IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 29, No. 2, April, 2024, pp. 599-608
Journal homepage: http://iieta.org/journals/isi

# Improved Vigenere Cipher-RSA-Based Medical Image Security Through Multiple Encryption Keys

Fairouz Hadi[1*], Yacine Slimani[2], Amel Douar[1], Adel Alti[1], Farah Saoud[3], Maroua Harkati[3]

[1] Networks and Distributed Systems Laboratory (LRSD), Computer Science Department, Ferhat Abbas University Sétif 1, Sétif 19000, Algeria
[2] Laboratory of Intelligent System (LSI), Faculty of Technology, Ferhat Abbas University Sétif 1, Sétif 19000, Algeria
[3] Computer Science Department, Ferhat Abbas University Sétif 1, Sétif 19000, Algeria

Corresponding Author Email: fairouz.hadi@univ-setif.dz



https://doi.org/10.18280/isi.290221

**Received:** 27 July 2023
**Revised:** 23 February 2024
**Accepted:** 25 March 2024
**Available online:** 25 April 2024

***Keywords:***
*cryptography, encryption and decryption, medical images, DICOM, RSA, security, transmission, Vigenere cipher*

**ABSTRACT**

With the rapid evolution of telecommunication technologies, new means to share patients' medical images have consistently developed, leading to changes in their protection strategies. Consequently, researchers are paying attention to increasing security and privacy of sensitive medical images. However, brute-force, geometric and non-geometric attacks and unlawful manipulation have occurred in recent years. This paper attempts to propose a robust and hybrid encryption approach using improved Vigenere cipher and RSA that helps enhance security and integrity in medical images and protect sensitive data. The medical images come from different modalities such as X-ray, CT and MRI. The traditional public and private keys for the RSA algorithm is enhanced by adding a second key to the medical image. The second key and RSA keys are used to encode and decode the image which makes the decryption process considerably more difficult with correct key combinations. By incorporating the second key, the proposed approach addresses the challenges related to confidentiality and security in medical image transmission. Therefore, the proposed approach shows promising results in enhancing security and providing good performance of image encryption/decryption processes.

## 1. INTRODUCTION

As Internet and communication technologies have rapidly developed, transmission of images in general, and medical images in particular, has become increasingly prevalent and plays a crucial role in information transmission, especially since the COVID-19. The transfer of images among healthcare professionals is essential to avoid physical contact and ensure efficient collaboration [1]. However, the security of image transmission and storage is a significant concern that requires ongoing attention. As medical images contain sensitive patient information, ensuring their confidentiality and integrity is paramount. The unauthorized access, interception, or tampering of these images could lead to privacy breaches and compromised patient care.

Encryption has proven to be one of the most effective solutions throughout history for ensuring the confidentiality and security of information. By encrypting medical images, sensitive data can be protected from unauthorized access and potential breaches. During encryption, cryptographic algorithms and keys are used to convert the images into an unreadable format, increasing the difficulty of interpretation of image content by unauthorized users.

Cryptography systems can be mainly categorized into asymmetric and symmetric encryption. Asymmetric encryption uses two keys: a public and a private one [2]. A public key is distributed publicly while a private key is kept confidential by their holders. With symmetric encryption, anyone can encrypt the data, the public key is used to encrypt data, but only the recipient who has the private key can decrypt it. Asymmetric encryption provides confidentiality, sender authentication and digital signatures. RSA is a frequently used asymmetric encryption algorithm. For symmetric encryption, both encryption and decryption are performed using the same key [3]. At the outset, standard encryption techniques are used to ensure the security of textual information, like DES (Data Encryption Standard), AES (Advanced Encryption Standard), and 3DES (Triple Data Encryption Standard). Symmetric encryption also called as private-key encryption, is effective and fast and therefore ideal for encrypting large amount of data.

In the field of medical image transmission, encryption provides an additional layer of security, safeguarding the confidentiality of patient data and preventing unauthorized interception or tampering. It allows medical professionals to ensure the privacy and integrity of medical. As technology continues to advance, the development of robust encryption methods and techniques remains crucial to address the evolving challenges of sensitive information privacy and medical image security.

Among these challenges, we can mention: sophisticated cybercrime [4], the increasing number of data breaches [5], privacy protection [6], user awareness and training [7], etc.

Confidentiality, securing medical image content, integrity and privacy of such data have become serious challenges. These challenges require constant efforts to enhance security measures, develop data protection strategies, strengthen user awareness and training, and adopt regulatory compliance practices to address the growing threats and risks in information security. Researchers and developers continue to explore new symmetric and asymmetric encryption algorithms, Post-Quantum Cryptography (PQC) [8], Homomorphic Encryption (HE) [9], Fully Homomorphic Encryption (FHE) [10], and Elliptic Curve Cryptography (ECC) [11] to reinforce the security and privacy of medical image contents and patient data in an increasingly networked world. Besides several standard encryption techniques have been developed and improved to secure sensitive data and medical images [12-16]. The Caesar cipher is one of the earliest known encryption techniques [17]. The Vigenere cipher is an extension of the Caesar cipher. Data Encryption Standard (DES) became the standard encryption algorithm for several decades [18]. Advanced Encryption Standard (AES) has succeeded DES and became the standard encryption technique for several applications [19]. Triple Data Encryption Standard (3DES) is a modification of the original DES algorithm that applies DES three times to each block of data [20]. It offers increased security through the use of multiple chippers, which makes it more robust to brute force. One of the shortcomings of existing encryption methods is the lack of robustness, which can lead to several serious attacks and unlawful manipulation. These encryption techniques paved the way for the development of more advanced algorithms like RSA, which revolutionized modern cryptography by introducing public-key encryption.

RSA encryption is one of the most widespread methods in the field of security. With the study by Rivest et al. [2] on the encryption and decryption of texts, it gained in importance. It offers a high degree of security based on the factorization of large prime numbers. However, RSA presents a serious weakness in terms of hardware utilization and high computational time. Encrypting/decrypting images with RSA [21] poses additional challenges compared to text encryption/decryption. Since images are typically larger and more complex than textual data, they require more time and resources in the encryption/decryption processes. With the latest advancements in computer hardware including faster processors and powerful computers, the performance of RSA has improved [2]. While encrypting/decrypting images with RSA may be more resource-intensive compared to text, technological advancements and optimization techniques such as hybrid encryption [22], chunking and parallel processing [23], compression techniques [24], hardware acceleration [25] and optimized implementations [26] can help mitigate these issues and make the use of RSA for images more practical.

