I.J. Image, Graphics and Signal Processing, **2025, 3, 146-158**
Published Online on June 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2025.03.08

Multi-Stage Medical Image Encryption System Combining RSA and Steganography

Jahin Ahmed
Department of Biomedical Engineering, Military Institute of Science & Technology (MIST), Mirpur Cantonment, Dhaka-1216, Bangladesh
E-mail: jahin.mist@gmail.com

Faizul Hakim
Department of Biomedical Engineering, Military Institute of Science & Technology (MIST), Mirpur Cantonment, Dhaka-1216, Bangladesh
E-mail: faizul.wbd@gmail.com
ORCID ID: https://orcid.org/0009-0006-8114-4541

Md. Asadur Rahman*
Department of Biomedical Engineering, Military Institute of Science & Technology (MIST), Mirpur Cantonment, Dhaka-1216, Bangladesh
E-mail: bmeasadur@gmail.com
ORCID ID: https://orcid.org/0000-0001-6194-664X
*Corresponding Author

Received: 20 June, 2023; Revised: 20 August, 2023; Accepted: 12 January, 2025; Published: 08 June, 2025

Abstract: Data security has become a major concern in the present era of the communication revolution, especially maintaining the confidentiality of medical images a prime concern in e-health establishments. As conventional techniques hold numerous drawbacks, this study aims to develop an image encryption algorithm by combining two renowned methods: the RSA algorithm and steganography. The proposed algorithm is modified with the help of the conventional RSA algorithm and steganography to provide an attainable solution to this alarming issue. RSA technique encrypts multiple medical images with distinct keys; further, these keys are embedded in two images to be transmitted secretly with the help of LSB steganography. The proposed system generates images of an unidentifiable pattern after encryption and decrypts those images without any loss. The claimed performances and robustness of the system are justified using different numerical and graphical measures such as PSNR, MSE, SSIM, NPCR, UACI, and histograms. This encryption method can be used for medical image transmission where image security is a vital concern.

Index Terms: Encryption, Decryption, RSA Algorithm, Steganography, Lossless System

1. Introduction

Secured image data transfer is an alarming issue in different sectors like military communication, international affairs, digital and cyber security, password protection, e-healthcare systems, and so on. In the medical field, this is a matter of the topic as secure medical image transmission plays a significant role throughout the entire clinical process, from diagnosis through treatment or surgical intervention and subsequent research [1]. Medical images frequently contain confidential information about the patients and are therefore vulnerable to different security risks when transmitted over a public network. Therefore, it is essential to protect these images while transmitting them over an open network [2]. The unauthorized use of medical images may compromise the confidentiality of patient information. Moreover, since these images are susceptible to even little alterations, a misdiagnosis might endanger patients' lives [3]. This data may be secured using a number of fundamental techniques against several forms of attacks, including interruption, alteration, fabrication, etc. The most popular information security strategies are cryptography, steganography, chaos-based encryption, watermarking, etc.

However, conventional encryption techniques hold some drawbacks like static keys, long computational time, recognizable patterns even after encryption, a large amount of loss in the decryption process, mandatory large key size,

and so on. To resolve these issues as well as to maintain a higher security level, this work proposes an efficient encryption-decryption system which is a combination of two renowned methods RSA and steganography with some application-based modifications.

In this work, the main contribution is made to focus on the sender and receiver ends where the encryption and decryption processes take place, respectively. If no loss of data occurs in the communication channel while transmitting the images, then our system acts as a lossless system. For a clear understanding, the system as a whole is given in Fig.1. Therefore, the overall contributions of this work are as follows:

- Key size reduction without compromising the effectiveness of the RSA algorithm
- Combining RSA with steganography to ensure multiple-step encryption without affecting the image quality and ensuring a lossless encryption-decryption system

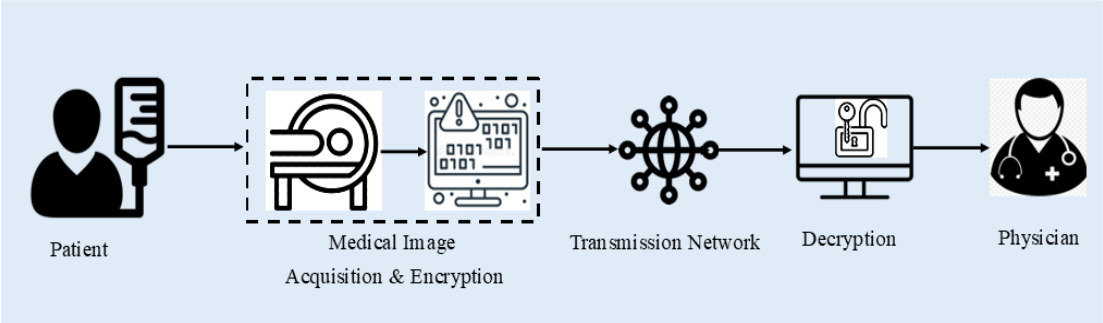


Fig. 1. Development of medical image encryption system for secure image-data transfer. Initially, the images are acquired and encrypted at the receiver end and then the encrypted images are transmitted through the transmission network. Encrypted images show a totally altered form of original images which protects them from any unauthorized access. On the receiver end, physicians can decrypt these images and can use them for further usage.

The RSA algorithm has certain limitations, including the need to select sufficiently large prime numbers to ensure robust security. Additionally, there is a constraint on the size of the input. It is advised that the minimum key size should be 2048 bits in length. Consequently, the RSA encryption algorithm is deemed unsuitable for the encryption of large-scale data due to its inherent limitations in processing efficiency, resulting in significantly slower encryption and decryption speeds. That's why this paper focused on the key size reduction of the RSA algorithm without compromising the quality of the encrypted image [4].

The paper is arranged in the following sections: a concise overview of the RSA cryptosystem and steganography is provided in Section 2. In Section 3, the work methodology is presented. In Section 4 results are described with evaluation parameters. Section 5 is the last portion of the paper which contains the conclusion.

2. Background Studies

2.1. RSA Cryptosystem

The study and practice of secure communication by destroying the message in a way that makes it impossible for strangers or the general public to access secret messages is cryptography. The prefix "crypt-" denotes "hidden", while the ending "-graphy" denotes "writing" [5]. The main objectives of cryptography are confidentiality, integrity, authentication, and non-repudiation [6]. Cryptography consists of encrypting and decrypting data so that only the intended recipient may read it. Encryption is the process of converting the original image or plaintext into an altered, unreadable form of ciphertext by using the key, and decryption is the opposite process of encryption [7].

