International Journal for Modern Trends in Science and Technology
Volume 11, Issue 07, pages 189-195.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol11issue07.html
DOI: https://doi.org/10.5281/zenodo.16131370

Medical Image Encryption Using RSA-Based Asymmetric Cryptosystem

K. Appala Raju, Sk Ishaaq, S Pramod, M Vamsi

Department of Electronics and Communication Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada, India.

To Cite this Article
K. Appala Raju, Sk Ishaaq, S Pramod & M Vamsi (2025). Medical Image Encryption Using RSA-Based Asymmetric Cryptosystem. International Journal for Modern Trends in Science and Technology, 11(07), 189-195. https://doi.org/10.5281/zenodo.16131370

Article Info
Received: 14 May 2025; Accepted: 06 July 2025.; Published: 17 July 2025.

KEYWORDS

Number of Pixel Change Rate, Unified Average Changing Intensity, Blum-Goldwasser Cryptosystem.

ABSTRACT

In the digital era, securing medical data is paramount due to its sensitive nature and increasing cyber threats. This article presents an innovative image encryption approach leveraging the strengths of the RSA algorithm and the Blum-Goldwasser Cryptosystem (BGC). The proposed method integrates chaotic properties from a sequence generator to enhance randomness in encrypted images, improving security. The encryption process begins with a secure key exchange mechanism using RSA, followed by probabilistic encryption through BGC. Pixel randomization is achieved via a chaotic map, ensuring a high degree of unpredictability in the encrypted image. The combination of RSA and BGC fortifies the security framework by incorporating the computational hardness of integer factorization, probabilistic encryption, and quadratic residuosity problems. This hybrid approach strengthens resistance against common cyber threats such as brute-force attacks and differential cryptanalysis.

Extensive simulations and performance evaluations confirm the effectiveness and computational efficiency of the proposed encryption scheme compared to existing methods. The experimental results demonstrate that the proposed method achieves an information entropy of 7.9998, an average correlation of 0.0010, a Number of Pixel Change Rate (NPCR) of 99.6901%, and a Unified Average Changing Intensity (UACI) of 33.5260%. Additionally, the total encryption time is recorded as 0.142 seconds, indicating the efficiency of the approach. These results highlight the robustness of the hybrid chaotic encryption method in ensuring data security, making it suitable for applications requiring high levels of protection. By integrating RSA and BGC with chaotic mapping, the proposed encryption framework offers a reliable and efficient solution for safeguarding sensitive

1. INTRODUCTION

Medical imaging has become an integral part of modern healthcare, serving as a crucial tool for diagnosing diseases, evaluating treatment efficacy, and planning surgical procedures. Advanced imaging technologies, ranging from X-rays to magnetic resonance imaging (MRI), provide invaluable insights into the internal structures of the human body[1]. These tools allow healthcare professionals to detect abnormalities that may not be visible during routine physical examinations, enabling early intervention and improved patient outcomes. Among these imaging modalities, dental radiographs play a significant role in oral healthcare. These images offer detailed visual representations of the teeth, gums, and jaw, allowing dentists to diagnose conditions such as cavities, bone loss, cysts, tumors, and misaligned teeth [2]. By leveraging dental radiographs, dental professionals can devise precise treatment plans, track disease progression, and ensure optimal patient care.

Beyond medical diagnostics, dental X-rays also hold importance in forensic science. They serve as a reliable method for human identification in legal and criminal investigations, aiding in cases where other means of identification are unavailable. Given their sensitive nature, protecting dental X-rays and other medical images from unauthorized access is paramount [3]. The increasing digitization of healthcare records, including medical imaging, has made cybersecurity a critical concern. Unauthorized access to these images can lead to privacy breaches, identity theft, and even manipulation of medical data [4]. To mitigate these risks, robust encryption mechanisms must be implemented to ensure secure storage, transmission, and access to medical images.

With the growing prevalence of cyber threats, researchers have focused on developing encryption methods that enhance the security of medical images while maintaining computational efficiency. This paper proposes a novel image encryption technique tailored for securing dental X- rays. Unlike traditional encryption techniques that rely solely on chaotic systems or minor improvements to existing algorithms, our approach integrates the RSA algorithm with the Blum- Goldwasser cryptosystem (BGC), strengthened by a chaotic sequence generator to enhance randomness and security [5]. This combination ensures robust protection against cyber threats by incorporating multiple layers of security principles, including integer factorization problems, probabilistic encryption, and quadratic residuosity problems. By leveraging these cryptographic foundations, our method enhances the security and resilience of encrypted medical images against various attacks, including brute force, differential analysis, and chosen plaintext attacks [6].

