Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
e-ISSN: 2790-4822p-ISSN: 2958-0862

Image Authentication Using Public Key

Mohammed Mahmoud Farhan[1]*

[1]Islamic University of Lebanon Faculty of Engineering Department of Graduate Studies, Lebanon.

*Corresponding Author: Mohammed Mahmoud Farhan

DOI: https://doi.org/10.55145/ajest.2025.04.01.007
Received June 2024; Accepted August 2024; Available online September 2024

ABSTRACT: This study talked about importance of data protection during Internet communication and highlights the utilize of image encryption as a specialized method. Image encryptions contain the utilize of unique key values to hide and show messages within images, with algorithms that are difficult to decryption. This work focuses on a modified version of the Rivest-Shamir-Adleman (RSA) encryption system, which is compatible with grayscale and color images and is implemented in C#. Additionally, it combines Advanced Encryption Standard (AES) and cryptography techniques to enhance encryption protection. Decrypting a confused image contain complex computations with large seed numbers. This proposed addresses image encryption, presenting a higher level of security compared to the original RSA encryption scheme. This research proposed experts in information technology should consider utilizing the modified RSA encryption system to support security during image transmission.

Keywords: Image authentication, RSA, Public key cryptography, Steganography

1. INTRODUCTION

Starts with an ancient Greek story about Hystaus utilizing cunning to convey a secret message in order to give a historical perspective on the idea of hiding information. It also mentions World War II-era developments in particle technology and the challenges of identifying hidden information in cover letters during the printing era [1-3]. The introduction highlights the importance of information security in the modern time, with a focus on encryption and cryptography in the context of digital data transmission [4,5]. It explains the division of cryptography into symmetric and asymmetric methods, emphasizing the limitations of asymmetric cryptography for handling large amounts of data, such as images [6]. The concept of steganography as a means to enhance security is introduced, with a mention of the LSB (Less Significant Bit) replacement technique [7]. Overall, the introduction sets the stage for a discussion on encryption, steganography, and their relevance in modern information security [8].

In the digital age need for strong security measures in the transmission of visual data has never been more important. Images as a significant average of information exchange, are often weak to unauthorized access, tampering, and other security threats [9,10]. To address these challenges this study focuses on the development of an advanced image encryption system that merges modern encryption techniques with cryptography. The main objective is to ensure the secrecy, integrity, and authenticity of images as they traverse the internet.

Efficient techniques are important for encrypting and decrypting internet-sent data in a time of critical data security [11]. The specialized part of encryption is image encryption, a process that employs a unique key to conceal and reveal hidden messages within images. The complexity and rarity of the algorithms involved make deciphering the code and uncovering the original message exceptionally challenging [12,13].

The research problem relates to the need to ensure the protection of data transmitted over the Internet, which requires the use of effective methods of encryption and decryption. One of the challenges in this context is securing images and ensuring the confidentiality of their content through encryption and authentication.

This research project aims to achieve the development of a modern image encryption system: The primary goal is to create a powerful system for encrypting and decrypting images using contemporary encryption techniques and the use of steganography techniques: integrating steganography techniques to embed additional information within images, ensuring secure and inconspicuous data transmission. Study and evaluate the effectiveness of certain technologies, including modified RSA and AES, in enhancing image security. Enhancing security levels: improving the general level of security and protection to ensure the confidentiality and integrity of images transmitted over the Internet. Provide

*Corresponding author: Ramiw483@gmail.com

experimental evidence: Provide empirical evidence showing how the use of the modified RSA encryption scheme enhances the security of image transmission and effectively

2. PROPOSED METHODOLOGY

The methodology for this project involves a multi-phase approach encompassing encoding, decoding, and execution to ensure the security of data transmitted through various media channels. The implementation is supported by both hardware and software interfaces, with the software component being developed using Microsoft .NET within a Windows environment. The key goal is to enhance data security via embedding sensitive information into a file, encrypting it, and then transmitting it. Upon receipt the data is decrypted utilizing a specialized tool [14]. The system utilizes a steganographic application built on the Microsoft .NET Framework to achieve this [15].

The study proposed a modified RSA algorithm that enhances security and efficiency in image encryption. Via adjusting key sizes, improving prime number selection, and optimizing exponentiation, the modified RSA algorithm offers faster and reliable encryption. AES is a symmetric key algorithm known for its efficiency, complements RSA, but its dependence on secure key distribution presents challenges. The proposed system ensures strong encryption and secure key management.

2.1 Hash Function

There exist various vulnerabilities that can be present in messages. To guarantee the integrity and authenticity of received messages, message authentication is employed. One widely used approach for message authentication involves the utilization of a hash function, as illustrated in Figure 1. The main objective of a hash function, denoted as H, is to transform an input string of any length, denoted as m, into a fixed-size output sequence referred to as a hash value, where h == H(m). This particular hash function possesses multiple important characteristics see Figure 1 [16].