It is possible to classify cryptographic algorithms as either symmetric keys or asymmetric keys. In symmetric encryption, encrypting and decrypting are both performed with the same key. It's easy to understand and use, but it comes with some major limitations. Once an attacker has the correct key, the data is easily accessible. When using asymmetric key encryption, the decryption and encryption processes each need their unique key. The sender's public key is shared with everyone, while the recipient's private key remains secret [8].

The main problem with this kind of key encryption is that it requires more time to process than symmetric techniques [7]. The most popular and widely used public-key cryptosystem or asymmetric key cryptography is RSA. Its security is contingent on the difficulty of obtaining the private key in a reasonable amount of time but not on the algorithm's specifics. The RSA encryption technique was developed by Ron Rivest, Adi Shamir, and Len Adleman [8]. RSA cryptosystem consists of 3 steps which are key generation, encryption, and decryption. These 3 steps are illustrated in Fig.2.

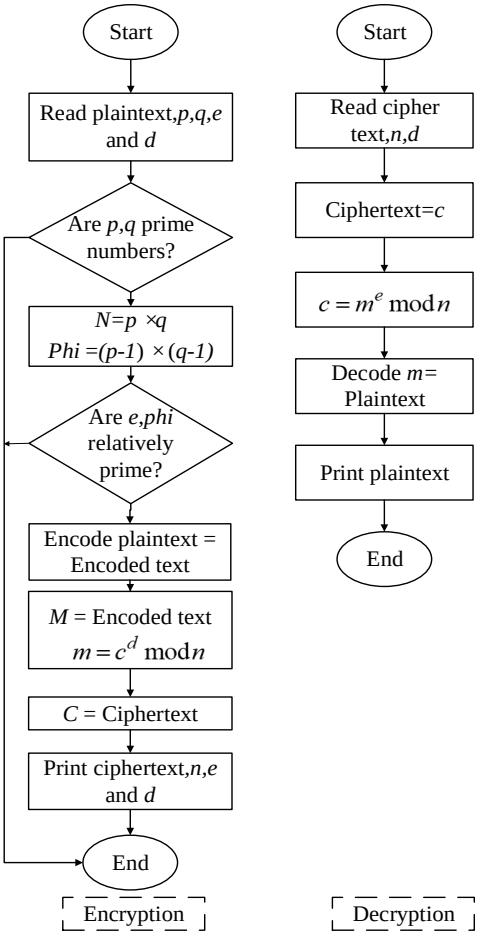


Fig. 2. Flow diagram of RSA cryptosystem.

2.2. Steganography

Steganography is a "harmless" method that makes it impossible for any individual to detect the existence of a hidden message. The structure of the secret message is unaltered [9]. To be more specific, steganography is used to conceal data so that an unauthorized recipient does not become suspicious of its presence [10]. To hide the secret data, a cover medium is used which can be image, audio, or video. Steganalysis is a means of extracting secret data from a stego image [11]. Steganography is used for this purpose to divert undesired attention away from the channels through which the message is conveyed [12]. The general process of steganography is shown with an example in Fig.3.

In the proposed security system, image-based spatial domain LSB steganography has been used. In a spatial domain approach, the secret information is hidden by altering specific pixels without using any intermediate steps. The least significant bit (LSB), pixel value differencing (PVD), texture-based, pixel intensity-based, histogram shifting-based, etc. are all examples of well-known spatial domain techniques. These methods are worthy, effective, of medium complexity, exhibit less medium degradation, and conceal more data. Yet, they are less robust and susceptible to attack. LSB steganography has been utilized in this system [13]. The representation of the impact on pixel value when LSB and MSB are modified is shown in Fig.4.

The lowest bit in a binary number is the least significant bit (LSB), often known as the right-most bit and it's also called the least important bit. The least important bit, for instance, is "0" in the binary number 10010010. By substituting the LSB of the image, information can be hidden inside of images using the LSB-Steganography approach.

However, if the message is too huge, it will start changing the second rightmost bit and so on. If the LSB of the cover image is changed, then it will cause only a 0.000002% change in bytes, whereas if the MSB (Most significant bit) of the cover image is changed, then it will change 99.99999% in bytes. Therefore, in LSB steganography, the MSB of a secret image can be hidden by replacing the LSB of the cover image to form a stego-image, and by using an extracting algorithm, a secret image can be extracted from the stego-image. As the LSB modification causes no image distortion, the final stage image will appear exactly like the cover image [14].

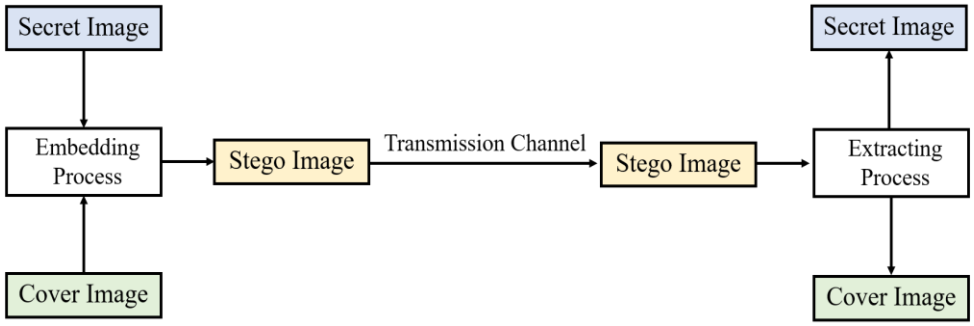


Fig. 3. General process of steganography

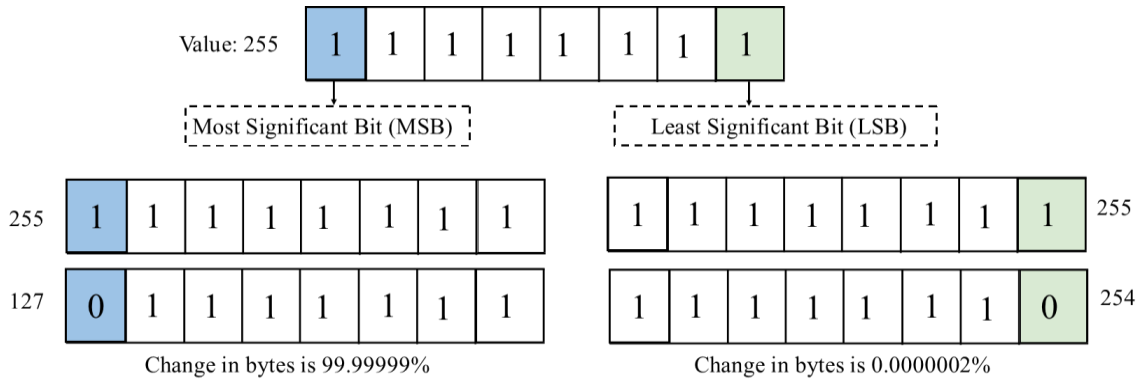


Fig. 4. Representation of the impact on pixel value when LSB and MSB are modified.