This paper proposes a new robust and hybrid cryptosystem for medical images based on enhanced Vigenere cipher and RSA algorithm. Our objective is to achieve high performance and high security of transmitted medical images. By incorporating a second image key, the proposed approach increases the privacy of sensitive data and addresses the challenges related to the confidentiality and security of medical images. Additionally, it makes medical data available while respecting patients' privacy rights and ensuring secure management of sensitive information by employing a second key and RSA public/private keys for image coding and decoding processes. However, the second key whose role is to enhance the security level of sensitive data. This key is used in the improved Vigenere cipher and RSA algorithm to ensure secure and strong medical image transmission in unsecured networks. The details of the contributions are as follows:

- Development of a new encryption system for medical images based on an improved Vigenere cipher and an RSA algorithm to ensure confidentiality and high security of the data. First, we apply the improved Vigenere cipher on the host image to produce the encrypted image. The encrypted image is then encrypted based on RSA using the second key. Finally, the encrypted data are decoded using the same encryption steps. The encrypted image content results in secure and robust encoded bits while knowing two secret keys requires infinite attempts. Thus, the proposed system leverages a good level of security for sensitive data.
- Experiments were conducted on medical image datasets with various modalities [27]. The results were encouraging and demonstrate that proposed technique super passes some newer encryption methods in terms of visual perception, performance, and protection degree of sensitive data. In addition, the proposed technique outperforms some recent security methods in terms of imperceptibility, performance, and protection degree of image content.

The structure is set up: The existing works in the field of medical image security is provided in Section 2. Section 3 explains the proposed medical images encryption approach based on symmetric and asymmetric cryptography with the addition of a second encryption key. In Section 4, the findings and analyses are given. Finally, section 5 concludes this paper and outlines some perspectives.

## 2. RELATED WORKS

Lakshmi et al. [14], presented medical image encryption by introducing a diffusion mechanism based on DWT (Discrete Wavelet Transform) and fuzzy composition. This purpose is intended to identify regions of interest to incorporate the encrypted watermark into DICOM images to achieve a strong medical encryption schema. The proposed approach gave more interesting results in terms of security and robustness. Through their proposed work, they combined watermarking and encryption techniques which led to considerable execution time.

Soualmi et al. [15] presented a blind multi-watermarking approach for medical images by hiding two watermarks in two different domains. The first watermark is incrusted in the frequency domain and the second watermark in the spatial domain using LWT, QR decomposition, and chaotic systems. This method provides interesting findings in terms of image fidelity and robustness. However, the payload is mediocre.

Kumar et al. [16] presented a hybrid approach that used cryptography, steganography, and watermarking to protect the medical images X-ray, Ultrasound, and CT scan. This method provides excellent analysis of privacy, security, and transmission of medical data reduction. However, the approach did not deal with computational complexity and false positive.

Maity et al. [28] combined symmetric and asymmetric encryption. Asymmetric encryption is performed using RSA method. A simple text of size 64 bits is encoded with a key of size 64. The modified Caesar cipher is used as a symmetric cipher and adapted for a more secure level. The results obtained were good and confirmed the precision, efficiency and privacy of this algorithm in tackling complex problems.

Despite these strengths, the algorithm is not free of flaws. One of the biggest weaknesses of this work relates to the key exchange process between sender and receiver. It was not secure enough and could be exploited as a security vulnerability.

Edan et al. [29] presented an algorithm for image encryption based on the RSA, which is known for its robust asymmetric encryption. The system splits the image into blocks of size 2×2 to enhance the encryption process. Each block is transformed into a vector, which is in turn converted to a binary, resulting in one binary number. This number is then transformed into decimal numbers to ensure compatibility with the cryptosystem RSA. The reliability, security, and suitability for image protection of this algorithm perform better through experiments in the MATLAB environment. Leveraging RSA's strength, the algorithm ensures secure transmission and protection for grayscale and color images over Internet. The lossless nature of the algorithm maintains data integrity, making it a promising solution for image encryption during COVID-19 and beyond. Unfortunately, this research seems to lack medical image encryption, although it is mentioned in the paper.

Xu et al. [30] proposed a solution that utilizes the Hadoop open-source project to design and study a distributed RSA encryption algorithm. They implemented module partitioning and process control to enable distributed encryption of data. Testing on a large-scale distributed cluster demonstrated the algorithm's efficiency in processing massive data. The use of Hadoop and the distributed nature of the RSA encryption algorithm offer scalability, efficiency, and data security benefits for handling large volumes of medical data. Although the paper primarily focused on testing the feasibility and efficiency improvements of distributed RSA encryption, future work could involve integrating this approach into real-world applications for encrypting massive data. Additional research and development would be needed to evaluate the system's performance and security in practical scenarios.

Zhang et al. [31] introduced MPVCNet, a privacy-friendly recognition network model for care images. They utilize Visual Cryptography (VC) to share and secure image transmission. This ensures privacy protection while minimizing performance loss. MPVCNet leverages VC's secret-sharing characteristics to transmit images securely in clear text, safeguarding privacy. To address VC's vulnerability to forgery, they use the advantages of both approaches: blind watermarking and trustworthy data processing. This enhances the authenticity and integrity of shared images by embedding verification information. Additionally, transfer learning is used to mitigate the side effects of visual cryptography, maintaining trustworthiness and recognition performance of recognition networks. Experimental results demonstrate that MPVCNet effectively preserves medical image privacy while maintaining recognition network performance. Although promising further evaluation and validation are needed for real-world applications.

Gutub [32] focus on ensuring the confidentiality of grayscale health images in the medical field. They propose a method that uses resilient randomization and XOR operations for image encryption. Various random generators are evaluated to identify the most effective one, adapting dynamically to e-health image variations. The authors explore different randomization structures as two consecutive encryption methods, employing substitution and transposition techniques. By testing various random variations, they successfully encrypt different medical grayscale images and provide valuable insights. The authors emphasize the flexibility of the most suitable pseudorandom number generator (PRNG) and its adaptive properties that improve privacy and mental security for medical grayscale images. This research offers promising opportunities for enhanced privacy and security measures in e-health applications.

Hameed and Sadeeq [33] introduced an innovative encryption strategy to ensure secure data exchange by enhancing data security through a novel key generation process. They avoided repeating keys and expanded the traditional Vigenere table of size 26×26 to 95×95, encompassing a wider range of characters. Their modified Vigenere cipher exhibited higher trust levels compared to the regular cipher when reconfiguring keys. The improvement was achieved by generating more random and unique keys using a function, instead of repeating the key. The evaluations based on the coincidence index and the calculation of entropy showed the superiority of their approach over other algorithms tested. Overall, their method holds promising potential for enhancing data security and encryption effectiveness.