Medical image encryption has garnered significant attention in recent years, with numerous studies proposing various approaches to enhance security [7]. Some researchers have prioritized reducing the time complexity of encryption algorithms, optimizing them for real-time medical applications. Others have focused on expanding the storage efficiency of encryption techniques to accommodate large volumes of medical images. Additionally, some studies have aimed to strengthen the overall security of encryption methods by introducing novel cryptographic models [8]. For example, one study proposed an encryption technique using fuzzy integer subsets and substitution-box (S-box) transformations, demonstrating improved security and dependability. Another research effort introduced a hyperchaotic system, ImproBsys, which combines compressive sensing with public key encryption to reduce data size and transmission overhead while maintaining encryption robustness [9]. However, higher compression ratios in multi-image encryption may affect image restoration quality.

Other researchers have focused on developing efficient pseudo-random number generators (PRNGs) for image encryption. One such study presented a lightweight PRNG based on elliptic curves, which leverages the discrete logarithm problem to generate secure bitstreams with minimal computational overhead. This approach is particularly suitable for real-time encryption applications due to its low resource consumption [10]. Another study combined elliptic curve ElGamal encryption with chaotic systems, employing SHA-512 hashing to generate initial values and improve pixel randomness. This method demonstrated high resistance to known plaintext and chosen plaintext attacks. Similarly, an encryption scheme using dynamic S-boxes and chaotic additive masks showcased resilience against cryptographic attacks while

achieving high encryption speeds of approximately 60 MB/s [11]. This technique is also adaptable for encrypting color images.

Chaotic maps have been widely explored in image encryption due to their ability to enhance randomness and diffusion properties [12]. A study employing chaotic 3D and 4D Arnold Cat maps improved encryption quality for grayscale and color images, demonstrating higher entropy and lower pixel correlation compared to conventional methods. Another research effort introduced an image encryption model using the Elliptic Curve Integrated Encryption Scheme (ECIES), integrating affine power transformation for diffusion. This scheme utilized a 128-bit symmetric key, dividing it into diffusion and confusion components to enhance security [13].

Other studies have emphasized the security of telemedicine systems, where encrypted medical images must be securely transmitted over networks. A research paper introduced an improved encryption scheme for Telemedicine Information Systems (TMIS) that incorporated ECIES for secure key negotiation and self-invertible matrix transformations to prevent exhaustive search attacks. Another work presented a public-key encryption strategy based on elliptic curves, which precomputed a public elliptic curve to reduce computational complexity [14]. This approach masked plaintext pixels with random numbers and scrambled them using dynamic S-box transformations.

Despite the advancements in elliptic curve cryptography (ECC)-based image encryption techniques, our research diverges from existing methodologies by replacing ECC with the RSA algorithm in conjunction with the Blum-Goldwasser cryptosystem. RSA, based on the complexity of integer factorization, provides a robust alternative to ECC while maintaining strong security guarantees. The inclusion of BGC introduces probabilistic encryption, which enhances the unpredictability of ciphertexts, making it more resistant to cryptographic attacks [15]. Furthermore, our method incorporates chaotic maps to ensure pixel-level diffusion and confusion, significantly improving the resilience of encrypted images.

Our proposed approach addresses key challenges in medical image encryption by offering a balance between security, efficiency, and computational feasibility. Through extensive performance evaluations, we demonstrate that our encryption scheme achieves superior entropy values, lower pixel correlation, and faster encryption times compared to conventional methods. These results validate the efficacy of our encryption model in safeguarding sensitive medical images, particularly dental radiographs, which are critical for both medical diagnostics and forensic applications. By integrating RSA, BGC, and chaotic sequence generators, our encryption framework offers a robust and efficient solution for protecting medical imaging data in an increasingly digital and interconnected healthcare environment.