2.3. Literature Review

A number of studies have been done relating cryptography and steganography, but most of them have specific problems. Conventional encryption algorithms like RSA contain some issues. For that reason, the conventional RSA algorithm is combined with other approaches in several studies. A comparison among numerous methods is shown in Table 1. The majority of issues with the previous methods are low values of quality matrices, the moderate security level of the algorithm, the time-consuming algorithm, decreased quality of images, and the similarity of the pattern of the encrypted image with the original image after using only the RSA algorithm, etc. To resolve these issues in our work two-level security is ensured using the RSA algorithm along with LSB steganography.

Table 1. Comparison table with using other algorithms for medical image security

Year	Authors	Methods	Limitations
2023	Simin et.al. [15]	RSA and Integer Wavelet Transform (IWT)	Time-consuming chaotic sequences
2023	Balasubramaniyan et. al. [16]	RSA and Image Steganography	Higher time usage for encryption
2022	Mustafa et.al. [17]	Steganography	Security and robustness are of moderate level.
2021	Karthikeyan et. al. [18]	RSA and Steganography	Unable to encrypt the image
2019	Zhang et. al. [19]	Steganography, IWT, Multi-Directional Line Encoding (MDLE)	Moderate level of data security
2019	Jassim et. al. [20]	RSA and LSB Steganography	Unable to encrypt the Image
2018	Shabir et. al. [21]	RC4 encryption and LSB steganography	Maintains not-so-high PSNR
2017	Moumen et.al. [22]	AES, RSA-Steganography	Moderate-level security
2017	Roselin et. al. [23]	RSA-Steganography-ECC	The security of ECC is higher than RSA
2017	Syifak et. al. [24]	Watermarking	Efficient precise detection and image recovery
2015	Wang et. al. [24]	RSA	Pattern-producing problem of RSA in encrypted image
2015	Irfan et. al. [25]	RSA -chaotic system	Elimination of the chance of identical patterns
2014	Saha et. al. [3]	Arnold's transformation and RSA	Enhancement of the quality of image encryption

3. Proposed Method

The proposed crypto-stegano system performs encryption and decryption only at the sender and receiver ends respectively. If no loss occurs in the transmission network, then this system acts as a lossless one. Moreover, any loss in the medical images must not face any kind of loss as these images are related to critical treatment processes. Any loss may lead to misdiagnosis and even severe complications that can endanger patients' lives. Therefore, this method aims at generating a lossless system. The methodology of the work is visually represented in Fig.5.

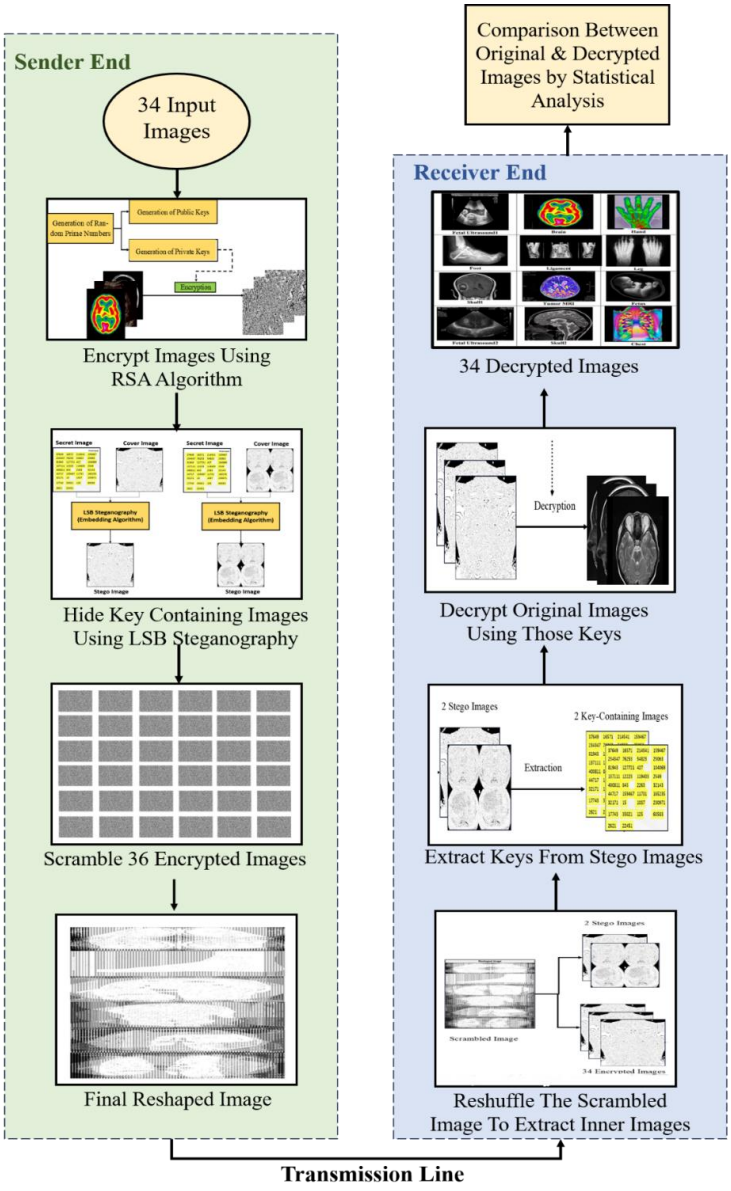


Fig. 5. Overall methodology of the proposed system.

