A Two-Level Security Layer for Medical Data

*[1]Adedayo A. Olayiwola, *[1]John B. Oladosu, *[2]Christopher A. Oyeleye, and *[3]Oluwaseun M. Alade
[1]Department of Computer Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[2]Department of Information Systems, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[3]Department of Cyber Security, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
aaolayiwola42@lautech.edu.ng | jboladosu @lautech.edu.ng | caoyeleye@lautech.edu.ng | oalade75@lautech.edu.ng

Received: 15-MARCH-2024; Reviewed 21-MARCH-2024; Accepted: 24-MARCH-2024
https://dx.doi.org/10.4314/fuoyejet.v9i1.6

ORIGINAL RESEARCH

Abstract— Implementing a two-level security approach comprising cryptography and steganography in Electronic Health Record (EHR) systems ensures comprehensive protection of sensitive patient information. Cryptography encryption methods alone may not provide adequate protection, as they can be susceptible to attacks and also, steganography, has the visual quality issues after embedding. The combination of RSA cryptography and DWT steganography will offers a comprehensive solution for securing medical data, ensuring confidentiality, integrity, and compliance with privacy regulations, while DWT steganography provides covert embedding within medical images, preserving diagnostic integrity and enhancing data protection. In this paper, a secure two-level layer of medical data security is proposed to encrypt secret information using Rivest-Shamir-Adleman (RSA) while the encrypted secret information is embedded using Discrete Wavelet Transform (DWT). The performance of the proposed method was evaluated using Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Normalized Cross-Correlation (NCC) metrics. The results obtained show that our method performs with a value of 0.105 for MSE, 49.713 for PSNR and 0.912 for NCC showing high visual quality and low imperceptibility.

Keywords— Cryptography, Discrete Wavelet Transform, Rivest-Shamir-Adleman, Steganography.

1 INTRODUCTION

The majority of Electronic Health Records (EHR) are transmitted or shared over an unsecured channel, putting the record at risk of a malicious attack that may cause alteration affecting the security, confidentiality, integrity, authentication, and capacity of the record when it contains medical images or patient information (Salameh, 2019; Thabit, 2021). As a result, protecting EHR is crucial because distance is no longer an impediment to effective patient care and diagnosis (Thabit, 2021). Watermarking, cryptography and steganography are three regularly used data security solutions for EHR that have gained popularity over time because of their Confidentiality, Integrity and Authentication (CIA) (Rout & Mishra, 2014; Roy & Laha, 2015; Kadhim et al., 2019; Jeevitha and Amutha Prabha, 2020).

Cryptography is a technique for ensuring data privacy that entails data encryption and decryption (Pawar & Kakde, 2014; Gaithuru et al., 2015). Data encryption uses encryption techniques suitable for transmission security to turn data into a secret (scribbled) form (Singh et al., 2022). When the key for decryption is shared, encrypted data is generated utilizing encryption techniques such as modification, permutation, replacement, haphazard ordering or substitution, allowing only the authorized party to access it (Suguna et al., 2016). A key can be symmetrical (one key for both encryption and decryption) or asymmetrical (two keys for both encryption and decryption) (Kadhim et al., 2019). However, encrypted data (cipher) appears to be worthless by enticing attackers who look for the actual data passed from the sender to the recipient (Saleh et al., 2016; Abd-El-Atty, 2023).

Steganography on the other hand, is a technique used to hide secret data within a cover carrier such as text, image, audio or video to keep it private (Akinola & Olatidoye, 2015; Roy & Laha, 2015; Alade et al., 2021). Steganography involves embedding data into a cover carrier to create a stego-file, and there are two types of steganography methods: spatial domain and frequency domain (Alade et al., 2021). These methods are evaluated using imperceptibility and robustness as metrics. However, when the hidden data is discovered, steganography becomes a problem (Saleh et al., 2016). Image steganography should be robust, have good visual quality, and be secure (Okediran, 2020; Abdullah, 2021). Overall, steganography is a useful technique for keeping data private but its effectiveness depends on its ability to maintain imperceptibility and robustness while avoiding detection (Abd-El-Atty, 2023).

The combination of cryptography and steganography provides a high level of security against intruders (Gabriel et al., 2013; Bafna et al., 2015; Olaniyi et al., 2018). This combined approach not only fortifies defense against external threats but also mitigates risks posed by insider breaches, ensuring compliance with healthcare regulations and bolstering trust in EHR systems' security measures.

