A Multi-Faceted Encryption Strategy for Securing Patient Information in Medical Imaging

Ammar Odeh[1*] and Anas Abu Taleb[2]

[1*] Assistant Professor, Princess Sumaya University for Technology, King Hussein School of Computing Sciences, Computer Science Department, Jordan. A.odeh@psut.edu.jo, Orcid: https://orcid.org/0000-0002-9929-2116

[2] Associate Professor, Princess Sumaya University for Technology. King Hussein School of Computing Sciences, Computer Science Department, Jordan. a.abutaleb@psut.edu.jo, Orcid: https://orcid.org/0000-0002-8286-1829

Received: August 26, 2023; Accepted: October 28, 2023; Published: December 30, 2023

Abstract

In modern healthcare, transmitting digital medical images through open-source networks for diagnosis in remote centers poses a significant security challenge due to the sensitive patient information involved. This paper presents an algorithm designed to encrypt these crucial medical images comprehensively. The algorithm generates hash code to validate image integrity, followed by feature-based watermarking, transformation into the frequency domain via Discrete Cosine Transform (DCT), and encryption using Advanced Encryption Standard (AES) and RSA encryption techniques. Each step plays a pivotal role in fortifying the images against unauthorized access, tampering, or interception during transmission, Guaranteeing the secrecy, unaltered state, and legitimacy of the included medical information. Implementing this encryption algorithm mandates strict adherence to cryptographic best practices, robust execution of encryption algorithms, secure key management, and compliance with industry standards. These meticulous measures bolster the confidentiality and integrity of medical images, which are crucial in protecting patient privacy and maintaining data integrity within healthcare systems. This comprehensive encryption strategy addresses the need for the purpose of ensuring safe and protected delivery and protection of sensitive medical information across networks.

Keywords: Homomorphic Encryption, Medical Images, Peak-Signal-to-Noise Ratio, Number of Pixel Change Rate, Unified Average Changing Intensity, Entropy.

1 Introduction

The HITECH Act enacted in 2009 was a significant catalyst in encouraging the widespread adoption of Electronic Health Records (EHR), aiming to revolutionize the accessibility and management of patient data (Gold, M., 2016). EHR systems simplify updating medical information electronically and foster seamless communication between healthcare providers, marking a monumental shift from traditional paper-based records (Furukawa, M.F., 2014).

EHR's pivotal role in enhancing healthcare quality cannot be overstated. Its digitized format consolidates a patient's comprehensive medical history, presenting a myriad of advantages when

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 14, number: 4 (December), pp. 164-176. DOI: *10.58346/JOWUA.2023.I4.012*

*Corresponding author: Assistant Professor, Princess Sumaya University for Technology, King Hussein School of Computing Sciences, Computer Science Department, Jordan.

compared to conventional paper records. Beyond the sheer capacity to manage vast volumes of patient data efficiently, EHR systems significantly enhance the overall quality of patient care through swift and precise record updates (Lite, S., 2020) (Reisman, M., 2017).

In tandem with the increasing reliance on medical imaging for diagnoses and treatment, concerns about the confidentiality of these images have surfaced. While instrumental in medical advancements, technologies like MRI and CT scans contain sensitive patient information (Panayides, A.S., 2020). The leakage or compromise of such data could have severe privacy implications for patients and legal ramifications for healthcare institutions. Consequently, extensive efforts have been undertaken to develop robust security solutions, such as cryptographic methods, to safeguard these invaluable medical images and protect patient privacy (Ramzan, M., 2022) (Kaissis, G.A., 2020).

Securing sensitive information within the digital domain of medical imaging presents a significant challenge (Rasool, R.U., 2022) (Nosrati, S., 2020). The exposure of these images on shared digital networks makes them susceptible to a spectrum of potential attacks, necessitating advanced cryptographic solutions (Singh, S., 2021). It is imperative to employ encryption techniques that render the data indecipherable, ensuring its confidentiality even if breaches occur or unauthorized access is gained. Among the various encryption approaches, symmetric encryption stands out for its efficacy in securing large volumes of data and upholding confidentiality (Shukla, S., 2022) (Bandari, V., 2023).

Innovatively, chaos theory has emerged as a promising frontier in modern cryptography, posing a challenge to traditional symmetric encryption systems such as AES (Zhang, J., 2020). Chaos-based cryptographic systems offer many advantages, including sensitivity to initial conditions, deterministic randomisation, structural complexity, a broad critical space, adaptability, and extensive periodicity. Developing improved algorithms and implementations in cryptographic solutions remains crucial to fortify medical images against evolving threats and maintain the utmost confidentiality of sensitive data in healthcare settings (Teh, J.S., 2020) (El-Latif, A.A.A., 2022).