3.1. RSA Encryption

The RSA technique is used to encrypt the 34 images that were used as input. To construct public and private keys for encryption and decryption, random prime integers are first obtained which are relatively small integers. Static keys, which are much less safe than dynamic keys, are a problem with traditional encryption systems. The proposed system generates different keys for each transmission and each image is encrypted using different keys. Therefore, this system produces dynamic keys which resolve the problem of static keys and it raises the security level by making it harder for the attacker to determine which key is required for which image. The steps included in the encryption process are illustrated in Fig.6.

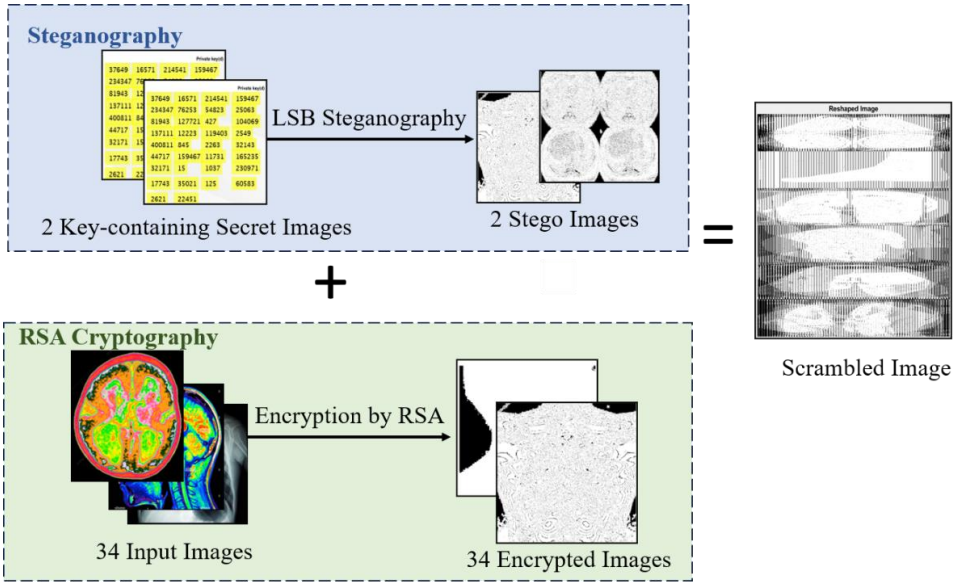


Fig. 6. The RSA encryption algorithm is applied to the input images to encrypt them. Before that generation of prime numbers is done to create public and private keys which are needed to perform RSA encryption.

3.2. LSB Steganography

The first step generates two key-containing images using public and private keys. These photos with the keys embedded in them are then subjected to a steganographic process. In this scenario, the MSB of secret-key-containing images has been replaced by the LSB of cover images using LSB steganography. The cover images are therefore encrypted using the RSA technique in this case. After this, two key-containing images are combined with two cover images to create two stego-images. This whole procedure of steganographic operation is shown in Fig.7.

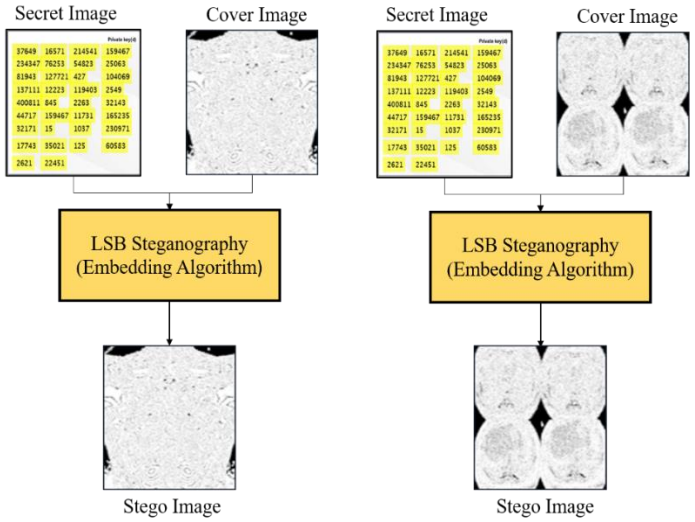


Fig. 7. Two stego-images are generated with the help of LSB steganography.

3.3. Scrambled Image

The RSA technique is used to encrypt a total of 34 images, and the LSB steganography algorithm is used to make two stego-images; these 36 images in their whole are then integrated into a single image. Each of the 36 images has a size of 300×300. This final image is then scrambled. As the RSA algorithm alone generates encrypted images with the same pattern as the original images, scrambling is done to change the pattern of the encrypted image. Because of this, a single image with the dimensions 1800×1800 is formed by blending a total of 36 different images. So, in our proposed system, we have introduced three stage encryption and reduced the key size of the RSA algorithm. An image after completely transformed or scrambled is given in Fig.8.

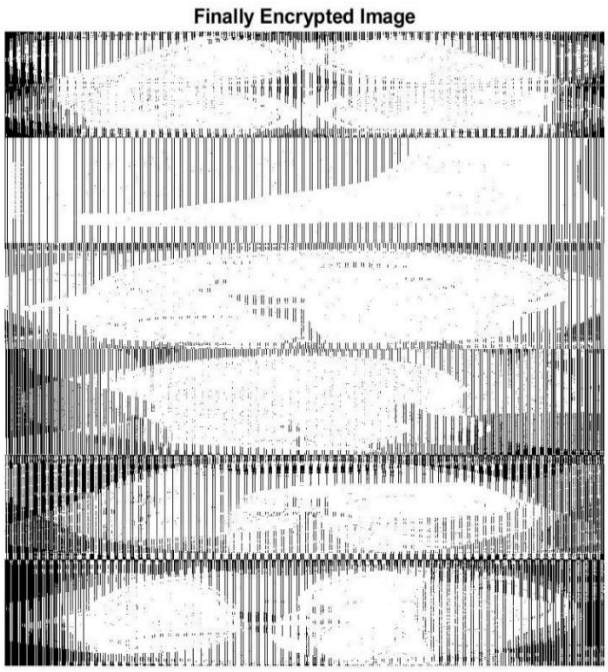


Fig. 8. Final reshaped or encrypted image from which the patterns of original images can't be identified.

3.4. Decryption Process

This system focuses on the transmission of medical images and accompanying information, as well as the recipient activities required before the images, may be used to serve further purposes. At the receiving end, the initial step is to convert and separate the 34 encrypted images and the two stego-images from one single scrambled image. Image decryption cannot be performed without steganographic extraction since stego data is composed of the image decryption key and is entirely dependent on it. Consequently, two images containing keys are retrieved from two stego-images through Steganography extraction. These images contain public keys which are used in the decryption stage of the RSA algorithm.