The aim of employing cryptography and steganography is to ensure the confidentiality, integrity, and authenticity of sensitive information while also concealing the very existence of covert communication. Cryptography achieves this by

*Corresponding Author

Section B- ELECTRICAL/COMPUTER ENGINEERING & RELATED SCIENCES
Can be cited as:
Olayiwola A. A., Oladosu J. B., Oyeleye C. A., and Alade O. M. (2024). A Two-Level Security Layer for Medical Data, FUOYE Journal of Engineering and Technology (FUOYE**JET), 9(1), 38-42.**
https://dx.doi.org/10.4314/fuoyejet.v9i1.6

encrypting data, rendering it unreadable to unauthorized individuals and protecting it from manipulation or interception. Meanwhile, steganography complements cryptography by embedding secret messages within innocuous cover media, obscuring their presence from scrutiny. Collectively, these methodologies enhance information security by not only protecting the content of messages but also concealing their presence, thereby guaranteeing the privacy and security of sensitive communications.

2 Review Of Related Works

Numerous image steganography methods and algorithms have been proposed and extensively studied to achieve better security. Abikoye et al., 2020 study addresses the pressing issue of biometric template attacks in iris recognition systems by integrating Cryptography (Twofish and Triple Data Encryption Standard (3DES)) algorithms with Steganography (Least Significant Bits). Twofish and Triple data encryption are robust cryptographic techniques employed to transform plain image data into encrypted cipher images, while Least Significant Bits (LSB) serves as a steganographic method to embed ciphertext or images directly into a cover image, producing a stego image. The research utilizes the Hough transform, Daugman rubber-sheet model, and Log Gabor filter for iris image segmentation, normalization, and feature extraction, respectively. The resulting iris template is encrypted using 3DES and Twofish algorithms. Subsequently, the cipher image is embedded into a cover image using LSB. The outcome of this approach subtly alters the master file after embedding the secret image (stego file), rendering it imperceptible to the human eye. Only a JPEG image is employed as the master or cover file. This dual-layered security technique offers ample embedded capacity and produces high-quality stego images capable of withstanding potential attackers. Gladwin & Gowthami (2020) proposed a robust and effective algorithm based on elliptic curve cryptography combined with Hill cipher to mitigate threats and increase information security. In its method, ciphertext and DCT coefficients of an image, are embedded into the base image based on LSB watermarking. The ciphertext is generated based on the Hill Cipher algorithm. Hill Cipher can, however, be easily broken and has weak security and to add complexity, Elliptic curve cryptography (ECC), is combined with Hill cipher. Based on the ECC algorithm, the key is produced, which is employed to generate ciphertext through the Hill cipher algorithm. This combination of both steganography and cryptography results in increased authority and ownership of the data for sub-optimal media applications and even if intercepted by the attacker the secret data and secret image is hidden, the attacker will not be able to know the exact location of the secret data. It is hard to extract the hidden data and the image without the proper key.

Hureib & Gutub (2020) explore methods through which secret information is encrypted then and hidden to increase the level of security in medical health data from being hacked. This is done through combining two methods of Elliptic curve cryptography and image steganography. In the first stage, the text would be encrypted by using ECC. In the second stage, steganography would be used to conceal the text inside an image. Selecting ECC, which is an algebraic structure of elliptic curves over finite fields, is considered as being a desired choice for being a public key. Furthermore, it can be used in many types of media which include medical record systems and in the field such as CT scans, and MRI scans. Selecting Image Steganography, which is a technique that helps many organizations, and institutions to hide encrypted information, obscures private information from a person who is not authorized to get access. It is a reliable technique giving and assuring the highest level of safety and security of the secret information.

In Okediran (2020), a hybrid algorithm combining the RSA algorithm, RC4 algorithm, and Spread Spectrum techniques for securing medical image data. The developed scheme was evaluated using various performance metrics, including PSNR, SNR, MSE, and BER, with the results suggesting that the scheme is highly reliable, robust, and imperceptible, and the original images can be retrieved without any deformation or alteration. While the proposed scheme adds a new perspective to medical data security, the lack of information on the specific implementation details of the scheme and the evaluation methodology makes it challenging to assess the reliability and generalizability of the findings. Nonetheless, the paper highlights the importance of securing medical data in electronic formats and suggests the need for robust security measures to ensure patient privacy and confidentiality.