Moreover, the implementation of such sophisticated encryption techniques not only ensures confidentiality but also strengthens the integrity of health records. However, the ever-evolving landscape of cybersecurity demands continuous refinement and vigilance in safeguarding patient information (Aram, S., 2016). As technology advances, efforts to mitigate potential vulnerabilities in cloud storage and encryption algorithms remain crucial. Additionally, expanding the application of these secure methodologies to various aspects of healthcare, such as telemedicine and remote patient monitoring, is pivotal for ensuring a comprehensive and robust healthcare data security framework.

The Following are the Key Contributions

- Design of improved multi-layered encryption process involving hash code generation, feature-based watermarking, transformation into the frequency domain using DCT, AES encryption for data security, and additional security layers through RSA encryption.
- Introduce `critical cryptographic techniques like hashing (SHA-256) to create a unique digital fingerprint, watermarking to embed the hash information imperceptibly, and frequency domain transformation (DCT) for enhanced representation of image content, thereby bolstering the image's resilience against potential attacks and un unauthorised modifications.
- Conduct an assessment to evaluate the execution performance and compare the findings with recent studies or works for comparative analysis.

2 Related Work

Numerous methods are commonly employed to safeguard data privacy in cloud storage. One such prominent technique is the Electronic Health Record (EHR), utilized for digitally managing patients' healthcare details. Cloud storage is preferred given the vast amount of data involved, although it raises significant security concerns in cloud computing (Jouini, M., 2019). As a result, numerous cryptographic algorithms have been suggested to bolster data security within the cloud. Introducing a lightweight encryption algorithm, the LSFE method has been implemented to provide medical records in a secure, encrypted format (Yao, F., 2021) (Hamza, N.A., 2019). This algorithm ensures encrypted data; further, image segmentation is executed for enhanced security. The reduction of images is achieved using Hadoop and MapReduce. Consequently, this method assures the confidentiality of healthcare data (Hamza, N.A., 2019).

In a prior study (Dzwonkowski, M., 2015), a method utilizing quaternions to encrypt DICOM images was presented and juxtaposed against the Advanced Encryption Standard Electronic Codebook (AES-ECB). This particular technique exhibited significantly swifter performance in contrast to ECB. Furthermore, in (Wadi, S.M., 2014) introduced an novel encryption method for new-definition medical image security, employing an adapted version of AES. However, this approach underwent cryptanalysis in (Yap, W.S., 2016) through an impossible variance cyberattack in subsequent investigations.

In (Li, L., 2012) presented an encrypted algorithm for secret medical images employed the Elliptic Curve ElGamal encryption algorithm. They selected elliptic curve parameters to resist attacks such as Pohlig-Hellman, Pollard’s rho (Pollard, J.M., 1978), and Isomorphism. The algorithm involved converting multiple pixel values into binary, combining them to form large integers below a prime modulo, and encoding these integers into elliptic curve coordinates utilize the Koblitz encoding technique. Compared to RSA and ElGamal schemes, Li et al.'s approach exhibited superior execution speed.

In (Tawalbeh, L.A., 2013) introduced a method for encrypting images content by utilizing elliptic curve cryptography, introducing two distinct models for medical image Encipherment. One algorithm involved image compression, followed by encrypting the DC components using ECC. In the second algorithm, ECC encryption targeted only the most significant bits. Despite ECC's high-security features relying the way the author has set up their elliptic curve parameter for ECDLP might not be large enough to effectively guard against attacks like Baby-step, giant-step, or Pollard’s Rho attack. Despite the strong security features of ECC based on ECDLP, the size of the cyclic order in the elliptic curve parameter might not be sufficient to fend off assaults such as Baby-step, giant-step, or Pollard’s Rho attack.

In a prior publication (Behnia, S., 2013), a system for encrypting medical images was proposed, employing Jacobian elliptic maps. The method involved utilizing the Jacobian elliptic map to create a disorderly sequence, subsequently generating a coded image through XOR operations between this disordered sequence and the pixel values of the original image. Furthermore, Manish et al. (Kumar, M., 2016) presented an alternative image encryption strategy in which pixel values were encoded using a DNA encoding method, followed by circular shifting using keys exchanged through an asymmetric encryption technique rooted in the Elliptic Curve Diffie-Hellman algorithm

The approach in (Yu, F., 2021) Chaos was employed to enhance security in encrypting two images simultaneously. The method included encrypting the extracted face from the image and then conducting a second encryption on the whole picture. The keystream used for the cryptographic system was produced by the 2D SFSIMM (a Two-dimensional hyperchaotic map, sinusoidal feedback Sine ICMIC modulation map), blending both scrambling and diffusion techniques. This approach showed robustness

against diverse statistical attacks because breaking the encryption algorithm necessitated overcoming two encryption rounds.