## 3. PROPOSED MEDICAL IMAGE CRYPTOSYSTEM

The main goal of the proposed medical image cryptosystem is to strengthen the security of medical images based on an improved Vigenere cipher and RSA. The medical images have undergone a variety of attacks to evaluate the performance of the proposed system in terms of visual perception and robustness based on well-known metrics.

The proposed system aims to ensure the confidentiality of medical images and protect them from unauthorized access. During encryption, the images are converted into an opaque format that makes it hard for unauthorized persons to interpret the content.

Besides, we developed a corresponding decryption process to allow authorized users to retrieve original images from the encrypted format. This will ensure that the images can be securely accessed and interpreted by the intended recipients.

### 3.1 Types of used images

To evaluate the effectiveness of the suggested scheme, different types of images commonly found in medical imaging have been used. These images are generated through different modalities and provide important diagnostic information. The types of used images are as follows [31]:

- Ultrasound Images: Ultrasound technology uses high-frequency sound waves to visualize internal body structures. Ultrasound images are often used in obstetrics, cardiology and numerous other medical specialties.
- X-ray Images: uses ionizing radiation to scan images of tissues and bones. X-rays often used to diagnose bone fractures, lung disease and to detect abnormalities in various areas of the body.
- CT Scan Images: CT (Computed Tomography) scans use X-ray technology and computer processing to produce detailed cross-sectional images of the body, known as CT scan images. CT scans are useful for detecting health problems in organs, blood vessels and bones.
- MRI Images: MRI utilizes a powerful magnetic field and radio waves to generate detailed images of the internal structure of the body. MRI is particularly suitable for imaging

soft tissues, organs and the central nervous system.

By working with these different types of medical images [34] that are often available in Digital Imaging and Communications in Medicine (DICOM), we aim to evaluate the effectiveness and applicability of our encryption and decryption system in different imaging modalities. This will enable us to assess the system's performance and robustness in different clinical situations and ensure its compatibility with different image formats. Some of the images used in our algorithm are illustrated in Figure 1.


**Figure 1.** Sample used images

### 3.2 Improved Vigenere cipher

The Vigenere cipher is a method of encoding alphabetic text by using multiple Caesar cipher shifts in a 26×26 matrix [17]. It was named after its inventor, Blaise de Vigenere, who lived during the sixteenth century. The Vigenere cipher uses a collection of mono-alphabetic substitution rules, involving Caesar ciphers with shifts ranging from 0 to 25. Initially considered unbreakable, it remained so until 1917. The encryption method involves combining the index of each plaintext character with the index of the corresponding password character using the Vigenere square. As a form of symmetric encryption, it utilizes private-key encryption for securing the ciphertext. Figure 2 shows the principals of Vigenere.

The Vigenere cipher's encoding and decoding processes of the Vigenere cipher are defined by Eq. (1) and Eq. (2):

$$\mathrm{CT} = (\mathrm{PT} + \mathrm{key})\%26 \quad (1)$$

$$\mathrm{PT} = (\mathrm{CT} - \mathrm{key})\%26 \quad (2)$$

where, CT, PT stand for the encrypted and original text, with Key being the secret used for encryption.

Our work aims to improve Vigenere cipher [33] for covering all key combinations by extending the original 26-character Vigenere cipher to a 95-character case-sensitive version, which incorporates numerals and other commonly used English symbols.

By referring to the formulas provided as Eq. (3) and Eq. (4), one can grasp the encryption and decryption process of the improved Vigenere cipher [33]:

$$\mathrm{CT} = (\mathrm{PT} + \mathrm{key})\%95 \quad (3)$$

$$\mathrm{PT} = (\mathrm{CT} - \mathrm{key})\%95 \quad (4)$$

where, CT, PT stand for the encrypted and original text, with Key being the secret used for encryption.

Vigenere cipher is a very promising approach in information security that focuses on protecting the data sensitivity that an image may have. Vigenere cipher is extended through 95-characters case-sensitive version which improves the security and robustness. Nevertheless, the Vigenere cipher can be susceptible to brute-force attacks. A brute force attack could lead to unauthorized access and result in significant alteration or theft of sensitive and personal information in medical images.

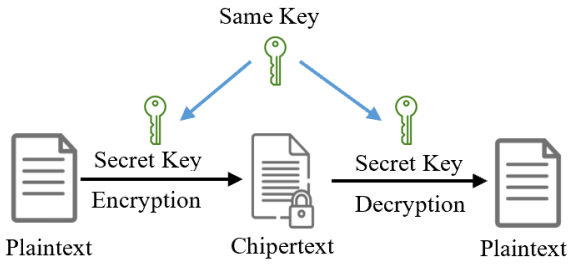



**Figure 2.** The principals of Vigenere cipher [17]

### 3.3 The RSA method

The RSA [2] algorithm, developed by Rivest, Shamir and Adleman, is a commonly used form of asymmetric encryption that can be used to protect medical images. It relies on the mathematical properties of prime numbers and standard arithmetic.

In the RSA [2] method, the first step is to create a set of keys that are mathematically linked: a public key and a private key. The public key is used to encrypt data, while the private key, is used to decrypt encoded data. The second step is to encrypt an original image, the sender uses the recipient's public key (Figure 3). This process converts the image into an encrypted format that requires the specific private key for decryption. Ultimately, the receiver employs their personal key to decipher the encoded image. The RSA algorithm offers strong security for encrypting and decrypting data. The main advantage comes from the challenge of breaking down large numbers into their prime factors, which is the basis of RSA's security.

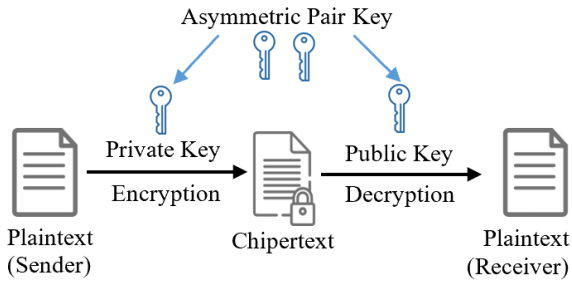



**Figure 3.** The principals of the RSA method [2]

The RSA keys are 1024 or 2048 bits. The steps of the key generation process are given below:

1. Select two large prime numbers $p$ and $q$.
2. Compute $n = p \times q$ and $\varphi(n) = (p-1) \times (q-1)$.
3. Select a number $e$ with $e$ in $[1, \varphi(n)]$.
4. Compute $d = e - 1\ mod\ (p-1) \times (q-1)$.
5. Make private key pairs as $(n, d)$ and public key pairs as $(n, e)$.