Tabassum & Mahmood (2020) proposed method combines Steganography and Cryptography, integrating the Blowfish and Advanced Encryption Standard algorithms with unique aspects of the residue numbering system, the Least Significant Bit algorithm, and the Genetic Algorithm operators. Results demonstrate a reduction of over 70% in minimal error for stego images compared to previous methods, as measured by Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). This approach exhibits reduced complexity in runtime and power consumption. Additionally, higher NPCR/UACI values in the results signify an enhanced level of security.

3 Methodology

The approach of this work contains the use of a publicly available medical dataset from Kaggle.com for the use of both cover and secret data. The secret data was encrypted and decrypted using the Rivest-Shamir-Adleman (RSA) Algorithm due to its faster encryption and decryption time and its strength of secure key exchange (Mahajan & Sachdeva, 2013; Patil et al., 2016) while the Discrete Wave Transform (DWT) was used to hide the secret message.

3.1 Encryption And Decryption

Rivest-Shamir-Adleman (RSA) was used for the encryption and decryption of medical images and information to increase the security level of their messages. In RSA, three stages were involved in the

https://dx.doi.org/10.4314/fuoyejet.v9i1.6 engineering.fuoye.edu.ng/journal

process, which are key generation, encryption and decryption.

i. Key generation

In the key generation process, firstly the prime numbers generated were used to generate a key pair that is public key and private key. Here is an algorithm for generating RSA keys:

1. Input two prime numbers, p and q generated
2. Count $n = p * q$(preferably that $p \neq q$, because if $p = q$then $n = p^2$ so p can be obtained by pulling the square root of r)
3. Count $\varphi(n) = (p-1)(q-1)$
4. Choose an integer e, such that e is a co-prime to $\varphi(n)$ and $1 < e < \varphi(n)$
5. Generate secret key$d$, such that$d * e = 1(mod\ \varphi(n))$

So, in the end, the RSA key generation algorithm assigns (e, n) as public key and d as private key.

ii. Encryption

The RSA encryption algorithm uses the exponential function in modular n as in the Equation 3.3. Given a plaintext P, represented as a number, the cipher text C is calculated as:

$$C = P^e\ mod\ n \quad (1)$$

iii. Decryption

The RSA decryption algorithm is an inverse of RSA encryption. Just like the encryption algorithm, the RSA decryption algorithm is a modular exponential function n by using the private key as in the Equation 3.4. Using the private key (n, d), the plaintext can be found using:

$$P = C^d\ mod\ n \quad (2)$$

3.2 Embedding And Extraction

The Discrete Wave Transform (DWT) was applied for embedding the secret message due to its projection of low and high-frequency details by decomposing the image into sub-bands using the DWT. This enables the identification and manipulation of the high-frequency coefficients that represent the edges and other details in the image. DWT on the edge detected cover-image will generate four wavelet sub-bands LL (approximation coefficients), LH (vertical details), HL (horizontal details) and HH (diagonal details). The embedding procedure was used for embedding the message into the cover-image. The steps of the embedding procedure as described in Algorithm 1.

The extraction process involves the reverse of the embedding process. The DWT coefficients are modified based on the positions of the embedded information, and the secret information is extracted from the modified coefficients. In the extraction phase, the stego-image (S) was decomposed into four sub-frames using DWT. The sub-frames are partitioned into non-overlapping blocks. The best matched blocks are extracted from S. The difference blocks are extracted from detail coefficients blocks. The steps of the extracting procedure as shown in Algorithm 2.

The implementation of the developed two-layered security technique for medical data involves using RSA and DWT which was developed using MATLAB R2023a version on a system of Windows 11, 64-bit Operating System (OS), Intel Core ™ i5 CPU with speed of 2.40GHz 2.50GHz, 16GB RAM.

Algorithm 1: DWT Embedding phase procedure

Step 1: Read the cover-image (C) and cipher secret information *(I)*

Step 2: Decompose the cover-image (C) into four sub-frames (C_{LL}, C_{LH}, C_{HL}, C_{HH}) respectively using the DWT filter.