In a different study (Yu, F., 2021), A new cryptographic system was created to encode and decode images using three secure maps. The sine map was used to rearrange pixel coordinates within the original image through a permutation method, followed by substitution using a second secret key, K. Finally, scrambling of the image based on CTM (Cipher-based Technique for Mapping) was performed using a bit XOR operation.

Another proposed technique for chaotic image encryption, outlined in (Cheng, Z., 2022), integrated Latin squares and random shifts. The algorithm involved key creation, pixel scrambling, pixel swapping, and bit scrambling. Improving the complexity of the resulting Latin square matrix enhanced the procedure's security and robustness. The key was initially generated from the plain image to heighten sensitivity in the cryptography approach. Pixel position scrambling followed, cyclically shifting each pixel to the right within every row of the image matrix. Coordinate elements of the image matrix were then replaced with the lookup table's values from a 256-by-256 Latin square matrix containing a chaotic sequence, determined based on the image's pixel values and the sequence's values. Implementing multimedia encryption techniques demands more resources (time and storage). Consequently, lightweight image encryption techniques, which require minimal memory, time, or energy while providing high security for low-powered devices, are gaining popularity.

Subsequently, Ferdush et al. (2021) explored lightweight image encryption based on chaos, introducing a standardised approach and method using two distinct chaotic maps—Arnold and Logistic.

Another study (Gururaj, H.L., 2023) discussed modifying pixel values and positions based on the SCAN algorithm and chaotic theory. The SCAN method involved converting image pixel values to new ones and rearranging pixels in a specific order. Chaotic maps were used to move pixel coordinates within blocks. Pixel diffusion occurred through the SCAN method, while chaotic maps generated permutations. Wavelet-based approaches faced limitations due to insufficient phase information, inadequate directionality, and sensitivity to shifts.

Table 1 provides an overview of the current landscape of various encryption methods utilized in the field. Referring to specific algorithms and their associated drawbacks, it showcases critical assessments aiming to enhance the security and functionality of these encryption techniques.

Table 1: An Overview of Various Encryption Techniques

Ref. No	Algorithm	Drawbacks
[19]	AES-ECB	These modifications include reducing computation costs by altering the number of rounds in the MixColumn transformation, enhancing security by improving the key schedule operation, replacing the S-boxes with a simpler version to reduce hardware requirements, and addressing pattern appearance problems through ciphering modes.
[20]	Modified AES	the vulnerability of the modified AES-128 cipher against an impossible differential attack contradicts claims of improved security. This finding raises concerns about the cipher's reliability and its suitability as a secure foundation for image encryption, necessitating a reevaluation of its design and potential improvements to ensure more robust security measures.
[21]	Elliptic Curve ElGamal encryption	Inadequate or incomplete standardization of ECEG might lead to interoperability issues or inconsistencies in different implementations, potentially causing security flaws or vulnerabilities.
[22]	Elliptic curve cryptography	The paper does not discuss the key generation, distribution, or management processes for ECC-based encryption in the context of multimedia content.
[23]	Jacobian elliptic maps	Complexity, implementation, performance, security, algorithmic intricacies, and standardization might pose issues in their practical usage.
[24]	Elliptic Curve Diffie-Hellman key	Weak key management practices could lead to security vulnerabilities

3 Proposed Model

Recognizing the significance of cryptographic methods in medical imaging, we aim to introduce an algorithm for a comprehensive encryption strategy. This strategy, known as a Multi-Faceted Encryption Approach, is designed specifically to secure patient information within medical imaging systems. Its primary objectives are to adhere to strict data privacy regulations in healthcare, safeguard sensitive patient data, and uphold the reliability and trustworthiness of these medical imaging systems.

In essence, the proposed algorithm orchestrates a comprehensive encryption process, commencing with hash code generation to validate image integrity, embedding the hash code through feature-based watermarking, transforming the image into the frequency domain via DCT, encrypting the frequency domain image using AES, and culminating in additional security layers through RSA encryption. Each step contributes significantly to fortifying the image against unauthorized access, tampering, or interception during transmission, thereby ensuring the confidentiality, integrity, and authenticity of sensitive medical data contained within the images.

Implementing this algorithm mandates attention to cryptographic best practices, robust implementation of encryption algorithms, secure key management, and compliance with industry standards to fortify the confidentiality and integrity of medical images, crucial in safeguarding patient privacy and maintaining data integrity in healthcare systems.

Medical images hold sensitive and confidential information, necessitating robust encryption techniques to ensure privacy and integrity during storage or transmission. This algorithm employs a multi-layered approach, beginning with extracting a cryptographic hash code using the SHA-256 algorithm. The hash code, represented as 'h', is a unique fingerprint for the original image 'X'. This mathematical representation enables verification of the image's integrity by comparing 'h' before and after encryption.