The RSA method can contribute to the security of medical images by ensuring that only authorized users possessing the private key can decrypt and access sensitive image data. It provides a reliable mechanism to guarantee the confidentiality and integrity of medical images during image transmission and save. RSA provides good resistance to most attacks by effectively encrypting medical data. However, RSA is

vulnerable to brute force attacks and generates random keys with high complexity in terms of processing despite its efficiency. These limitations make medical image protection in real-time applications a somewhat difficult task.

### 3.4 Medical image cryptography system

The cryptography system proposed in this paper consists of two main phases: image encryption and image decryption. Let's examine the architecture of each phase (Figure 4). Algorithm 1 outlines the steps for encrypting and decrypting messages using the enhanced Vigenère cipher and RSA scheme.

**1) Image encryption phase**

***Inputs:*** *Medical image.*

***Outputs:*** *Image encryption.*

a) Receive the medical images that need to be encrypted from databases.

*b)* Generate and manage the RSA key pairs. Store the private keys and distribute the corresponding public keys to authorized recipients.

c) Encrypt the original image using the improved Vigenère cipher.

*d)* Store the intermediate encrypted image.

e) Convert the intermediate encrypted image into an array of pixels.

f) Apply the RSA encryption algorithm to the array of pixels.

g) Convert the array of pixels to an image format.

h) Store the final encrypted image. ensure that the final encrypted images are protected from unauthorized access and maintain their integrity during storage.

**2) Image decryption phase**

***Inputs:*** *Image encrypted.*

***Outputs:*** *Image decrypted.*

*a)* receive the encrypted image.

*b)* Convert the encrypted image into an array of pixels.

c) Utilize the recipient's private key to decrypt the array of pixels using the RSA decryption algorithm.

*d)* Convert the array of pixels to an image format. store the intermediate decrypted image *a.*

*e)* Decrypt the intermediate decrypted image using the improved Vigenère cipher.

*f)* Deliver the final decrypted images to the authorized recipients.

The architecture of the proposed system follows a clear separation between the encryption and decryption phases. This design model ensures that the sensitive medical images are encrypted and decrypted using the improved Vigenere cipher and RSA algorithm.

**Algorithm 1:** Improved Vigenere cipher and RSA schema

***/* ---------- Key Generation ----------*/***

1. Select two distinct prime numbers, $p$ and $q$ .
2. Compute $n = p \times q$.
3. Compute Euler's function: $\varphi(n) = (p - 1) \times (q - 1)$.
4. Select an integer $e$ such that $1 < e < \varphi(n)$ and $e$ is coprime with $\varphi(n)$.
5. Compute $d$, the modular multiplicative inverse of $e$ modulo $\varphi(n)$, i.e., $d \equiv e^{-1} \pmod{\varphi(n)}$.
6. The public key is $(n, e)$, and the private key is $(n, d)$.

***/* ---------- Encryption ----------*/***

1. Encrypt the original image using the improved Vigenere cipher.
2. Convert the image into a sequence of integers representing the pixels. Turning them into an array of pixels.
3. Compute $C = M^e \bmod n$ (RSA encryption).

***/* ---------- Decryption ----------*/***

6. Compute $M = C^d \bmod n$ (RSA decryption).
7. Convert array of pixels to rebuild the decryption image.
8. Decrypt the encrypted image using the improved Vigenere cipher.

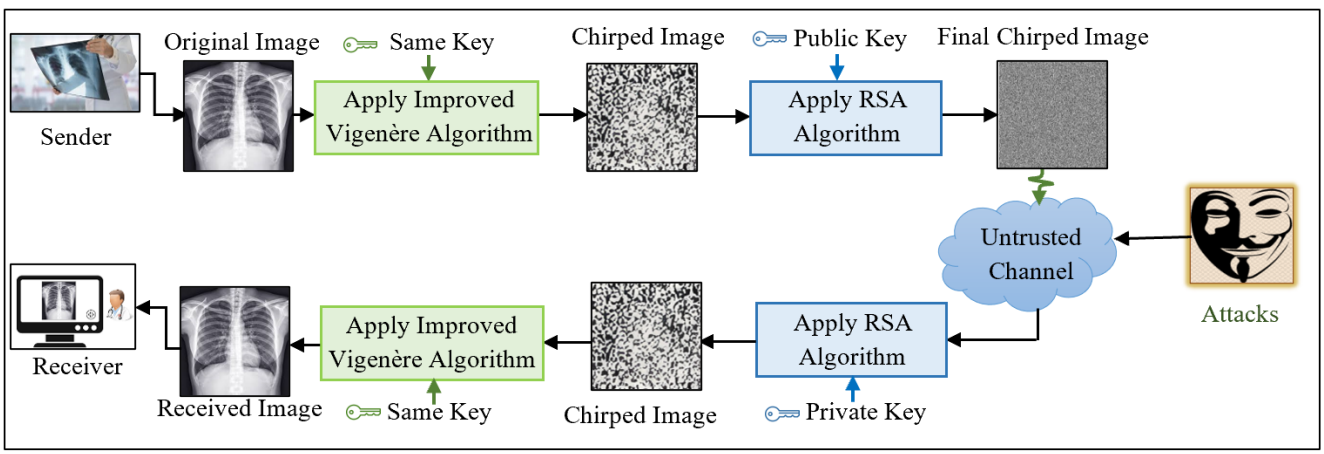



**Figure 4.** The system architecture

### 3.5 Implementation

The main difficulty we encountered when implementing our algorithm was the encryption of image data with the RSA algorithm, which was specially developed for the encryption of numerical or string data. However, in our model, we are attempting to encrypt image data. To solve this problem, we have implemented a method in which the images are converted into a pixel array [35] containing Red Green Blue intensities and then encoded bit by bit. Converting images into pixel

arrays and encrypting them using RSA encryption for more secure image data. By representing the image as an array of pixels with RGB values ranging from 0 to 255, we can apply the encryption algorithm to each pixel individually. By using RSA encryption to encrypt the pixel values, the privacy and accuracy of the image data can be protected. Each pixel value is treated as a separate piece of data to be encrypted, allowing the encryption algorithm to operate on the image data in a bit-by-bit manner.

After the encryption process, it is important to ensure that the resulting encrypted pixel values remain within the valid range of 0 to 255. To achieve this, we performed a modulus 256 operation on the encrypted values, which wraps the values back into the valid range. Once the encryption and modulus operations were completed, we converted the set of pixel values back into an image format. This enables us to see and preview the eventual encrypted image.