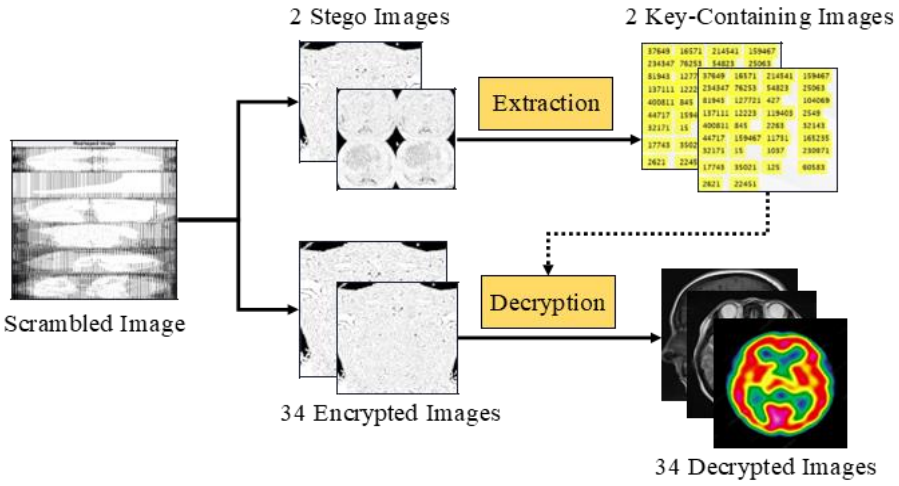


Fig. 9. The decryption process is shown in this figure which is the opposite of the encryption procedure.

Since any loss in medical image content caused by this decryption technique will have some distorting effects or eliminate certain essential features in the medical image, it might lead to misdiagnosis and make it difficult for the physician to identify the patient's health status. It is an extremely significant procedure that must be performed cautiously and retrieved in the most efficient way possible. In the final step, 34 images are decrypted in their original 300×300 dimensions using those public keys extracted from stego-images which contained those keys. The decryption process is illustrated in Fig.9.

4. Results and Discussions

In this section, the result part along with several studies (e.g., statistical analysis, differential analysis, strength against some cryptographic attacks, etc.) have been used to evaluate the security level, efficacy, and reliability of the proposed image encryption system. NPCR, UACI, PSNR, MSE, SSIM, and histograms are employed as evaluation metrics in this context. The effectiveness of the proposed approach, encryption based on the RSA algorithm and LSB steganography, is tested for different images. Three grayscale images with different sizes are used as input images. The proposed method is facilitated by the MATLAB 2020b program on the Windows 11 platform since it provides efficient numerical calculation, data processing, and visualization capabilities. It also serves as a tool for application development. MATLAB facilitates the usage of its functions by guiding the user through the encryption and decryption procedures from and into the cover. In this section, the results of our system are shown. A single image is encrypted using RSA and the recovered image which is given in Fig.10. The pattern of the encrypted image in the middle is quite similar to the original image, which is a problem with the conventional RSA cryptosystem. Our suggested approach for embedding and retrieving several images from a scrambled image is shown in Fig.11.

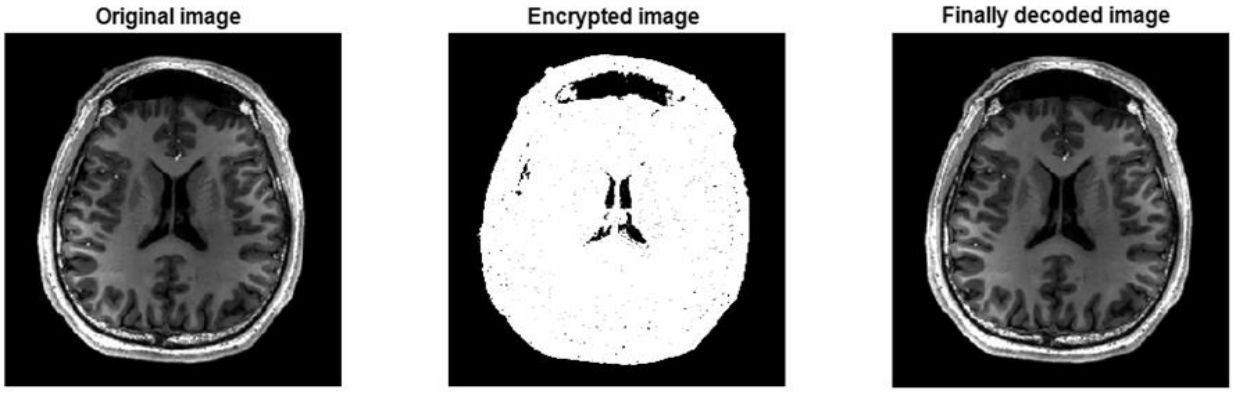


Fig. 10. Single image encryption and decryption using RSA cryptosystem

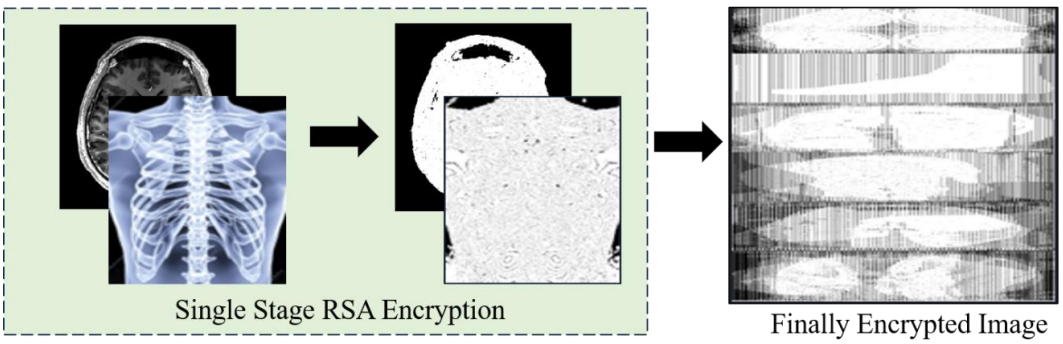


Fig. 11. Finally encrypted images after combing multiple encrypted images by RSA encryption.