Following hash code generation, the algorithm embeds 'h' into the image 'X' through feature-based watermarking. Feature-based watermarking techniques subtly modify specific image features without significantly altering their visual appearance. This embedding process, denoted as 'Y = WatermarkFeature(X, h)', ensures that the hash information becomes imperceptibly integrated into the image. This step fortifies the image against tampering or unauthorised modifications by concealing the hash code within its features.

Subsequently, the algorithm transitions the image 'Y' into the frequency domain using the Discrete Cosine Transform (DCT), denoted as 'Z = DCT(Y)'. This transformation facilitates the conversion of the image data from the spatial domain to the frequency domain, expressing it as a set of cosine functions. The use of DCT enables effective representation of image content in a manner conducive to subsequent encryption processes, laying the groundwork for enhanced security measures.

The encrypted frequency domain image 'Z' undergoes encryption using the Advanced Encryption Standard (AES) algorithm. AES encryption, employing a symmetric key, 'AES_Key', secures the transformed image data. The symmetric key is critical in safeguarding the image content, ensuring confidentiality and preventing unauthorised access to the encrypted data. The resultant encrypted data 'E = AES_Encrypt(Z, AES_Key)' ensures the image's confidentiality and privacy during storage or transmission.

Further fortifying the encryption, the algorithm applies RSA encryption, a widely used asymmetric cryptographic technique. RSA encryption involves using public and private keys, ensuring secure transmission of sensitive information. The encrypted data 'E' is encrypted again using the recipient's

RSA public key, generating 'F = RSA_Encrypt(E, RSA_Public_Key)'. This multi-layered encryption enhances the security posture of the medical image by employing both symmetric and asymmetric encryption mechanisms.

Encryption Algorithm

Step1: Read Medical Image (X)

Step 2: Generate a cryptographic Hash(h)

H=Hash(X)

- 'X' is the original image.
- 'h' represents the hash code generated using a cryptographic hash function (e.g., SHA-256).

Step 3: Apply WaterMarking for embedding Y

Watermarking Algorithm : Y = Watermark(X,h)

- 'Y' results from embedding the hash code 'h' into the image 'X' using watermarking techniques.
- The watermarking algorithm could involve altering pixel values or image features to encode the hash information.

Step 4: Convert Image to Frequency Domain (Z):

Frequency Transform: Z=FrequencyTransform(Y)

- The operation transforms the image 'Y' into the frequency domain, representing it as 'Z'.
- Mathematical transformations like Discrete Fourier Transform (DFT) or Discrete Cosine Transform (DCT) might be used.

Step 5: Apply Encryption Algorithm (E):

Encryption: E=Encrypt(Z,K)

- 'E' denotes the result of applying an encryption algorithm to the frequency domain representation 'Z' using a key 'K'.
- This step might involve symmetric encryption (e.g., AES) or homomorphic encryption for securing the image data.

Step 6:Apply Key-Based RSA Encryption (F):

RSA Encryption: F=RSAEncrypt(E,RSAPublicKey)

- 'F' represents the encrypted data obtained by applying RSA encryption to 'E' using the public RSA key.
- RSA encryption secures 'E' using the recipient's RSA public key.

Step 7:Output Encrypted Image (F)

Decryption Algorithm

Step 1:Read the Encrypted Image (F):

Step 2: Apply Key-Based RSA Decryption (E'):

RSA Decryption:

E′=RSADecrypt(F,RSA_Private_Key)

- 'E" represents the decrypted data obtained by applying RSA decryption to 'F' using the recipient's RSA private key.
- RSA decryption retrieves the AES encrypted frequency domain data 'E'.

Step 3: Apply AES Decryption Algorithm (Z'):

AES Decryption:

Z′=AESDecrypt(E′,AES_Key)

- 'Z" denotes the decrypted frequency domain image 'Z' using AES decryption with the symmetric key 'AES_Key'.
- AES decryption retrieves the transformed image data in the frequency domain.

Step 4: Convert Image from Frequency Domain using IDCT (Y'):

IDCT Transformation:

$Y' = IDCT(Z')$

- 'Y" represents the image 'Y' obtained by inverse Discrete Cosine Transform (IDCT) applied to 'Z".
- IDCT converts the frequency domain image 'Z" back to the spatial domain image 'Y'.

Step 5:Verify Watermark and Extract Hash Code (h'):

Watermark Extraction:

$h' = h' = ExtractWatermarkFeature(Y')$

- 'h" denotes the extracted hash code 'h" from the image 'Y" using watermark extraction.
- Watermark extraction retrieves the embedded hash information from the spatial domain image 'Y".

Step 6 Verify Hash Integrity:

Compare Hash Codes:

$(h, h')Match = CompareHashes(h, h')$

- 'Match' indicates whether the original hash code 'h' matches the extracted hash code 'h".
- Comparison checks the integrity by verifying if the extracted hash 'h" matches the initially generated hash 'h'.