Decryption is the opposite of encryption. The encrypted numbers are processed by the decryption algorithm to obtain the decrypted file, which should match the RSA-encrypted file. Upon receiving the decrypted file, it is processed with the RSA decryption algorithm and, if necessary, with the desalination process to retrieve the decrypted pixel values. These pixel values are then reconverted into an image file. If the encryption and decryption algorithms work correctly, the decrypted and converted image file should be identical to the original image. This shows that the integrity of the image has been successfully decrypted and preserved.

In the developed cryptosystem, (1) the medical image is encrypted in the sender's local servers, and (2) after receiving the encrypted medical image via untrusted channel, the recipient decrypts the received data and then performs diagnostic analytics. Encryption and decryption processes are performed using public, private, and secret keys. All these keys are stored in secure locations of the receiver and sender's servers. The sender and receiver exchange public and secret keys with each other via a trusted channel and never exchange their private keys.

Our encryption system requires increased memory usage for multiple encryption keys. This is due to the fact that the machine needs to store additional data about encryption keys and images. Even with higher memory consumption, we maintain a certain level of consistency in terms of processing speed. This is to guarantee the efficiency of the system and ensure that physics receives medical images within a reasonable time and fidelity. Our objective is to create a strong and efficient system that prioritizes robustness, security, memory usage, and processing time to effectively protect against different types of attacks.

In the next section, we will present some findings using the developed crypto-system and discuss the obtained results and outcomings.

## 4. RESULTS AND DISCUSSIONS

Three techniques were used to evaluate the proposed algorithm. Each technique is examined in detail below.

### 4.1 Histogram comparison

Indeed, the histogram of an image [36] is a discrete function that illustrates how intensities are distributed in the image. In the context of image encryption, it is desirable for the encrypted images to have uniform histograms, where all intensities have an equal probability of occurrence. This uniformity helps enhance their resistance to statistical analysis.

Making sure the histogram of the encrypted image is noticeably distinct from the original image, it is difficult for an attacker to gain information from the histogram of the encrypted image. This makes statistical attacks less effective in breaking the encryption and extracting sensitive data.

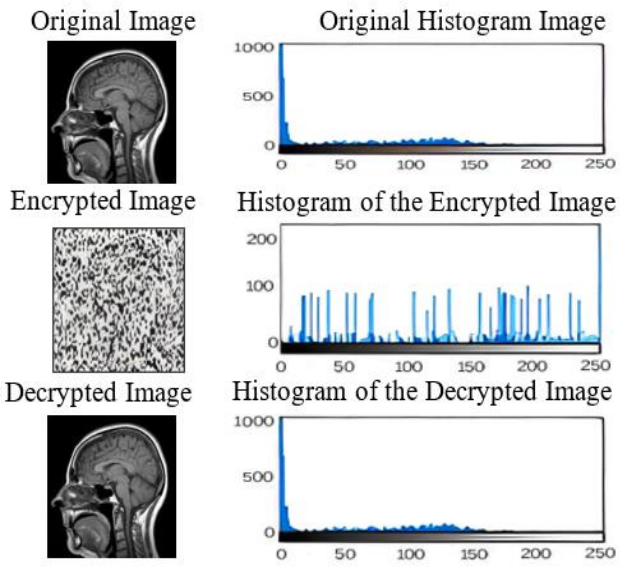
A good encryption algorithm should introduce sufficient randomness and complexity into the encrypted image, in which the resulting histogram appears uniform quasi-uniform. Achieving a uniform histogram can be considered an important aspect of preserving the security and confidentiality of encrypted content.

The obtained results show that (see Figure 5):

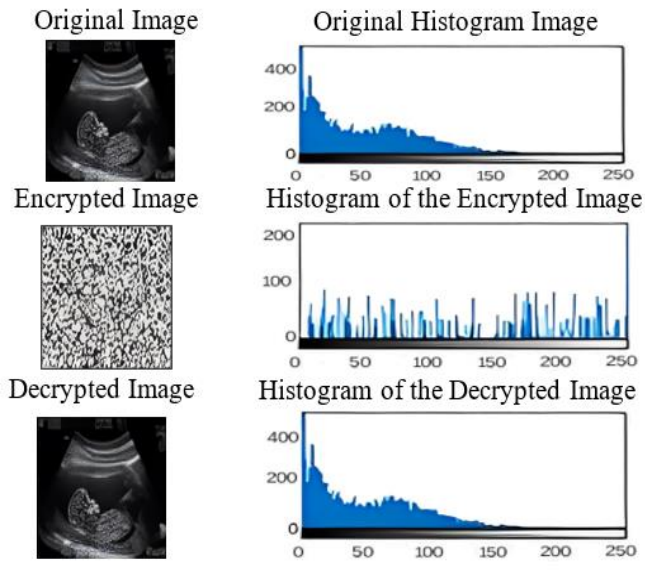
The original images have uniform histograms.

The histograms of the encrypted images are not evenly distributed.

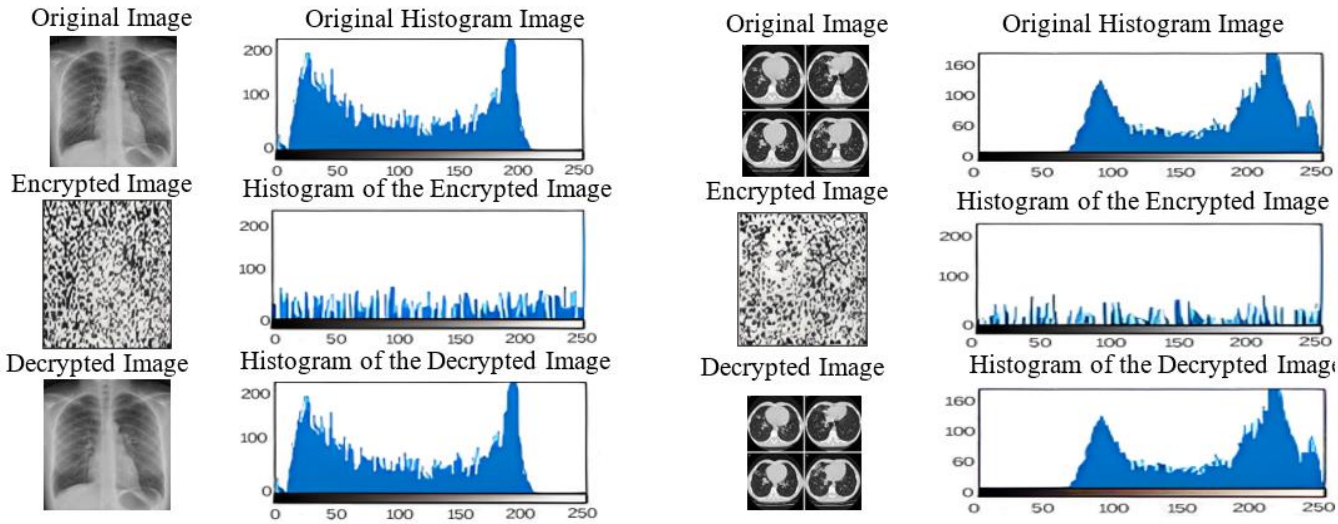
The decrypted images show histograms that are similar to those of the original images.