Unified Average Changing Intensity (UACI): The average intensity of the variations between two encrypted images, representing a difference of one pixel in the plain images, UACI must be minimized. The UACI should be at least 33.4653 to defend from differential attack [26]. The process of equating UACI is given in (1).

$$UACI = \frac{\sum_{i,j} E(i,j) - E'(i,j)}{255 \times W \times H} \times 100 \tag{1}$$

Number of Pixel Change Rate (NPCR): It is the percentage of bits that are different between two encrypted images whose unencrypted versions vary by exactly one pixel. The range is [0, 100] for NPCR. A great result for an encrypted image's NPCR is approximately 100. To mathematically define NPCR, Equation (2) is used, where W and H are the width and height of the original image, and $D(i,j)$ is the difference between the encrypted images of the original and the modified image. The value of NPCR for two random images, which is a foreseeable estimate for a good encryption technique, is 99.69 [26].

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \tag{2}$$

Structural Similarity Index (SSIM): The range of SSIM [-1 1]. The similarity between the encrypted and original picture is identified by SSIM. Because the negative values are irrelevant, SSIM ranges from 0 to 1. SSIM measures the quality of imperceptibility in a steganographic image and SSIM equal to 1 defines that the original images and the recovered images have complete structural similarity. Equation (3) provides a mathematical definition of SSIM.

$$SSIM = \frac{(2\mu_I\mu_D + C_1)(2\sigma_{ID} + C_1)}{(\mu_I^2 + \mu_D^2 + C_1)(\sigma_I^2 + \sigma_D^2 + C_2)} \tag{3}$$

Mean Squared Error (MSE): MSE is mathematically defined by Equation (4), where x and y are the pixel coordinates of images with the size of M×N pixels. The encrypted image is labeled O, while the decrypted image is labeled R. The value of MSE is [0, infinity]. There should be a minimal mean squared error (MSE) between the original and the decrypted version. MSE is used to analyze the quality of decrypted images. An MSE value equal to 0 means the system is lossless and there is no difference between the decrypted image and the original image [27].

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}[O(x,y) - R(x,y)]^2 \tag{4}$$

Peak Signal to Noise Ratio (PSNR): The PSNR interval is [0,1]. The PSNR between the encrypted and decrypted images should be as high as possible. The PSNR value depends on MSE. When PSNR is high, it means the quality of the decrypted image is good, there is less difference between the original image and the decrypted image, and there is less loss of the system [27]. PSNR is defined as (5).

$$PSNR = 10\log_{10}^{\frac{(2^n-1)^2}{MSE}} \tag{5}$$

Histogram analysis: An image histogram is a graphical representation of the distribution of pixel intensities in a digital image. Let r_k, for $k = 0,1,2...,L-1$, represent the intensities of an L-level digital image, $f(x,y)$.The unnormalized histogram,

$$h(\mathrm{r}_k) = n_k \tag{6}$$

Where n_k corresponds to the number of pixels in f with intensity r_k.

The normalized histogram of f can be defined as follows,

$$p(\mathrm{r}_k) = \frac{h(\mathrm{r}_k)}{MN} = \frac{n_k}{MN} \tag{7}$$

The divisions of the intensity scale are referred to as histogram bins. M and N denote the number of image rows and columns, respectively. The sum of $p(\mathrm{r}_k)$ for all values of k is always 1. The components of $p(\mathrm{r}_k)$ represent estimates of the probabilities of intensity levels appearing in an image.

This function counts the number of pixels in the image with each possible intensity value, creating a distribution of pixel intensities. The resulting histogram summarizes the image's tonal characteristics, allowing for contrast, brightness, and dynamic range analysis.

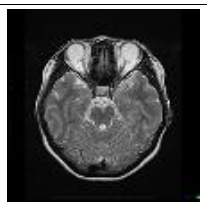
The evaluation parameters are computed for five different images, and the results are projected in Table 2. The performance assessment of the proposed system indicates that PSNR values are infinite and MSE values are zero for all evaluated images. These measures demonstrate a precise correlation between the encrypted and original pictures, with no discernible changes in pixel values. The existence of infinite PSNR and zero MSE highlights the system's capacity to properly reconstruct the original image without losing quality or data.

The resilience of the encryption system against differential attacks was further evaluated using the NPCR and UACI metrics, both established criteria in encryption security evaluation. Differential attacks use subtle alterations in the source image to deduce information on the encryption process. In this method, all evaluated images have NPCR scores above 99% and UACI values exceeding 33%. Greater NPCR scores indicate that alterations are widespread across the image, preventing differential attacks from depending on limited analysis to reveal patterns. Simultaneously, the

increased UACI values indicate that the encryption process induces significant intensity changes at the pixel level, rendering it impossible to discern any remaining patterns from the original image.

The study reveals that the SSIM for each image is 1, signifying the exact structural similarity between the decrypted and original images. This finding is crucial since it indicates that the encrypted image preserves all original structural elements, confirming that the decryption process is lossless and that no information has been compromised during the transformation.

Table 2. Evaluation parameter values for different images using our algorithm

Image Name	Image	NPCR	UACI	PNSR	MSE	SSIM
Cameraman		100	60.47	∞	0	1
CT		82.0213	65.8144	∞	0	1
USG		76.1152	55.1468	∞	0	1
Fetus		83.6776	53.7133	∞	0	1
Chest X-ray		100	66.68	∞	0	1

Histogram analysis is a crucial metric for evaluating the efficacy of an image encryption method since it reveals the extent to which the encryption algorithm conceals the real image information. An image histogram graphically illustrates the distribution of pixel values in an image. In the realm of image encryption, the histogram of an encrypted image should ideally mimic a uniformly random distribution analogous to white noise. This consistency indicates that the encryption process has successfully randomized the pixel values, eliminating any discernible patterns or recognized structures that might point to the original image information. This modification is essential to guarantee that the encrypted image lacks any structural patterns or statistical features of the plaintext image, which could make it vulnerable to statistical attacks. A statistical attack involves analyzing the patterns and frequencies of an encrypted image's pixel values to deduce the original information.

The ciphertext image histogram analysis is one of the simplest techniques for demonstrating image encryption quality. Since an effective image encryption technique prefers to encrypt a plaintext image to random-like, a ciphertext image should have a uniformly distributed histogram. The corresponding histograms of each layer of the encrypted images deviate substantially from those of the original image.

Histogram analysis of a reference Baboon image and an ultrasound fetus image is presented in Fig. 12 and Fig. 13, respectively. The baboon image is a conventional test image widely used image in digital image processing. We have also applied our proposed system to a real medical image. The suggested encryption system yields a histogram with a flat

distribution, reducing the likelihood of a statistical attack for both images. The resulting histograms are shown in both figures.