Step 7 Output Decrypted Image (Y'):

4 Performance Evaluation

4.1 Analysis

Enforcing this algorithm requires a focus on adhering to best cryptographic practices, ensuring robust implementation of encryption algorithms, maintaining secure key management, and complying with industry standards. These efforts are vital in strengthening the confidentiality and authenticity of medical images, playing a pivotal role in protecting patient privacy and preserving data integrity within healthcare systems.

Importance of Hashing

The algorithm initiates the generation of a cryptographic hash code using the SHA-256 algorithm. The significance of hashing lies in its ability to produce a fixed-size string unique to the input data. In the context of medical images, this hash serves as a digital fingerprint, representing the image without revealing its contents. This fingerprint, 'h', acts as a reference for image integrity. By comparing the hash values before and after encryption, any alterations or unauthorized modifications to the image can be detected.

Integration of Watermarking Techniques

The subsequent step involves embedding the hash code 'h' into the image using feature-based watermarking. This technique strategically alters specific features or attributes within the image, effectively concealing the hash information while preserving the image's visual quality. Feature-based watermarking ensures that the embedded data remains imperceptible to the human eye, safeguarding the integrity of the image against potential alterations or unauthorised access.

Transformation into the Frequency Domain

Transitioning the image 'Y' into the frequency domain via Discrete Cosine Transform (DCT) provides several advantages in encryption. DCT converts the image data from the spatial to the frequency domain,

facilitating better representation and manipulation of the image content. By transforming the image into a set of cosine functions, it prepares the data for subsequent encryption techniques, enhancing the image's resilience against potential attacks.

Strengthening Security through AES Encryption

The encrypted frequency domain image 'Z' undergoes Advanced Encryption Standard (AES) encryption, a symmetric key encryption method known for its robust security measures. AES employs a shared secret key ('AES_Key') to encrypt and decrypt data, ensuring confidentiality during transmission or storage. The use of AES enhances the security posture of the image data, preventing unauthorised access and maintaining confidentiality, which is crucial in protecting sensitive medical information.

Multi-Layered Security via RSA Encryption

To further fortify the encryption, the algorithm employs RSA encryption, an asymmetric cryptographic technique that adds an extra layer of security. RSA encryption involves a pair of keys (public and private), with the public key used for encryption and the private key for decryption. By encrypting the already encrypted data 'E' with the recipient's RSA public key, denoted as 'F = RSA_Encrypt(E, RSA_Public_Key)', the algorithm enhances data security, ensuring confidentiality even if intercepted during transmission.

4.2 Simulation

The efficiency of the suggested encryption technique was assessed through practical testing. This evaluation was conducted on an Intel Core i9 system with 16 GB RAM and a 3.70 GHz processor. A set of 300 digital medical images, comprising six categories with 50 medical images each (including Magnetic Resonance Imaging (MRI), Computed Tomography (CT), X-ray scans., and Ultrasound images sized at 512 × 512), underwent scrutiny. Mecial images were obtained from the "National Library of Medicine’s Open Access Biomedical Images Search Engine" at https://openi.nlm.nih.gov. Figure 1 showcases a compilation of medical images utilized to analyze and appraise the proposed encryption method. These images serve as the foundation for assessing how well the proposed encryption system works and whether it is appropriate for use in the field of medical imaging.

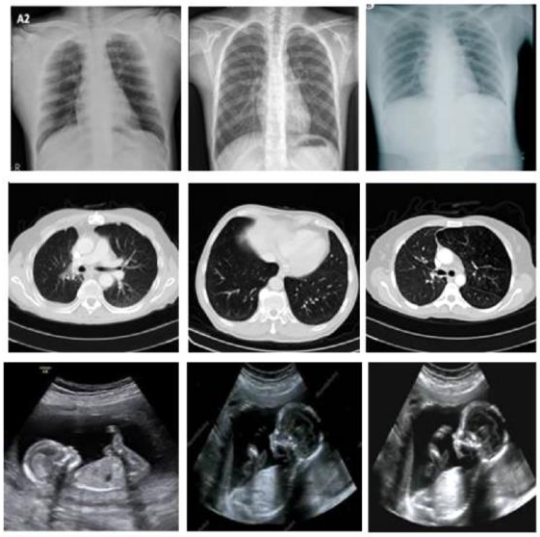

Figure 1: Medical Images Used for the Analysis of the Proposed Scheme

Figure 2 showcases both the original image (a) and its embedded counterpart (b), visually representing the watermarking process. The original image (a) serves as the baseline, while the embedded image (b) demonstrates subtle modifications where the watermark has been seamlessly incorporated into the visual content. This comparison visually illustrates how the watermarking technique subtly alters specific image features without significantly impacting their appearance. Additionally, the corresponding histogram accompanying the images reveals the distribution of pixel intensities, highlighting any changes introduced by the embedding process. The histogram aids in quantitatively assessing the alterations in pixel values caused by the watermarking, offering insights into the impact on the image's tonal distribution and potential perceptual changes. Overall, Figure 2 provides a comprehensive visual and quantitative depiction of the embedded watermark within the image, shedding light on the effectiveness of the watermarking process while preserving the image's visual integrity.