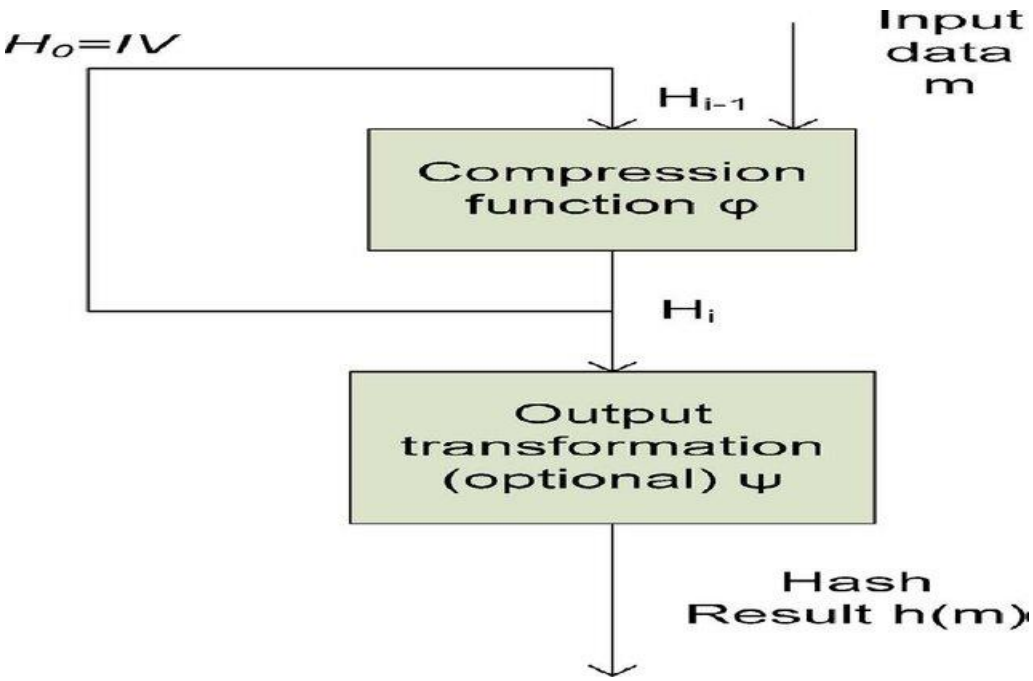

FIGURE 1. - Block diagram of hash function H [16]

2.2 Advanced Encryption Standard (AES)

In 2001, the US introduced the AES as a replacement for DES and 3DES. AES is popular in WLAN security and compression tools due to its simple implementation, low memory requirements, and support for key lengths of 128, 192, or 256 bits [17]. Figure 2 shows AES encryption algorithm.

