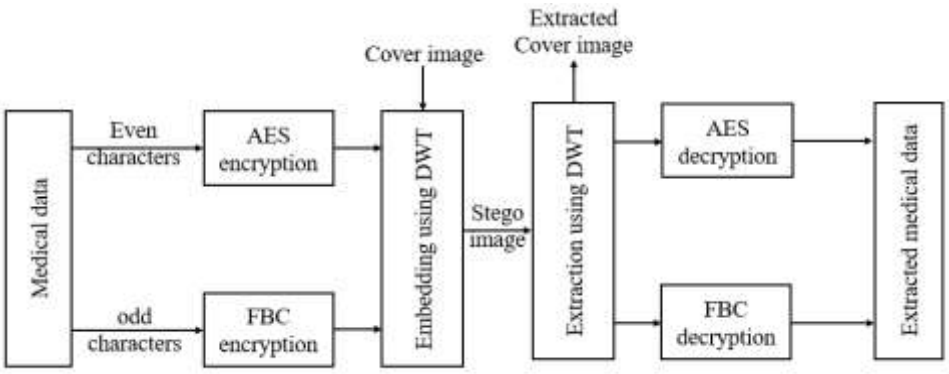


Figure 1. Proposed block diagram.

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.

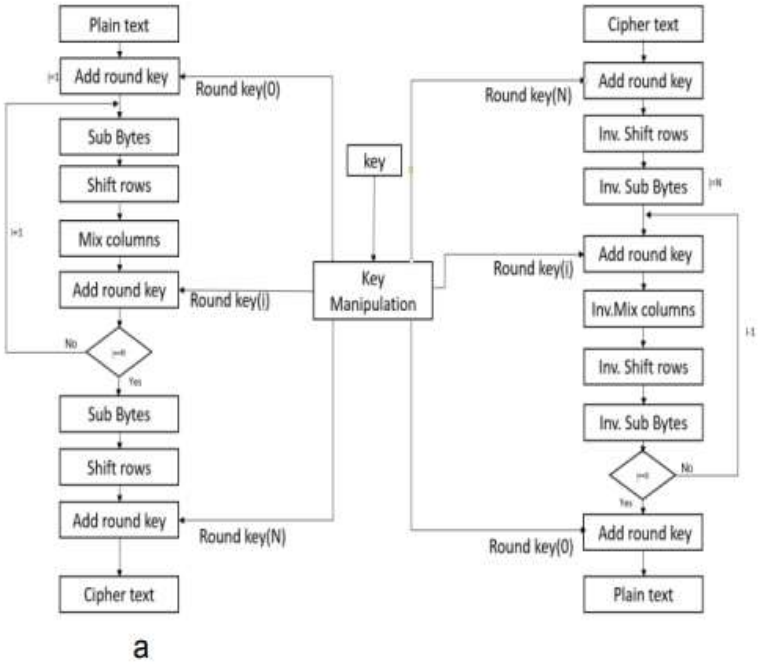


Figure 2. Flow diagram of AES Crypto Processor: a) Encryption b) Decryption

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:

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

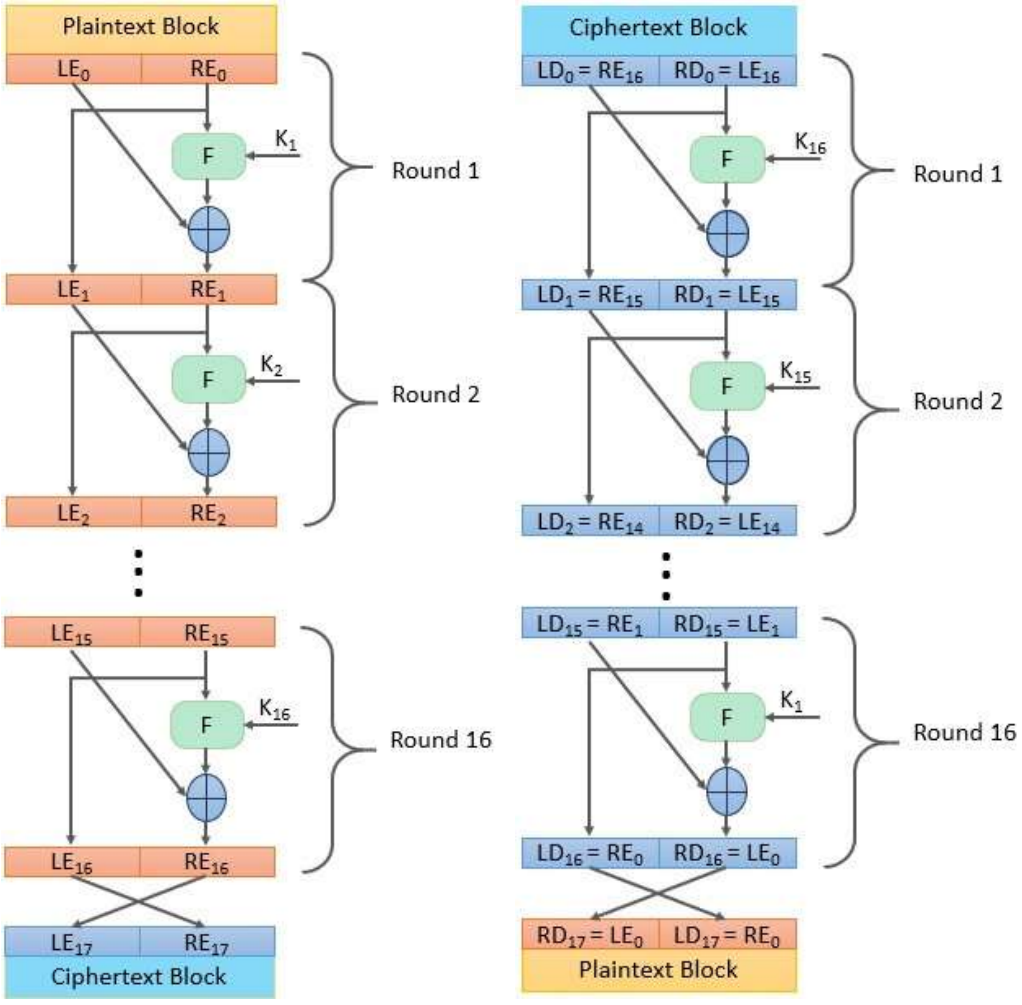
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \quad (2)$$

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 3 (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.



(a) (b)

Figure 3. FBC process (a) encryption, (b) decryption

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 3 (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 texat 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.

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.

(a)

(b)

Figure 4: Illustration of images. (a) original image. (b) stego image.

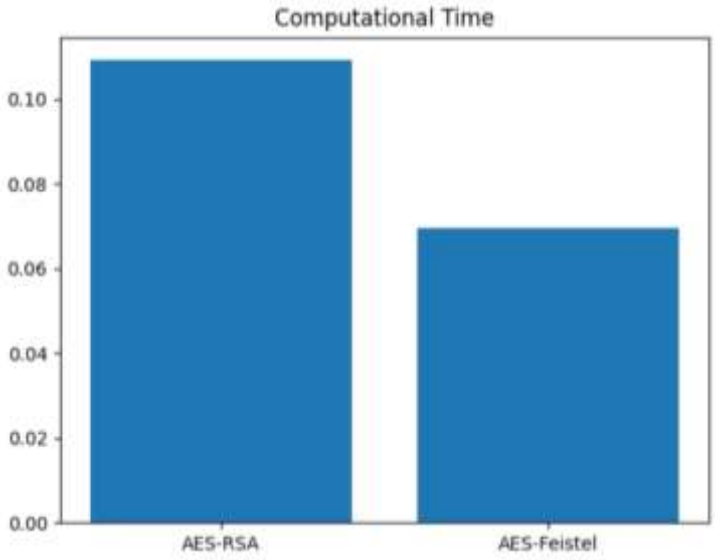


Figure 5. Computational time.

5. CONCLUSION

This research demonstrates that the proposed AES-FBC encryption combined with DWT steganography offers significant advancements in data security. By addressing the vulnerabilities and efficiency limitations of the conventional AES-RSA system, the proposed system provides enhanced confidentiality, integrity, and performance. The innovative integration of encryption and steganography establishes the AES-FBC with DWT steganography system as a robust solution for securing sensitive information in various digital environments. The findings underscore the necessity for continuous evolution in data protection methodologies to keep pace with emerging threats and technological advancements.

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] Srinivasarao, G., Penchaliah, U., Devadasu, G. et al. Deep learning based condition monitoring of road traffic for enhanced transportation routing. J Transp Secur 17, 8 (2024). https://doi.org/10.1007/s12198-023-00271-3

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.