(a) US




(b) IRM




(c) RX (d) Scanner

**Figure 5.** Histogram's comparisons

The histograms of the original images differ from the histograms of the encrypted images.

These results indicate that the attacker is not able to retrieve information from the histogram of the encoded images. The non-uniformity of the histograms in the encrypted images indicates that the encryption process has introduced randomness and complexity, making it difficult to infer any meaningful information solely from the histogram.

Additionally, the resemblance between two histograms of the host and decrypted images, suggests that the decryption process successfully restores the original image characteristics and preserves data integrity.

The results show that the suggested image encryption algorithm is both feasible and effective. The suggested method protects the information by making it a potential solution to analyze various encrypted images including histogram comparison while considering other security aspects and assessing the resistance of the encryption method against different types of attacks.

### 4.2 Distortion measurement (PSNR)

Peak Signal to Noise Ratio (PSNR) [37] is a distortion measurement commonly used in digital image processing, particularly in image compression. It quantifies the performance of image encoders by evaluating the visual quality of the reconstructed compressed image compared to the original.

It is measured in decibels (dB) and calculated using the Eq. (5):

$$PSNR(i, i') = 10log_{10}\left(\frac{2^r - 1}{MSE}\right) \text{dB} \quad (5)$$

where, $i$ and $i'$are the original image and the processed one, $r$ represents the number of bits designated for a pixel, and $MSE$ is the Mean Squared Error.

If the $MSE$ value is zero, the original image and the processed one are identical and the *PSNR* value will be infinite. A higher *PSNR* indicates that the processed image is very similar to the original. In general, a *PSNR* value exceeding 20 dB is considered acceptable (this may vary depending on the specific problem).

We notice that $PSNR$ metric is only used to compare intensity values and does not provide any information on structural similarities. Therefore, it is often recommended to use other similarity methods, such as $SSIM$ (Structural Similarity Index Measure), which takes into account both intensity and structural similarities, for a more comprehensive evaluation of image quality.

### 4.3 Structural similarity measurement (SSIM)

The second approach, called $SSIM$ (Structural Similarity Index Measure) is focused on assessing the structural resemblance of two images [37]. It is grounded in the assumption that the Human Visual System (HVS) places significant importance on the structural information of an image. $SSIM$ can be defined with the formula as in Eq. (6):

$$SSIM(i_1, i_2) = l(i_1, i_2)c(i_1, i_2)s(i_1, i_2) \quad (6)$$

where,

$l(i_1, i_2)$*:* function that measures the intensities of image $i_1$ compared to image $i_2$.

$c(i_1, i_2)$*:* function that measures the contrast of image $i_1$ compared to image $i_2$.

$s(i_1, i_2)$*:* function that measures the structures of image $i_1$ compared to image $i_2$.

*SSIM* is a similarity measure between two images, with values ranging from 0 to 1. An *SSIM* value of 1 indicates a perfect match between the reconstructed image and the original image, while a value of 0 indicates complete dissimilarity.

In general, *SSIM* values close to 1 are considered as indicators of good-quality reconstruction techniques.

*SSIM* considers three components: structure, luminance, and contrast. It evaluates the similarity between corresponding local patches in the images, considering both the pixel values and their spatial relationships. By considering these structural factors, *SSIM* provides a more comprehensive assessment of image quality compared to metrics that solely focus on pixel-level differences, such as *MSE* or *PSNR*. Using *SSIM* as a similarity measure helps to assess how well the reconstructed image captures the structural details of the original image. Higher *SSIM* values indicate a closer match between the two

images in terms of their structural features.

By incorporating both *PSNR* and *SSIM*, we can gain insights into the quality of the reconstructed image in terms of both intensity fidelity and structural preservation. These metrics together provide a more comprehensive evaluation of image reconstruction techniques.

**Table 1.** Performance measurements of our system

| Evaluation Metrics | Cameraman | Rayon X | IRM |
|---|---|---|---|
| PSNR | 7.17 | 6.04 | 7.77 |
| | 39.09 | ∞ | ∞ |
| SSIM | 0.05 | 0.04 | 00.01 |
| | 0.99 | 1.00 | 0.79 |

Based on our results (see Table 1), we have observed the following:

• *PSNR < 20 dB*: This indicates that the encrypted image is significantly different from the original image. A low PSNR value suggests a relatively high level of distortion or loss of information during the encryption process.

• *PSNR > 20 dB*: This suggests that the decrypted image is very similar to the original image. A higher PSNR value indicates a better quality of reconstruction and a closer match to the original image.

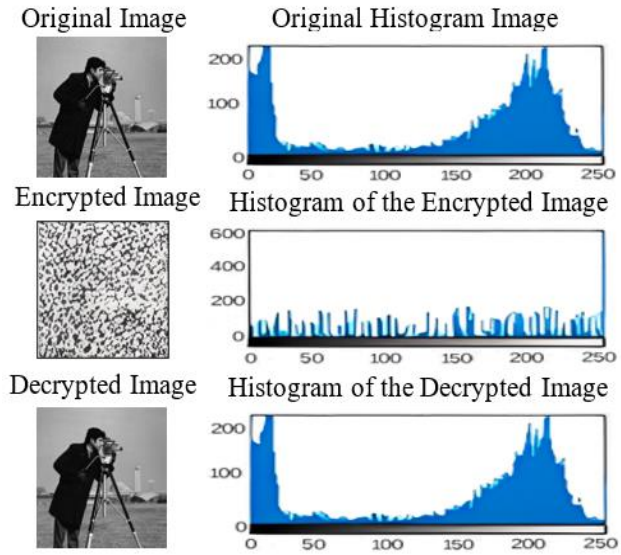
• *SSIM = 0*: An *SSIM* value of 0 indicates a complete dissimilarity between the original and encrypted images. This suggests a significant loss of structural similarity during the encryption process.

• *SSIM ≈ 1*: This indicates that the reconstructed image perfectly matches the original image. A higher *SSIM* value implies a higher level of structural similarity and a better preservation of the original image's characteristics.