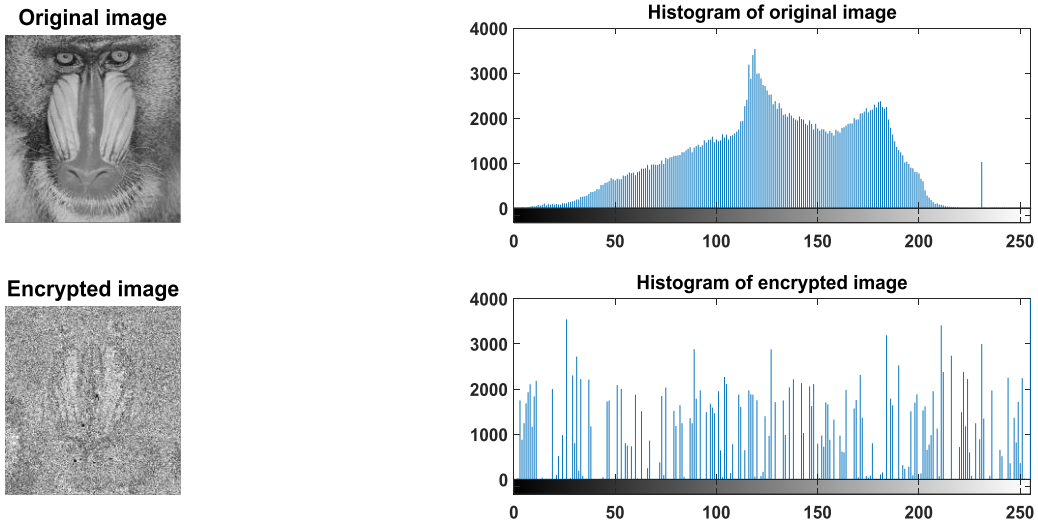


Fig. 12. Histogram analysis of Baboon.

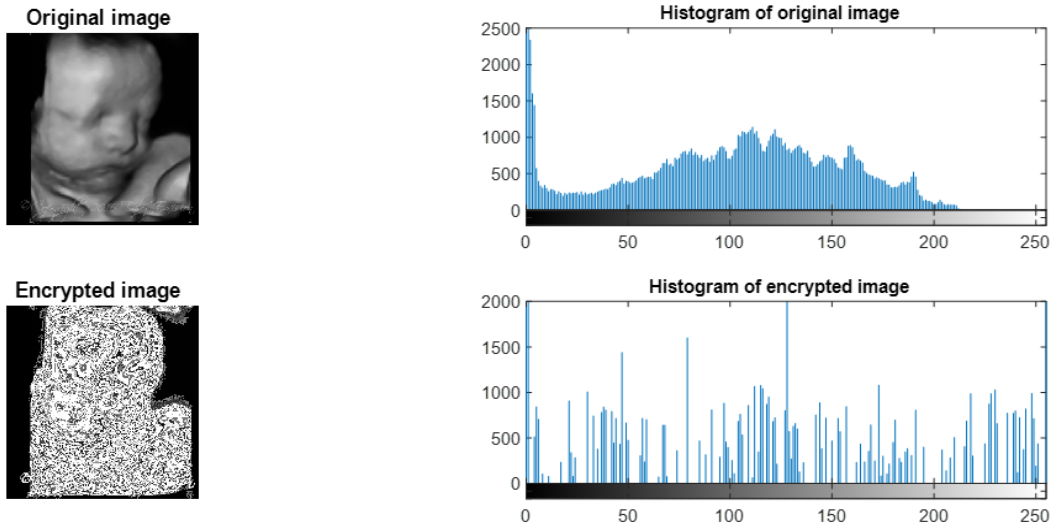


Fig. 13. Histogram analysis of Ultrasound Fetus Image.

The proposed encryption method exhibits superior performance with lossless image reconstruction (infinite PSNR and zero MSE) and complete structural similarity (SSIM of 1). It is significantly resistant to differential attack, with NPCR values above 99% and UACI scores surpassing 33%, indicating robust diffusion and intensity modification. Histogram analysis verifies a uniformly random distribution, resisting statistical attacks. Overall, this approach efficiently safeguards images while guaranteeing lossless decryption.

5. Conclusions

This work addressed an issue that involves protecting the privacy of patients' medical data. The proposed work addressed some problems of traditional encryption methods used in protecting medical images such as static keys, lengthy processing time, identifiable patterns even after encryption, and significant losses during the decoding process. The proposed method overcame the mentioned issues by combining two well-known techniques, RSA and steganography. With some constructive modifications of those methods, the proposed lossless system provides decrypted images identical to the original images. Though this work offers a secured transfer of confidential medical data, it may not be suitable for data transfer. Secured data communication over the internet should be of different methods that can be considered further in future work. To improve the robustness of the system, the target is to implement the proposed system utilizing various encryption approaches in the future, such as the traditional inverted bit least significant bit steganography algorithm or the close logistic map using the singular value decomposition (SVD) method.

References

[1] C. Francesco, I. Donato and P. Giuseppe, "A Medical Image Encryption Scheme for Secure Fingerprint-Based Authenticated Transmission," Applied Sciences, vol. 13, no. 10, 2023.

[2] J. Jaishree and J. and Arpit, "Securing E-Healthcare Images Using an Efficient Image Encryption Model," Scientific Programming," Scientific Programming, p. 11, 2022.

[3] K. Sara, H. Khalid, E. Taha, D. Mohamed and F. Mostafa, "A New Image Encryption Algorithm for Grey and Color Medical Images," IEEE Access, vol. 9, pp. 37855-37865, 2021.

[4] W. Siriboonpipattana, C. Soomlek and P. Seresangtakul, "Increasing the input data length of RSA cryptosystem by applying a hybrid lossless data compression algorithm," Journal of Physics: Conference Series, vol. 1502, no. 1, p. 012036, 2020.

[5] R. Bharat, M. Gunasekaran and P. Alexender, "Cryptography," in Cybersecurity and Identity Access Management, Singapore, Springer, 2023.

[6] Y. Hua, F. Yao, L. Chen and W. Chen, "Experimental quantum secure network with digital signatures and encryption," National Science Review, vol. 10, no. 4.