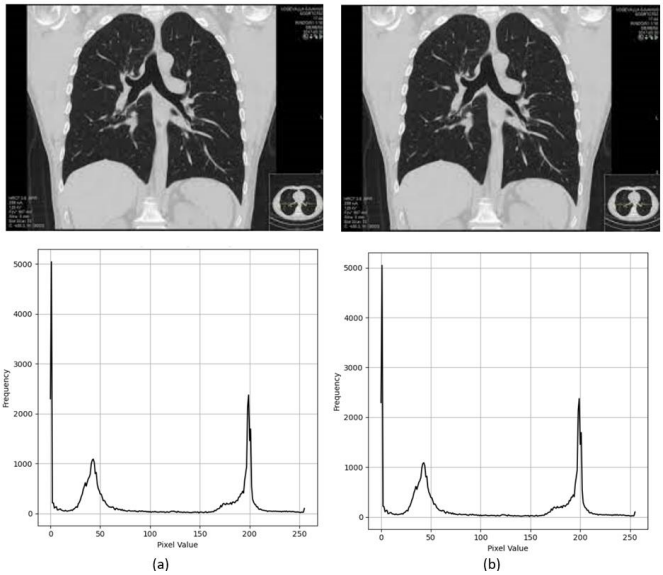

Figure 2: The Original (a) and the Embedded (b) Image and the Corresponding Histogram

Figure 3 compares pixel intensity distributions between the original medical image and the encrypted version after applying the RSA encryption method. This visualisation serves as a crucial analysis tool, shedding light on the alterations in pixel intensity values resulting from the encryption process. By juxtaposing the histograms of the original and encrypted images, this figure offers a clear insight into how the encryption scheme impacts the pixel intensity distribution. The comparison enables a quantitative assessment of potential changes in the image's tonal range, highlighting any shifts or variations introduced by the RSA encryption. Analysing these pixel intensity distributions aids in evaluating the fidelity of the encrypted image concerning the original, ensuring that while sensitive medical data is protected through encryption, the essential diagnostic information within the image remains intact. Figure 3's visual representation of pixel intensity comparisons provides valuable insights into the encryption's impact on image characteristics, facilitating a comprehensive understanding of the algorithm's performance in preserving confidentiality and image integrity within healthcare systems.

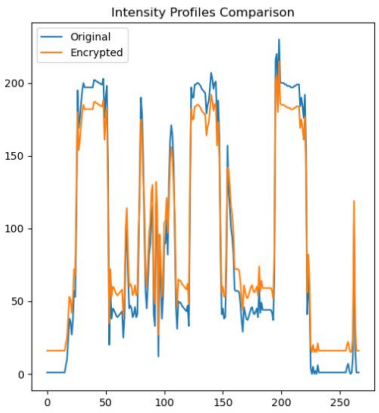

Figure 3: The Pixel Intensity Compares the Original and Encrypted Image After Applying the RSA

4.3 Comparison

This section delves into a comprehensive comparison of various metrics utilised to evaluate the performance and effectiveness of medical image encryption algorithms. In image encryption, assessing the fidelity, security, and robustness of encrypted images is crucial. To this end, several quantitative measures and statistical analyses are employed to gauge the quality and safety of the proposed algorithm.

Peak-Signal-to-Noise Ratio (PSNR): This metric quantitatively assesses encrypted images' quality by measuring the mean square error between the original, unencrypted image (ground truth) and the encrypted image.

$$PSNR = 20\ \log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}||f(i.j) - g(i,j)||^2$$

NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity): These metrics are pivotal in assessing the level of variation and dispersion within encrypted images. NPCR measures the percentage of pixel changes, while UACI quantifies the average intensity change between the original and encrypted images, offering valuable insights into the encryption algorithm's behavior.

$$NCPR = \frac{1}{M * N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) * 100\%$$

$$D(i,j) = \begin{cases} 0, & if\ A(i,j) = B(i,j) \\ 1. & if\ otherwise \end{cases}$$

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|A(i,j) - B(i.j|}{255} * 100\%$$

Entropy: A fundamental measure of randomness and unpredictability in encrypted data, entropy serves as a crucial indicator of the effectiveness of encryption techniques. High entropy signifies increased randomness, making decryption without the proper key significantly more challenging.

$$E = \sum_{i=0}^{255} P(i)\log_2\left(\frac{1}{P(i)}\right)$$

$$P(i) = \frac{Frequecny\ of\ the\ pixel\ value\ i}{Total\ number\ of\ image\ pixels}$$

It is apparent that a comparison with analogous studies can be conducted, encompassing diverse methodologies. This comparison involves assessing the image encryption process by referencing similar works. Subsequently, Table 2 presents the PSNR, NPCR, UACI, and entropy values, focusing on average metrics derived from implementations in various related works.