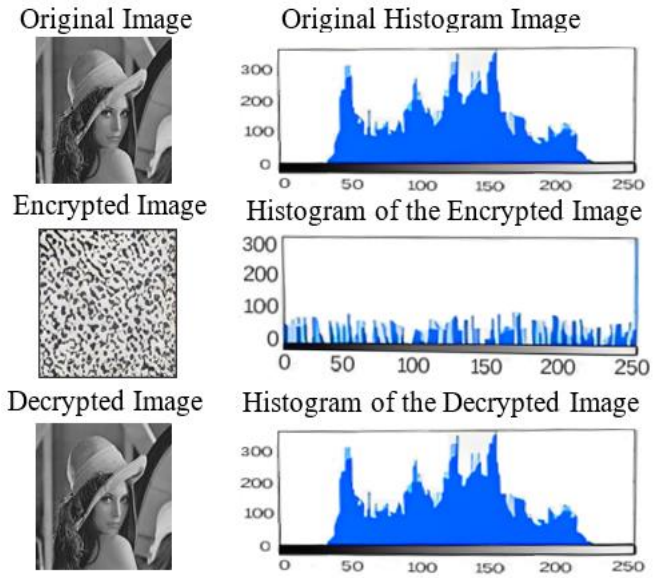
These findings provide insights into the quality and fidelity of the suggested system. The *PSNR* values suggest the level of distortion or similarity between the original and encrypted/decrypted images, while the *SSIM* values specifically assess the structural similarity between the images. It is important to consider both *PSNR* and *SSIM* measurements to assess the effectiveness and visual quality of the encryption and decryption techniques. A higher *PSNR* and closer-to-1 *SSIM* value generally indicate better image reconstruction and preservation of image details.

Similarly, this paper assessed images from diverse databases to prove the efficiency of the algorithm (Figure 6). Firstly, when we look in the histogram comparisons for Cameraman image, we note that all values of histogram values of the original and decrypted are very close. The same interpretations are in the case of Lena image, where most of histogram values and their difference are also very close which means that there is a good similarity between the original image and their corresponding decrypted one. Thus, our method presents very interesting results and reflects security and image fidelity.

By using a diverse range of images from these databases, we aim to evaluate the model's performance across various image types and scenarios. Testing the model with generalist databases allows us to assess its ability to handle different image formats, resolutions, and content. It also provides an opportunity to analyze the performance of the implemented system in terms of encryption speed, decryption accuracy, and the preservation of image quality and integrity. By conducting comprehensive testing with a wide range of images, we can gather empirical evidence to support the efficacy of our model. The obtained results from these tests will help validate the robustness and reliability of our encryption and decryption processes, providing insights into the model's real-world applicability and potential limitations.




(a) Cameraman




(b) Lena

**Figure 6.** Evaluation of the histogram with pictures

## 5. CONCLUSIONS

In this paper, we have achieved successful protection for medical images by exploiting both symmetric and asymmetric encryption features. We utilized the improved Vigenere cipher for the RSA algorithm for symmetric and asymmetric encryption respectively. The obtained results are promising, indicating that the encryption and decryption techniques used are effectively securing the images. Nevertheless, recognizing the limitation of our research and contemplating potential enhancements for the future is crucial. Many limitations and future research areas will be investigated, including rigorous evaluation of improved Vigenere cipher and RSA algorithm against various cryptanalytic techniques, the application of the proposed medical image encryption system in hospitals and

medical institutions and finally, enhancements and optimizations of the suggested approach to enhance its speed and scalability.

Overall, this work has demonstrated the potential of cryptographic techniques in securing medical images. By addressing the aforementioned limitations and exploring future perspectives, we can enhance the security of medical image transmission and storage even more, which will ultimately help healthcare institutions and protect the privacy and integrity of sensitive patient data.

## ACKNOWLEDGMENT

This work was completed with the support of DGRSDTMESRS (Algeria).

## REFERENCES

[1] Priyanka, Singh, A.K. (2023). A survey of image encryption for healthcare applications. Evolutionary Intelligence, 16(3): 801-818. https://doi.org/10.1007/s12065-021-00683-x

[2] Rivest, R.L., Shamir, A., Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2): 120-126. https://doi.org/10.1145/359340.359342

[3] Abusukhon, A., AlZu'bi, S. (2020). New direction of cryptography: a review on text-to-image encryption algorithms based on rgb color value. In 2020 Seventh International Conference on Software Defined Systems (SDS), Paris, France, pp. 235-239. https://doi.org/10.1109/SDS49854.2020.9143891

[4] Collier, B., Clayton, R. (2022). A "sophisticated attack"? innovation technical sophistication and creativity in the cybercrime ecosystem. In 21st Workshop on the Economics of Information.

[5] Almulihi, A.H., Alassery, F., Khan, A.I., Shukla, S., Gupta, B.K., Kumar, R. (2022). Analyzing the implications of healthcare data breaches through computational technique. Intelligent Automation & Soft Computing, 32(3): 1763-1779. https://doi.org/10.32604/iasc.2022.023460

[6] Chi, X., Yan, C., Wang, H., Rafique, W., Qi, L. (2022). Amplified locality-sensitive hashing-based recommender systems with privacy protection. Concurrency and Computation: Practice and Experience, 34(14): e5681. https://doi.org/10.1002/cpe.5681

[7] Ansari, M.F., Sharma, P.K., Dash, B. (2022). Prevention of phishing attacks using AI-based cybersecurity awareness training. Prevention, 3(6): 6. https://doi.org/10.47893/IJSSAN.2022.1221

[8] Joseph, D., Misoczki, R., Manzano, M., et al. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605(7909): 237-243. https://doi.org/10.1038/s41586-022-04623-2

[9] Munjal, K., Bhatia, R. (2022). A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex & Intelligent Systems, 9(4): 3759-3786. https://doi.org/10.1007/s40747-022-00756-z

[10] Al Badawi, A., Bates, J., Bergamaschi, F., et al. (2022). Openfhe: Open-source fully homomorphic encryption library. In Proceedings of the 10th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, Los Angeles, USA, pp. 53-63. https://doi.org/10.1145/3560827.3563379

[11] Ullah, S., Zheng, J., Din, N., Hussain, M.T., Ullah, F., Yousaf, M. (2023). Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. Computer Science Review, 47: 100530. https://doi.org/10.1016/j.cosrev.2022.100530

[12] Agrawal, M., Mishra, P. (2012). A comparative survey on symmetric key encryption techniques. International Journal on Computer Science and Engineering, 4(5): 877-882.