2. BASIC PRELIMINARIES

The RSA algorithm, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is one of the most widely used public-key cryptographic systems. It is primarily employed for secure data transmission and digital signatures. Unlike symmetric encryption methods that use a single key for both encryption and decryption, RSA employs a pair of keys: a public key for encryption and a private key for decryption. This asymmetry makes RSA highly secure, provided the key size is sufficiently large. The security of RSA is based on the computational difficulty of factoring large prime numbers, a problem that remains infeasible for classical computers at large scales. The algorithm begins with key generation, where two large prime numbers, pp and qq, are chosen and multiplied to obtain nn, the modulus for both the public and private keys. The totient function $\phi(n)\backslash phi(n)$ is computed as $(p-1)(q-1)(p-1)(q-1)$, and a public exponent ee is selected, typically 65537, for its mathematical properties that balance security and computational efficiency. The private exponent dd is then calculated as the modular inverse of ee with respect to $\phi(n)\backslash phi(n)$, ensuring that encryption and decryption are mathematically reversible. Encryption in RSA is performed using the public key, where plaintext is raised to the power of ee and taken modulo nn, resulting in ciphertext. Decryption follows the reverse process, raising the ciphertext to the power of dd modulo nn, restoring the original plaintext. RSA's security is reinforced by the fact that, given only nn and ee, an attacker would need to factorize nn to compute dd, a task that is computationally infeasible for large values of nn. Despite its robust security, RSA is computationally intensive compared to symmetric algorithms, making it

less suitable for encrypting large data volumes. Instead, it is often used in hybrid cryptographic systems where it encrypts symmetric keys, which then handle bulk data encryption. RSA is widely used in digital signatures, where a sender signs a message using their private key, and the recipient verifies the authenticity using the sender's public key. This ensures data integrity and non-repudiation, making RSA crucial for securing financial transactions, email communication, and authentication mechanisms.

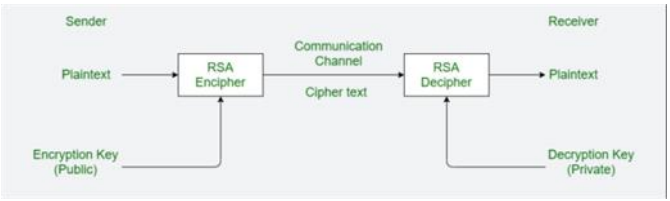

Fig.1 RSA Algorithm

However, RSA is not immune to threats, especially with advancements in quantum computing, which could potentially break its security through Shor's algorithm. To mitigate this, cryptographic research is focusing on post-quantum algorithms that can resist quantum attacks. Despite these challenges, RSA remains a cornerstone of modern cryptography, trusted for securing sensitive data in various applications, from online banking to secure communications. To enhance its security, implementations often use padding schemes like OAEP (Optimal Asymmetric Encryption Padding) to prevent attacks such as chosen-plaintext attacks. Furthermore, RSA key sizes have progressively increased over time, with a minimum recommended size of 2048 bits for adequate security. Organizations handling highly sensitive data may even use 4096- bit keys for enhanced protection. Overall, RSA's enduring relevance is a testament to its mathematical elegance and effectiveness in providing confidentiality, authentication, and data integrity in the digital age.

3. RESULTS AND DISCUSSION

a) Entropy and Security Analysis

Entropy measures the randomness or unpredictability of a system, which is a key indicator of encryption strength. In the RSA algorithm, a high entropy value signifies a well-encrypted message with a strong level of security. Since RSA encryption transforms plaintext into an unpredictable ciphertext through modular exponentiation, its entropy is generally high, making it resistant to attacks that rely on pattern recognition. A robust cryptographic system ensures that ciphertext distributions appear random and exhibit no discernible patterns. This is crucial because lower entropy values might indicate a weak encryption method, making it susceptible to attacks. When evaluating RSA's effectiveness, comparing entropy values with other encryption techniques helps assess its resilience against cryptographic attacks. The higher the entropy of RSA-encrypted data, the more secure it is from unauthorized decryption attempts.

b) Peak Signal-to-Noise Ratio (PSNR) in Image Encryption

When applying RSA encryption to images, the effectiveness of the method can be assessed using the Peak Signal-to-Noise Ratio (PSNR). PSNR measures the ratio between the maximum possible power of an image and the noise introduced during encryption. In the context of RSA-based image encryption, PSNR values tend to be low since the encryption process significantly alters the pixel values to make the image unrecognizable. A lower PSNR value indicates that the encrypted image is vastly different from its original counterpart, thereby improving security. However, when decrypting the image, the goal is to restore the original content as accurately as possible. A higher PSNR value between the decrypted and original images suggests that the decryption process is successful with minimal loss of information. Comparing PSNR values of RSA with other cryptographic techniques provides insights into its efficiency in securing visual data.