Table 2: Performance Comparison with other Related Works

Research	PSNR	NPCR	UACI	Entropy
Proposed Algorithm	27.88	0.997	0.283	7.985
[19]	27.813	0.986	0.279	7.908
[20]	27.601	0.979	0.279	7.624
[21]	27.705	0.986	0.281	7.654
[22]	27.516	0.980	0.273	7.638
[23]	27.874	0.981	0.280	7.601
[24]	27.850	0.978	0.276	7.781
[25]	27.771	0.983	0.274	7.857
[26]	27.760	0.984	0.278	7.642

5 Conclusions and Future Work

The proposed encryption algorithm has been meticulously developed to fortify the security of patient information within medical imaging systems. By embracing cryptographic methodologies tailored specifically for medical imaging, this approach upholds paramount objectives: compliance with stringent healthcare data privacy regulations, protection of sensitive patient data, and the unwavering assurance of reliability and trustworthiness in medical imaging systems.

Upon comparison with cutting-edge encryption methods, the suggested encryption approach displays characteristics akin to a robust cipher. Through a commendable encryption assessment, yielding high values in Peak Signal-to-Noise Ratio (PSNR), Non-Probabilistic Convergence Ratio (NPCR), and Unified Average Changing Intensity (UACI), coupled with a substantial entropy value, the proposed encryption method showcases considerable resilience and effectiveness in preserving the confidentiality and integrity of critical medical data. This amalgamation of statistical and security analyses reaffirms the strength and efficiency of the proposed encryption approach, highlighting its potential as a fundamental component in securing patient information within medical imaging systems.

Author Contributions: Idea development, approach, detailed analysis, research, and initial drafting by A.O.; A.A. and A.O. contributed to editing and revising the written content. All authors have reviewed and approved the manuscript for publication.

Acknowledgments: The authors express their genuine appreciation to Princess Sumaya University for Technology for their assistance and support throughout this project.

Conflicts of Interest: The authors declare no conflicts of interest.

References

[1] Aram, S., Shirvani, R. A., Pasero, E., & Chouikha, M. F. (2016). Implantable Medical Devices; Networking Security Survey. *Journal of Internet Services and Information Security (JISIS)*, *6*(3), 40-60.

[2] Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. *International Journal of Business Intelligence and Big Data Analytics*, *6*(1), 1-11.

[3] Behnia, S., Akhavan, A., Akhshani, A., & Samsudin, A. (2013). Image encryption based on the Jacobian elliptic maps. *Journal of Systems and Software*, *86*(9), 2429-2438.

[4] Cheng, Z., Wang, W., Dai, Y., & Li, L. (2022). A High-Security Privacy Image Encryption Algorithm Based on Chaos and Double Encryption Strategy. *Journal of Applied Mathematics*, *2022*.

[5] Dzwonkowski, M., Papaj, M., & Rykaczewski, R. (2015). A new quaternion-based encryption method for DICOM images. *IEEE Transactions on Image Processing*, *24*(11), 4614-4622.

[6] El-Latif, A.A.A., Ramadoss, J., Abd-El-Atty, B., Khalifa, H.S., & Nazarimehr, F. (2022). A novel chaos-based cryptography algorithm and its performance analysis. *Mathematics*, *10*(14), 1-22.

[7] Ferdush, J., Begum, M., & Uddin, M.S. (2021). Chaotic lightweight cryptosystem for image encryption. *Advances in Multimedia*, *2021*, 1-16.

[8] Furukawa, M.F., King, J., Patel, V., Hsiao, C.J., Adler-Milstein, J., & Jha, A.K. (2014). Despite substantial progress in EHR adoption, health information exchange and patient engagement remain low in office settings. *Health Affairs*, *33*(9), 1672-1679.

[9] Gold, M., & McLaughlin, C. (2016). Assessing HITECH implementation and lessons: 5 years later. *The Milbank Quarterly*, *94*(3), 654-687.

[10] Gururaj, H. L., Almeshari, M., Alzamil, Y., Ravi, V., & Sudeesh, K. V. (2023). Efficient SCAN and Chaotic Map Encryption System for Securing E-Healthcare Images. *Information*, *14*(1), 1-15.

[11] Hamza, N.A., Jafeer, S.H., & Ali, A.E. (2019). Encrypt 3d model using transposition, substitution, folding, and shifting (tsfs). *In IEEE 2nd Scientific Conference of Computer Sciences (SCCS)*, 126-131.

[12] Jouini, M., & Rabai, L.B.A. (2019). A security framework for secure cloud computing environments. In *Cloud security: Concepts, methodologies, tools, and applications*, 249-263. IGI Global.