Step 3: Perform embedding of cipher secret information *(I)*

Step 4: Calculate inverse DWT (IDWT)

Algorithm 2: DWT Extraction phase procedure

Step 1: Decompose the stego-image*(S)* into four sub-frames (S_{LL}, S_{LH}, S_{HL}, S_{HH}) respectively using DWT filter

Step 2: Extract the best matched block from sub-frame S_{LL}

Step 3: Perform extraction of cipher secret information *(I)*

Step 4: Perform IDWT to generate the original C

Step 5: Return I and C

4 Experimental Results And Discussion

In our study, samples were obtained from an online public database (Kaggle.com). The dataset's selection was driven by the availability of diverse medical imaging modalities, providing a valuable resource for research and analysis in the field of healthcare. The experiment utilized six (6) gray-scale medical images of 1024 by 1024 dimensions selected at random and two (2) benchmark images as shown in Table 4.1(a) for Cover Image (CI). CI1 is a JPEG chest X-ray image with no infection, CI2 is a JPEG Kidney image with no infection, CI3 is a JPEG brain image with an infection of glioma tumor, CI4 is a PNG chest X-ray image with COVID infection, CI5 is a PNG joint X-ray image with no infection, CI6 is a PNG joint X-ray image with osteoarthritis infection and Lena and Peppers benchmark images in PNG format were all used as cover image.

Also, seven (7) gray-scale medical data were used as the Secret Image (SI) in jpg format as shown in Table 4.1(b). SI1, SI2 and SI3 are prescription images, SI4, SI5 and SI6 are medical reports and SI7 is an image of a lung without infection.

Table 1

Cover Image (CI)	Secret Image (SI)	MSE	PSNR	NCC
CI1	SI1	0.117	42.402	0.896
CI1	SI7	0.135	42.376	0.865
CI2	SI2	0.259	35.116	0.741
CI3	SI6	0.361	33.954	0.761
CI4	SI4	0.153	36.463	0.773

https://dx.doi.org/10.4314/fuoyejet.v9i1.6 engineering.fuoye.edu.ng/journal

CI4	SI7	0.244	36.051	0.772
CI5	SI3	0.307	38.083	0.809
CI6	SI5	0.121	41.954	0.891
LENA	SI3	0.109	49.713	0.910
PEPPERS	SI5	0.105	48.355	0.912

In Table 1, which focuses on the stego-image quality when a single secret image is embedded, DWT demonstrates a notably low MSE of 0.105. These results indicated that DWT introduces less distortion into the stego-image compared to the other techniques, showcasing its ability to maintain higher image quality during single-image embedding.

In Table 1, which pertains to the embedding of a single secret image, DWT attains a peak PSNR of 49.713. These outcomes underscore the significantly reduced perceptible distortion introduced by DWT, thus showcasing its ability to generate stego-images of superior quality when image embedding is employed.

In Table 1, specifically focusing on the scenario where a single secret image is embedded, DWT achieves an impressive NCC value of 0.912, indicating a significant resemblance between the stego-image and the original cover image. These results showed DWT's capability to generate stego-images that closely align with the visual characteristics of the source cover image, underscoring its proficiency in concurrently maintaining data concealment and visual consistency during the process of embedding a single secret image.

5 Conclusion And Future Work

This research delves into medical image security, combining Discrete Wavelet Transform (DWT) with RSA cryptography. The research systematically explores the interaction of these techniques and their implications. DWT's embedding potential while RSA cryptography fortified the system, safeguarding against unauthorized access and tampering during data transmission and storage. This comprehensive approach addressed both security and perceptual aspects, crucial for protecting sensitive medical data. The fusion of DWT and RSA offered a robust framework for securing medical images with efficient data hiding and encryption mechanisms.

RSA cryptography and DWT steganography have limitations. RSA is vulnerable to quantum computing attacks, threatening its future security. DWT-based steganography faces trade-offs between hiding capacity and image quality, potentially arousing suspicion with noticeable image degradation. Moreover, sophisticated analysis methods can detect hidden data, diminishing the reliability of DWT steganography.

Future research could address limitations in RSA cryptography and DWT steganography. Efforts may focus on post-quantum cryptographic algorithms to resist quantum computing attacks and optimize RSA encryption for resource-constrained devices. In steganography, novel embedding algorithms balancing hiding capacity and image quality, potentially leveraging deep learning, could be explored.

References

Abdullah, D. M., Ameen, S. Y., Omar, N., Salih, A. A., Ahmed, D. M., Kak, S. F., & Rashid, Z. N. (2021). Secure Data Transfer Over Internet Using Image Steganography. *Asian Journal of Research in Computer Science*, 10, 33-52.

Abikoye, O. C., Ojo, U. A., Awotunde, J. B., & Ogundokun, R. O. (2020). A Safe and Secured Iris Template Using Steganography and Cryptography. *Multimedia Tools and Applications*, 79(31), 23483-23506.