[7] I. Omar, Y. Sura, H. Isam, A. Wisam and H. Ali, "Implementation of El-Gamal algorithm for speech signals encryption and decryption," Procedia Computer Science, no. 169, pp. 1028-1037, 2020.

[8] H. Aljaafari and K. Basant, "A Review Paper on DES, AES, RSA Encryption Standards," in 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 2020.

[9] O. Elharrouss, N. Almaadeed and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," in in IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020.

[10] M. Pascal and A. Tohari, "Information hiding scheme for digital images using difference expansion and modulus function," Journal of King Saud University - Computer and Information Sciences, vol. 31, no. 3, pp. 335-347, 2019.

[11] S. Lingamallu and V. Vijayaraghavan, "Steganography using wavelet transform for secured data transmission," Journal of Ambient Intelligence and Humanized Computing, vol. 14, p. 9509–9527, 2023.

[12] M. Khairullah, "A novel steganography method using transliteration of Bengali text," Journal of King Saud University Computer and Information Sciences, vol. 31, no. 3, pp. 348-366, 2019.

[13] M. Dalal and M. Juneja, "Steganography and Steganalysis (in digital forensics): a Cybersecurity guide," Multimedia Tools and Applications, vol. 80, pp. 5723-5771, 2021.

[14] A. Abdul, H. Mehdi, W. Ainuddin and I. Yamani, "High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution," Applied Sciences, vol. 8, no. 11, p. 2199, 2018.

[15] D. Simin and Y. Guodong, "IWT and RSA based asymmetric image encryption algorithm," Alexandria Engineering Journal, no. 66, pp. 979-991, 2023.

[16] K. Balasubramaniyan, K. Bharath and G. Manikandan, "A Combination of RSA Algorithm with Image Steganography to Ensure Enhanced Encryption," in Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2023.

[17] S. T. Mustafa, S. Mohd, M. Mohammed and N. Hiyam, "High payload image steganography scheme with minimum distortion based on distinction grade value method," Multimedia Tools and Applications, vol. 81, no. 18, pp. 25913-25946., 2022.

[18] N. Karthikeyan, K. Kousalya, N. Jayapandian and G. Mahalakshmi, "Assessment of composite materials on encrypted secret message in image steganography using RSA algorithm," Materials Today: Proceedings, vol. 81, no. 2, pp. 848-852, 2021.

[19] Z. Hua and H. Liting, "A data hiding scheme based on multidirectional line encoding and integer wavelet transform," Signal Processing: Image Communication, vol. 78, no. 3, p. 331–344, 2019.

[20] N. Jassim, N. Ahmed, N. Asama, P. Bagus, N. Emil, M. Mardhiah, H. Inge and P. Zico, "Hybrid cryptography and steganography method to embed encrypted text message within image," Journal of Physics: Conference Series, vol. 1339, no. 1, p. 012061, 2019.

[21] P. Shabir, S. Javaid, A. Jahangir, L. Nazir and B. Ghulam, "Information hiding in edges: A high capacity information hiding technique using hybrid edge detection," Multimedia Tools and Applications, vol. 78, pp. 185-207, 2018.

[22] A. Moumen and H. Sissaoui, "Images encryption method using steganographic LSB method, AES and RSA algorithm," Nonlinear Engineering, vol. 6, no. 1, pp. 53-59, 2017.

[23] K. Roselin and T. S. Sharmila, "Performance analysis in secured image encryption and data hiding using LSB algorithm," in IEEE International Conference on Circuits and Systems (ICCS), India, 2017.

[24] X. Y. Wang, Z. Ying-Qian and B. Xue-Mei, "A colour image encryption scheme using permutation-substitution based on chaos," Entropy, vol. 17, no. 6, pp. 3877-3897, 2015.

[25] P. Irfan, P. Yudi and R. Imam, "Image encryption using combination of chaotic system and rivers shamir adleman (RSA)," International Journal of Computer Applications, vol. 123, no. 6, 2015.

[26] Y. Bedir, F. Khalifa and A. Makram, "A novel image encryption/decryption scheme based on integrating multiple chaotic maps," AIP Advances, vol. 10, no. 7, 2020.

[27] O. F. Abdel, A. I. Hussein and H. Hamed, "Hiding data in images using steganography techniques with compression algorithms," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 17, no. 3, pp. 1168-1175, 2019.

Authors' Profiles

Jahin Ahmed received her BSc Engg and is currently pursuing her M.Sc. Engg in the Biomedical Engineering Department of Military Institute of Science & Technology (MIST), Mirpur Cantonment, Dhaka-1216, Bangladesh. In addition to her postgraduate studies, she serves as a Lecturer in the same department of MIST. Her research interests are diverse, including Biomedical Image Processing, Biomedical Signal Processing, Medical Image Encryption, Embedded System Design, etc. Her current research is focused on the spatiotemporal modelling of brain activation patterns using electroencephalography (EEG) and functional near-infrared spectroscopy (fNIRS) signals.

Faizul Hakim received his BSc Engg and is currently pursuing his M.Sc. Engg in the Biomedical Engineering Department of Military Institute of Science & Technology (MIST), Mirpur Cantonment, Dhaka-1216, Bangladesh. Alongside his postgraduate studies, he serves as a Lecturer in the same department of MIST. He is currently focused on assessing surgical tasks and investigating the impact of neurostimulation on skill acquisition using optical neuroimaging data. His research interests span image cryptography for secure data transfer, spatiotemporal modeling of brain activity from EEG signals, deep learning, signal and image processing, etc.

Md Asadur Rahman (Member, IEEE, and IEB) received the B.Sc. and M.Sc. degrees from the Department of Electrical and Electronic Engineering, KUET, Bangladesh, in 2012 and 2014, respectively, and the Ph.D. degree from the Department of Biomedical Engineering, KUET, in 2020. Now, he is an assistant professor at the Department of Biomedical Engineering, MIST, Dhaka, Bangladesh. His research interests include neuro-imaging, brain–computer interfaces, intelligent algorithms, functional brain mapping, medical image encryption, embedded system design, etc. He contributes as an editor in Frontiers in Neuroscience journal and reviewer of more than 20 internationally reputed journals.

How to cite this paper: Jahin Ahmed, Faizul Hakim, Md. Asadur Rahman, "Multi-Stage Medical Image Encryption System Combining RSA and Steganography", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.17, No.3, pp. 146-158, 2025. DOI:10.5815/ijigsp.2025.03.08