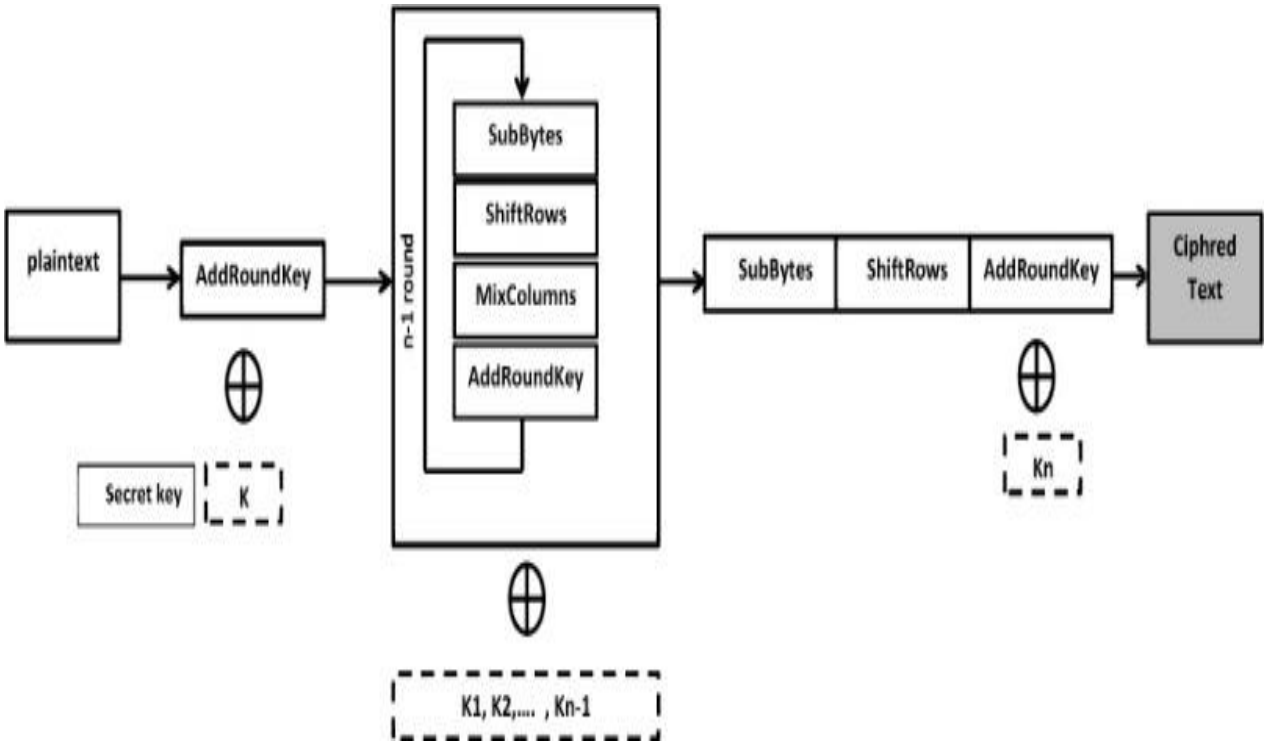

FIGURE 2. - AES encryption algorithm [17]

2.3 RSA Algorithm

In 1977, MIT introduced the world's first public key system called RSA. RSA uses a single algorithm for both encryption and decryption, relying on two keys: one public and one private. The creators, Ron Rivest, Adi Shamir, and Leonard Adleman, documented their work on manipulating extensive numerical quantities. Figure 3 shows asymmetric encryption and decryption.

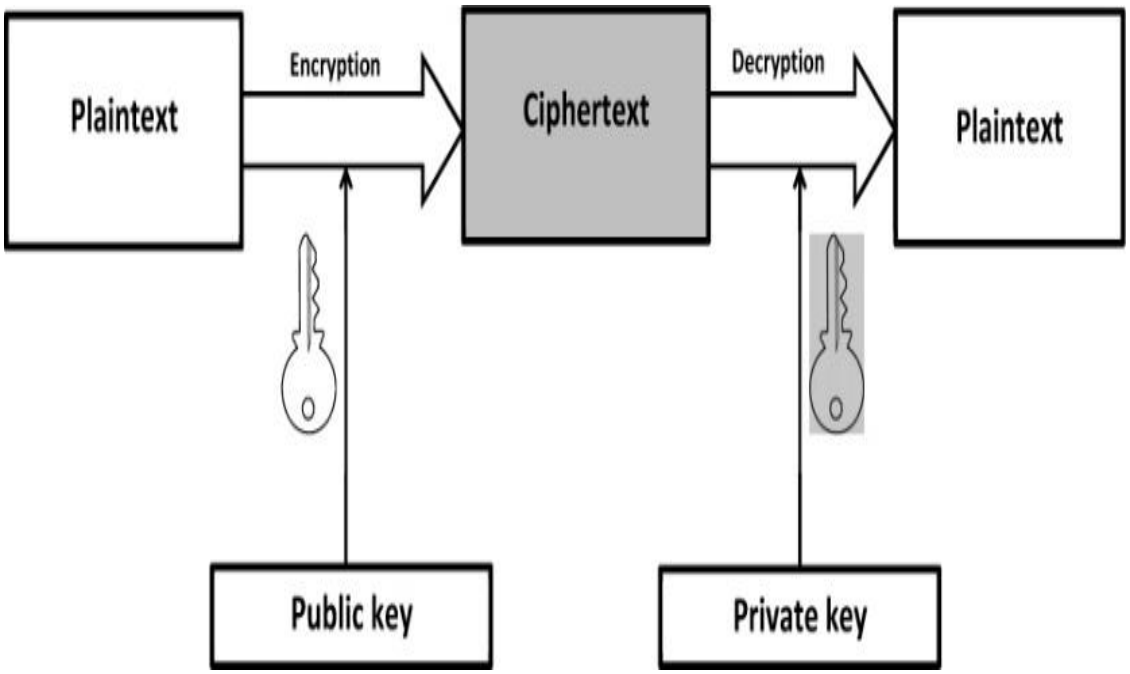

FIGURE 3. - Asymmetric encryption and decryption

RSA employs a single algorithm for both encryption and decryption, necessitating a pair of keys: a public key and a private key [18].