Akinola S. O. & Olatidoye A. A. (2015). On the Image Quality and Encoding Times of LSB, MSB and Combined LSB-MSB Steganography Algorithms using Digital Images. *International Journal of Computer Science & Information Technology*, 7(4), 79-91.

Alade O. M., Amusan E. A., Adedeji O. T. & Alo O. O. (2021). Image Steganography using Pixel Value Differencing (PVD) Technique Based on Firefly Algorithm. *Journal of Scientific Research and Reports*, 27(7), 80-86.

Bafna B. S., Mutha B. H., Gawali A. D. & Govind A. J. (2015). A Survey on Cryptosteganography: A Multilayer Security Data Hiding. *International Journal of Advance Research and Innovative Ideas in Education*, 1(4), 346-354.

Gabriel A. J., Alese B. K., Adetunmbi A. O. & Adewale O. S. (2013). Post-Quantum Crystographic: A Combination of Post-Quantum Cryptography and Steganography. *In 8th International Conference for Internet Technology and Secured Transaction*, 449-452.

Gaithuru J. N., Bakhtiari M., Salleh M. & Muteb A. M. (2015). A Comprehensive Literature Review of Asymmetric Key Cryptography Algorithms for Establishment of the Existing Gap. *In 9th Malaysian Software Engineering Conference*, 236-244.

Gladwin S. J.& Gowthami P. L. (2020). Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images. *In 2020 International Conference on Artificial Intelligence and Signal Processing (AISP)*, 1-5

Hureib E. S. & Gutub A. A. (2020). Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography. *International Journal Computer Science Network Security (IJCSNS)*, 20(8), 1-8.

Jeevitha S. & Amutha Prabha, N. (2020). Effective Payload and Improved Security using HMT Contourlet Transform in Medical Image Steganography. *Health and Technology*, 10, 217-229.

Kadhim I. J., Premaratne P., Vial P. J. & Halloran B. (2019). Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research. *Neurocomputing*, 335, 299-326.

Mahajan, P., & Sachdeva, A. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology*, 13(15), 15-22.

Okediran O. O. (2020). A Hybrid Cryptosystem and Watermarking for Secure Medical Image Transmission. *Asian Journal of Research in Computer Science*, 5(1), 1-14.

Olaniyi O. M., Arulogun O. T., Kawonise A. K. & Ajimati T. (2018). Bio-Crystographic Techniques for Secure Electronic Voting System. *Advance in Electrical and Telecommunication Engineering*, 1(2), 55-64.

Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, 78, 617-624.

https://dx.doi.org/10.4314/fuoyejet.v9i1.6 engineering.fuoye.edu.ng/journal

Pawar S. S. & Kakde V. (2014). Review on Steganography for Hiding Data. *International Journal of Computer Science and Mobile Computing*, 3(4), 225-229.

Rout H. & Mishra B. K. (2014). Pros and Cons Cryptography, Steganography and Perturbation Techniques. *IOSR Journal of Electronics and Communication Engineering*, 76-81.

Roy R. & Laha S. (2015). Optimization of Stego Image Retaining Secret Information using Genetic Algorithm with 8-connected PSNR. *Procedia Computer Science*, 60, 468-477.

Salameh J. N. B. (2019). A New Approach for Securing Medical Images and Patient's Information by Using a Hybrid System. *International Journal of Computer Science and Network Security*, 19(4), 28-39.

Selah M. E., Aly A. A.& Omara F. A. (2016). Data Security Using Cryptography and Steganography Techniques. *International Journal of Advanced Computer Science and Application*, 7(6), 390-397.

Singh, B., Singh, M., & Sarangal, H. (2022). Chaotic Maps and DCT-based Image Steganography-cum-encryption Hybrid Approach. *In International Conference on Communication and Intelligent Systems* (pp. 181-193). Singapore: Springer Nature Singapore.

Suguna, S., Dhanakoti, V., & Manjupriya, R. (2016). A study on symmetric and asymmetric key encryption algorithms. *International Research Journal of Engineering & Technology (IRJET)*, 3(4), 27-31.

Tabassum T. & Mahmood M. A. (2020). A Multi-Layer Data Encryption and Decryption Mechanism Employing Cryptography and Steganography. *Emerging Technology in Computing, Communication and Electronics*, 978(1).

Thabit R. (2021). Review of Medical Image Authentication Techniques and their Recent Trend. *Multimedia Tools and Applications*, 80(9), 13439-13473

https://dx.doi.org/10.4314/fuoyejet.v9i1.6