c) Structural Similarity Index (SSIM) for Image Comparison

The Structural Similarity Index (SSIM) measures the visual similarity between two images, with values ranging from -1 to 1. In an ideal encryption scheme using RSA, the SSIM between the original and encrypted image should be close to zero, indicating minimal resemblance and ensuring strong security. A higher SSIM value between the decrypted and original images signifies successful decryption, demonstrating RSA's ability to preserve image integrity. The effectiveness of RSA encryption can be analyzed by comparing SSIM values with other encryption methods. Since RSA operates on large numerical values derived from

modular arithmetic, its encrypted output differs significantly from the input, ensuring secure data protection.

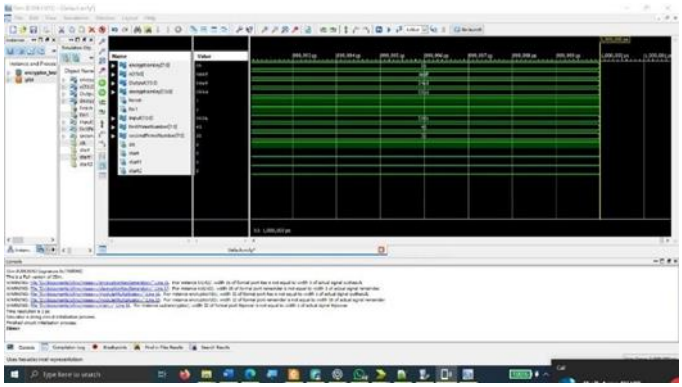

Fig.2 Encryption Output using RSA

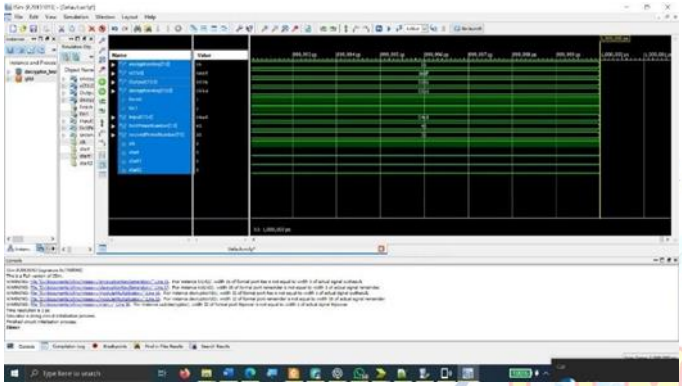

Fig.3 Decryption Output using RSA

d) Histogram Analysis for Encrypted Images

A histogram represents the distribution of pixel intensities in an image. In an unencrypted image, the histogram exhibits distinct peaks corresponding to variations in colors and intensities. However, after encryption using RSA, the histogram should appear uniform, eliminating identifiable patterns that could be exploited by attackers. This randomness is a key feature of strong encryption. If an encrypted image retains the structured histogram of the original, it indicates potential weaknesses in the encryption process. By analyzing histograms, RSA's ability to generate unpredictable ciphertext for image encryption can be evaluated and compared with other encryption schemes to determine its robustness.

e) Key Space Analysis and Resistance to Brute Force Attacks

The strength of an encryption algorithm heavily depends on its key space, which refers to the total number of possible keys that can be used. In RSA, security is based on the difficulty of factoring large prime numbers. For a standard RSA implementation with a 2048-bit key, the key space is approximately 220482^{2048}, making brute-force attacks computationally infeasible. Compared to other encryption techniques, RSA provides superior security by leveraging mathematical complexity rather than just key length. The RSA algorithm's security is further enhanced when larger key sizes, such as 3072-bit or 4096-bit, are used. A comparison of RSA's key space with other cryptographic methods highlights its robustness against brute-force decryption attempts.