[13] Kaissis, G.A., Makowski, M.R., Rückert, D., & Braren, R.F. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. *Nature Machine Intelligence*, *2*(6), 305-311.

[14] Kumar, M., Iqbal, A., & Kumar, P. (2016). A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. *Signal Processing*, *125*, 187-202.

[15] Li, L., Abd El-Latif, A.A., & Niu, X. (2012). Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. *Signal Processing*, *92*(4), 1069-1078.

[16] Lite, S., Gordon, W.J., & Stern, A.D. (2020). Association of the meaningful use electronic health record incentive program with health information technology venture capital funding. *JAMA network open*, *3*(3), 1-10.

[17] Nosrati, S., Sabzali, M., Heidari, A., Sarfi, T., & Sabbar, S. (2020). Chatbots, counselling, and discontents of the digital life. *Journal of Cyberspace Studies*, *4*(2), 153-172.

[18] Panayides, A.S., Amini, A., Filipovic, N.D., Sharma, A., Tsaftaris, S.A., Young, A., & Pattichis, C.S. (2020). AI in medical imaging informatics: current challenges and future directions. *IEEE journal of biomedical and health informatics*, *24*(7), 1837-1857.

[19] Pollard, J.M. (1978). Monte Carlo methods for index computation (*modp*). *Mathematics of computation*, *32*(143), 918-924.
[20] Ramzan, M., Habib, M., & Khan, S.A. (2022). Secure and efficient privacy protection system for medical records. *Sustainable Computing: Informatics and Systems*, *35*.
[21] Rasool, R.U., Ahmad, H.F., Rafique, W., Qayyum, A., & Qadir, J. (2022). Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. *Journal of Network and Computer Applications*, *201*.
[22] Reisman, M. (2017). EHRs: the challenge of making electronic data usable and interoperable. *Pharmacy and Therapeutics*, *42*(9), 572-575.
[23] Shukla, S., George, J. P., Tiwari, K., & Kureethara, J.V. (2022). *Data Ethics and Challenges*. Springer, 41-59.
[24] Singh, S., Hosen, A.S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access*, *9*, 13938-13959.
[25] Tawalbeh, L.A., Mowafi, M., & Aljoby, W. (2013). Use of elliptic curve cryptography for multimedia encryption. *IET Information Security*, *7*(2), 67-74.
[26] Teh, J.S., Alawida, M., & Sii, Y.C. (2020). Implementation and practical problems of chaos-based cryptography revisited. *Journal of Information Security and Applications*, *50*, 1-41.
[27] Wadi, S.M., & Zainal, N. (2014). High definition image encryption algorithm based on AES modification. *Wireless personal communications*, *79*, 811-829.
[28] Yao, F. (2021). Hybrid Encryption Scheme for Hospital Financial Data Based on Noekeon Algorithm. *Security and Communication Networks*, *2021*, 1-10.
[29] Yap, W.S., Phan, R.C.W., & Goi, B.M. (2016). Cryptanalysis of a high-definition image encryption based on AES modification. *Wireless Personal Communications*, *88*(3), 685-699.
[30] Yu, F., Qian, S., Chen, X., Huang, Y., Cai, S., Jin, J., & Du, S. (2021). Chaos-based engineering applications with a 6D memristive multistable hyperchaotic system and a 2D SF-SIMM hyperchaotic map. *Complexity*, *2021*, 1-21.
[31] Zhang, J., Li, G., Marshall, A., Hu, A., & Hanzo, L. (2020). A new frontier for IoT security emerging from three decades of key generation relying on wireless channels. *IEEE Access*, *8*, 138406-138446.

Authors Biography

Ammar Odeh received his Ph.D. Degree in Computer Science and Engineering with a concentration in Computer Security (Steganography) from the University of Bridgeport. He received an M.S. in Computer Science with a concentration in Reverse Software Engineering and Computer Security from the University of Jordan, College of King Abdullah II School for Information Technology (KASIT). In 2002, he finished his B.Sc. Degree in Computer Science and applications from the Hashemite University, Prince Al-Hussein Bin Abdullah II for Information Technology. During his Ph.D., he worked as a Research Assistant, Teaching Assistant, and Instructor. He is currently an assistant professor in computer science at Princess Sumaya University for Technology.

Anas Abu Taleb is an associate professor in the Department of Computer Science at Princess Sumaya University for Technology, Amman, Jordan. He received a Ph.D. in Computer Science from the University of Bristol, UK, in 2010, an MS.c. in Computer Science from the University of the West of England, UK, 2007 and a BS.c. Degree in Computer Science from Princess Sumaya University for Technology, Jordan, 2004. Dr. Abu Taleb has published several journal and conference papers on sensor networks. In addition to sensor networks, Dr. Abu Taleb is interested in network fault tolerance, routing algorithms, and mobility models.