[13] Chen, P.Y., Wu, J.X., Li, C.M., Kuo, C.L., Pai, N.S., Lin, C.H. (2020). Symmetric cryptography with shift 2 n-1, hash transformation, optimization-based controller for medical image infosecurity: Case study in mammographic image. IEEE Photonics Journal, 12(3): 1-15. https://doi.org/10.1109/JPHOT.2020.2987769

[14] Lakshmi, C., Thenmozhi, K., Rayappan, J.B.B., Amirtharajan, R. (2018). Encryption and watermark-treated medical image against hacking disease - An immune convention in spatial and frequency domains. Computer Methods and Programs in Biomedicine, 159: 11-21. https://doi.org/10.1016/j.cmpb.2018.02.021

[15] Soualmi, A., Alti, A., Laouamer, L. (2021). Multiple blind watermarking framework for security and integrity of medical images in e-health applications. International Journal of Computer Vision and Image Processing, 11(1): 1-16. http://doi.org/10.4018/IJCVIP.2021010101

[16] Kumar, S., Chaurasia, P.K., Khan, R.A. (2022). Securing transmission of medical images using cryptography steganography and watermarking technique. In International Conference on Cryptology & Network Security with Machine Learning, pp. 407-420. http://doi.org/10.1007/978-981-99-2229-1_34

[17] Aliyu, A.A.M., Olaniyan, A. (2016). Vigenere cipher: Trends, review and possible modifications. International Journal of Computer Applications, 135(11): 46-50.

[18] Biham, E., Shamir, A. (2012). Differential Cryptanalysis of the Data Encryption Standard. Springer science & business media. https://doi.org/10.1007/978-1-4613-9314-6

[19] Daemen, J., Rijmen, V. (1999). AES proposal: Rijndael. The Rijndael Block Cipher. https://www.cs.miami.edu/home/burt/learning/Csc688.012/rijndael/rijndael_doc_V2.pdf.

[20] Bhanot, R., Hans, R. (2015). A review and comparative analysis of various encryption algorithms. International Journal of Security and Its Applications, 9(4): 289-306. http://doi.org/10.14257/ijsia.2015.9.4.27

[21] El-Deen, A., El-Badawy, E., Gobran, S. (2014). Digital image encryption based on RSA algorithm. Journal of Electronics and Communication Engineering, 9(1): 69-73. https://doi.org/10.9790/2834-09146973

[22] Kurosawa, K., Desmedt, Y. (2004). A new paradigm of hybrid encryption scheme. In Advances in Cryptology–CRYPTO 2004: 24th Annual International Cryptology Conference, Santa Barbara, California, USA, pp. 426-442. http://doi.org/10.1007/978-3-540-28628-8_26

[23] Liu, J.J., Tsang, K.T., Deng, Y.H. (2022). A variant RSA acceleration with parallelisation. International Journal of Parallel, Emergent and Distributed Systems, 37(3): 318-332. https://doi.org/10.1080/17445760.2021.2024535

[24] Hussein, N.H., Ali, M.A. (2022). Medical image compression and encryption using adaptive arithmetic coding, quantization technique and RSA in DWT domain. Iraqi Journal of Science, 63(5): 2279-2296. https://doi.org/10.24996/ijs.2022.63.5.38

[25] Venkatalakshmi, K., Gayathri, P., Likhitha, T.S., Shinde, S., Kumar, M.P. (2022). Design of montgomery multiplier–RSA algorithm. Journal of Physics: Conference Series, 2325(1): 012022. https://doi.org/10.1088/1742-6596/2325/1/012022

[26] Rani, P., Singh, P.N., Verma, S., Ali, N., Shukla, P.K., Alhassan, M. (2022). An implementation of modified blowfish technique with honey bee behavior optimization for load balancing in cloud system environment. Wireless Communications and Mobile Computing, 2022: 3365392. https://doi.org/10.1155/2022/3365392

[27] Islam, S.K., Nasim, M.D., Hossain, I., Ullah, D.M.A., Gupta, D.K.D., Bhuiyan, M.M.H. (2023). Introduction of Medical Imaging Modalities. arXiv preprint arXiv:2306.01022. https://doi.org/10.48550/arXiv.2306.01022

[28] Maity, A., Ghosh, R., Bhadra, S. (2022). Image encryption using RSA and advanced caesar cipher method. In 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), Bhubaneswar, India, pp. 1-5. https://doi.org/10.1109/ASSIC55218.2022.10088329

[29] Edan, S.J., Rasoul, M.N., Aljarrah, A.A. (2022). RSA-based encryption algorithm for digital images. In 2022 Iraqi International Conference on Communication and Information Technologies (IICCIT), Basrah, Iraq, pp. 303-308 https://doi.org/10.1109/IICCIT55816.2022.10010627

[30] Xu, Y., Wu, S., Wang, M., Zou, Y. (2020). Design and implementation of distributed RSA algorithm based on Hadoop. Journal of Ambient Intelligence and Humanized Computing, 11: 1047-1053. https://doi.org/10.1007/s12652-018-1021-y

[31] Zhang, D., Ren, L., Shafiq, M., Gu, Z. (2023). A privacy protection framework for medical image security without key dependency based on visual cryptography and trusted computing. Computational Intelligence and Neuroscience, 2023: 6758406. https://doi.org/10.1155/2023/6758406

[32] Gutub, A. (2023). Dynamic smart random preference for higher medical image confidentiality. Journal of Engineering Research, 11(3): 100-111. https://doi.org/10.36909/jer.17853

[33] Hameed, T.H., Sadeeq, H.T. (2022). Modified Vigenère cipher algorithm based on new key generation method. Indonesian Journal of Electrical Engineering and Computer Science, 28(2): 954-961. https://doi.org/10.11591/ijeecs.v28.i2.pp954-961

[34] https://www.kaggle.com/datasets/andrewmvd/medical-mnist. accessed on Jan. 10, 2023.

[35] Saravanan, M., Priya, A. (2019). An algorithm for security enhancement in image transmission using steganography. Journal of the Institute of Electronics and Computer, 1(1): 1-8. https://doi.org/10.33969/JIEC.2019.11001

[36] Kong, N.S.P., Ibrahim, H., Hoo, S.C. (2013). A literature review on histogram equalization and its variations for digital image enhancement. International Journal of Innovation, Management and Technology, 4(4): 386-389. https://doi.org/10.7763/IJIMT.2013.V4.426

[37] Setiadi, D.R.I.M. (2021). PSNR vs SSIM: Imperceptibility quality assessment for image steganography. Multimedia Tools and Applications, 80(6): 8423-8444. https://doi.org/10.1007/s11042-020-10035-z