f) Correlation Coefficient in Encrypted and Decrypted Data

In image encryption, the correlation coefficient measures the degree of similarity between the original and encrypted images. Ideally, encrypted images should exhibit a low correlation coefficient, meaning the encryption process has effectively obscured patterns from the original image. Since RSA encryption applies modular exponentiation, it significantly alters pixel values, resulting in low correlation coefficients. However, the correlation coefficient between the original and decrypted image should be close to 1, indicating successful decryption. This metric is particularly useful in assessing RSA's performance in image encryption and ensuring that patterns from the original data are not retained in the encrypted output.

g) Key Sensitivity Analysis

A highly secure encryption scheme must be sensitive to even minor modifications in the key. In RSA, if a slightly altered key is used for decryption, the resulting plaintext should be vastly different from the original, demonstrating the method's sensitivity. This is because RSA relies on precisely calculated mathematical relationships between the public and private keys. Any deviation in the private key disrupts the decryption process, preventing unauthorized access. Testing RSA's key sensitivity by introducing small changes in the decryption key helps evaluate its resilience against attacks attempting to derive the private key from the public key.

h) Time Performance Analysis

The efficiency of an encryption algorithm is critical, especially in real-time applications requiring fast processing. RSA, while highly secure, is computationally intensive compared to symmetric- key encryption techniques due to its reliance on modular exponentiation. However, RSA is often used in

conjunction with symmetric encryption in hybrid cryptosystems, where it encrypts session keys rather than large datasets, optimizing performance. Benchmark tests comparing RSA's encryption and decryption times with other cryptographic methods highlight its relative efficiency. The execution time of RSA is influenced by key size, with larger keys requiring more processing time. Despite its computational demands, RSA's security benefits make it a preferred choice for applications requiring secure key exchange and digital signatures.

The RSA algorithm remains one of the most reliable cryptographic techniques due to its strong security foundation based on number theory. Its high entropy ensures randomness in encrypted data, while PSNR and SSIM metrics confirm its effectiveness in image encryption. Histogram analysis and correlation coefficients demonstrate RSA's ability to remove patterns, enhancing security. With a vast key space, RSA offers strong resistance to brute-force attacks, and its key sensitivity prevents unauthorized decryption. Though RSA is computationally intensive, it is widely used for securing sensitive communications and digital transactions. A comparative analysis of its performance metrics with other encryption methods reaffirms its role in modern cryptography.

4. SUMMARY AND CONCLUSIONS

One of the primary strengths of the RSA encryption algorithm lies in its foundation on the difficulty of factorizing large prime numbers. This makes it highly secure against conventional cryptanalysis techniques. By integrating RSA with the Blum- Goldwasser Cryptosystem, the proposed approach enhances randomness and unpredictability in encrypted data, thereby reducing the risk of pattern recognition attacks. Additionally, the RSA algorithm's ability to provide strong encryption with asymmetric key pairs ensures that even if one part of the system is exposed, decryption remains computationally infeasible without the correct private key. This feature is particularly useful in medical image security, where data integrity and confidentiality are paramount.

The proposed method is also highly sensitive to encryption keys, meaning even a minor alteration in the key leads to significantly different encrypted outputs. This property ensures resistance against brute-force attacks, where attackers attempt to guess encryption keys. Furthermore, the resilience of RSA against various cryptographic threats, such as chosen plaintext and differential attacks, strengthens its suitability for medical image encryption. Given the sensitive nature of medical data, any encryption technique must be able to safeguard against evolving cybersecurity threats. RSA's reliance on public and private keys makes it an ideal choice for secure data transmission, particularly in cloud-based healthcare systems where data is often transmitted across multiple networks.

Another key advantage of this method is its adaptability to real-time encryption applications. The computational efficiency achieved through RSA's modular exponentiation ensures that encryption and decryption processes are executed with minimal delays. In medical environments, where timely access to imaging data is essential for diagnosis and treatment, the speed of encryption is a crucial factor. The proposed RSA-based encryption system effectively balances security and performance, making it a viable option for practical deployment in healthcare institutions.

However, one potential limitation of RSA encryption is its vulnerability to quantum computing attacks. Future advancements in quantum computing could significantly reduce the time required to factorize large prime numbers, thereby compromising RSA's security. While current computational resources make breaking RSA encryption infeasible, the emergence of quantum cryptographic algorithms may necessitate modifications or alternative encryption schemes in the future. Researchers are already exploring post- quantum cryptographic techniques to mitigate these potential threats, ensuring that encryption remains secure even as technology evolves. Despite this concern, RSA continues to be one of the most widely used and trusted encryption algorithms in digital security.

Beyond medical imaging, the proposed RSA-based encryption method holds promise for broader applications, including securing audio and video data. Many fields, such as defense, finance, and multimedia communications, require robust encryption to protect sensitive information. The versatility of RSA encryption makes it a strong candidate for extending its use beyond medical applications to various industries requiring high- security standards. By refining and optimizing RSA- based encryption techniques, future implementations can further enhance security,

efficiency, and adaptability to new technological advancements.

The encrypted medical images used in this study are available from the corresponding author upon reasonable request. Additional standard images utilized for comparative analysis were obtained from publicly available datasets. All generated and analyzed data that contributed to the conclusions of this study are documented in the article and supplementary materials. The research findings highlight RSA's potential as a powerful encryption tool for securing medical images while maintaining computational efficiency. By addressing key security challenges and optimizing performance, the proposed encryption technique paves the way for improved data protection in digital healthcare environments.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Razaq, A., Maghrabi, L. A., Ahmad, M., Aslam, F., & Feng, W. (2024). Fuzzy logic-based substitution-box for robust medical image encryption in telemedicine. Ieee Access, 12, 7584-7608.

[2] Odeh, A., & Taleb, A. A. (2023). A Multi-Faceted Encryption Strategy for Securing Patient Information in Medical Imaging. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14(4), 164-176.

[3] Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., ... & Hassan, M. A. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access, 9, 47731-47742.

[4] Singh, K. N., Singh, O. P., Singh, A. K., & Agrawal, A. K. (2023). EiMOL: a secure medical image encryption algorithm based on optimization and the Lorenz system. ACM Transactions on Multimedia Computing, Communications and Applications, 19(2s), 1- 19.

[5] Ahmed, S. T., Hammood, D. A., Chisab, R. F., Al-Naji, A., & Chahl,

[6] J. (2023). Medical image encryption: a comprehensive review. Computers, 12(8), 160.

[7] Afzal, I., Parah, S. A., Hurrah, N. N., & Song, O. Y. (2024). Secure patient data transmission on resource constrained platform. Multimedia Tools and Applications, 1-26.

[8] Alslman, Y., Alnagi, E., Ahmad, A., AbuHour, Y., Younisse, R., & Abu Al-haija, Q. (2022). Hybrid encryption scheme for medical imaging using autoencoder and advanced encryption standard. Electronics, 11(23), 3967.

[9] Jain, J., & Jain, A. (2022). Securing E-Healthcare Images Using an Efficient Image Encryption Model. Scientific Programming, 2022(1), 6438331.

[10] Rehman, M. U., Shafique, A., Khan, M. S., Driss, M., Boulila, W., Ghadi, Y. Y., ... & Ahmad, J. (2024). A novel medical image data

[11]

[12] protection scheme for smart healthcare system. CAAI Transactions on Intelligence Technology, 9(4), 821-836.

[13] Singh, A. K. (2022). Fastmie: faster medical image encryption without compromising security. Measurement, 196, 111175.

[14] Singh, K. N., Baranwal, N., Singh, O. P., & Singh, A. K. (2024). Deepenc: Deep learning-based roi selection for encryption of medical images through key generation with multimodal information fusion. IEEE Transactions on Consumer Electronics.

[15] Khan, J., Li, J., Haq, A. U., Parveen, S., Khan, G. A., Shahid, M., ... & Ruinan, S. (2019, December). Medical image encryption into smart healthcare IOT system. In 2019 16th international computer conference on wavelet active media technology and information processing (pp. 378-382). IEEE.

[16] Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., & Fouda, M. M. (2021). A new image encryption algorithm for grey and color medical images. Ieee Access, 9, 37855-37865.

[17] Khan, J., Li, J. P., Ahamad, B., Parveen, S., Haq, A. U., Khan, G. A., & Sangaiah, A. K. (2020). SMSH: Secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption. IEEE Access, 8, 15747-15767.

[18] Ahmad, M., Alkanhel, R., El-Shafai, W., Algarni, A. D., Abd El-Samie, F. E., & Soliman, N. F. (2022). Multi-objective evolution of strong S-boxes using non-dominated sorting genetic algorithm-II and chaos for secure telemedicine. IEEE Access, 10, 112757-112775.