2.4 Non-functional requirements

The elements of a system that extend beyond its core functionality pertain to its performance, dependability, protection, and user-friendliness. These prerequisites establish the system's comprehensive demeanor, limitations, and characteristics of excellence, our main goal when it comes to user interfaces is to create a consistent look and feel that is easy to use and free from unnecessary elements. This strategy enables greater flexibility and scalability within the interface, The entirety of the program will be conducted using the English language, In order for the program to be effective, it is imperative that its processing speed is swift, The program has a series of consecutive tasks that it must execute. To begin, it must apply encryption techniques to both hide and secure the information contained within the file. Afterward, the entire file should undergo encryption. Once the encryption process is complete, the program should then employ a hash function to verify the integrity of the file, ensuring that no unauthorized alterations have taken place. Following this, it needs to decrypt the file and extract the ciphertext. Lastly, it should decrypt the file once more and accurately extract the original file from it, For the system to be classified as high-quality, it is absolutely necessary for all functions to function smoothly and efficiently [19].

A system's non-functional requirements include performance, dependability, protection, and user-friendliness. The main goal is to create a user-friendly interface with a consistent look and feel. The program will be conducted in English, and its processing speed is crucial for effectiveness. It must use encryption techniques, a hash function, decrypt, and extract the original file. For a system to be high-quality, all functions must function smoothly and efficiently as shown in Figure 4.

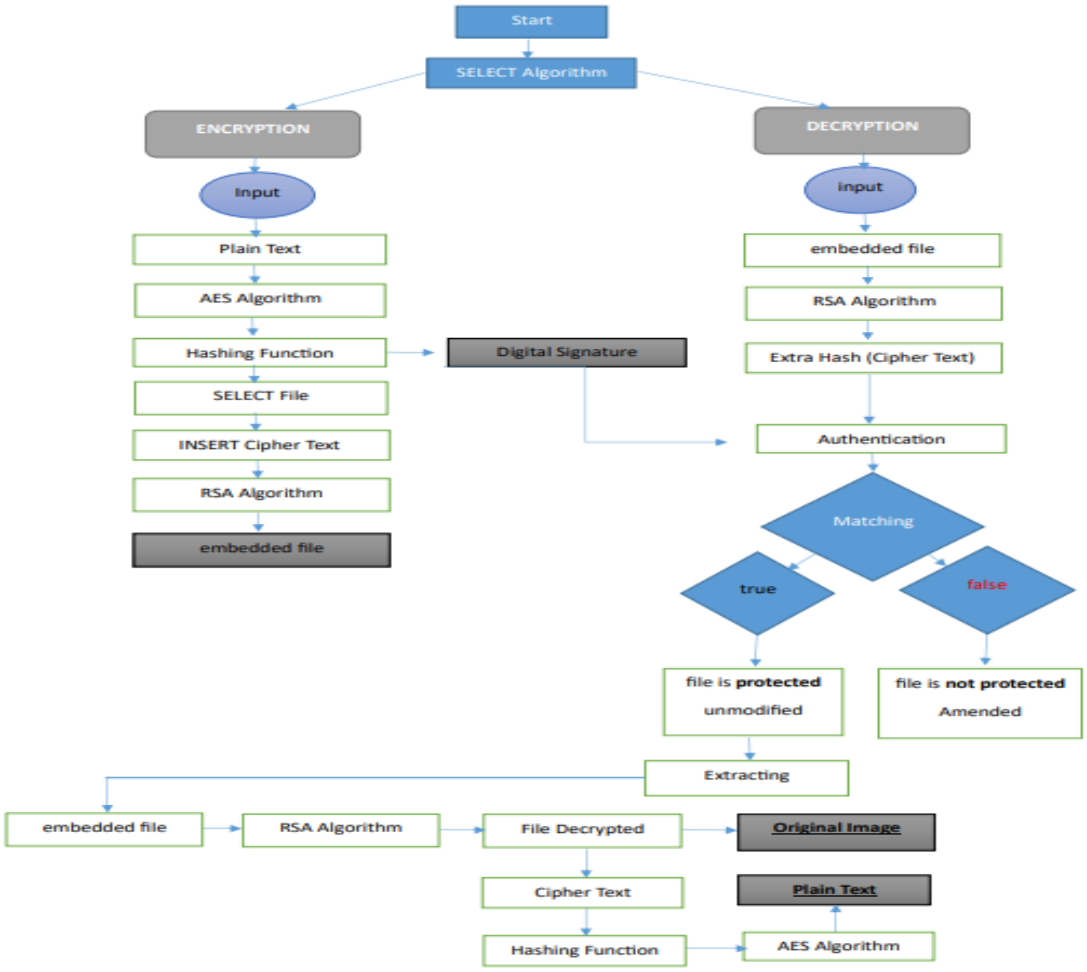

FIGURE 4. - System Data Flow Diagram

The graphical depiction of the movement of data within an information system is known as a data flow diagram (DFD). It serves as a visual model that showcases how the system operates and represents various aspects of its functionality. Typically, this diagram is the initial stage in establishing a comprehensive system overview that can be expanded upon in the future.

The Encryption and Decryption feature button is displayed (see Figure 5).

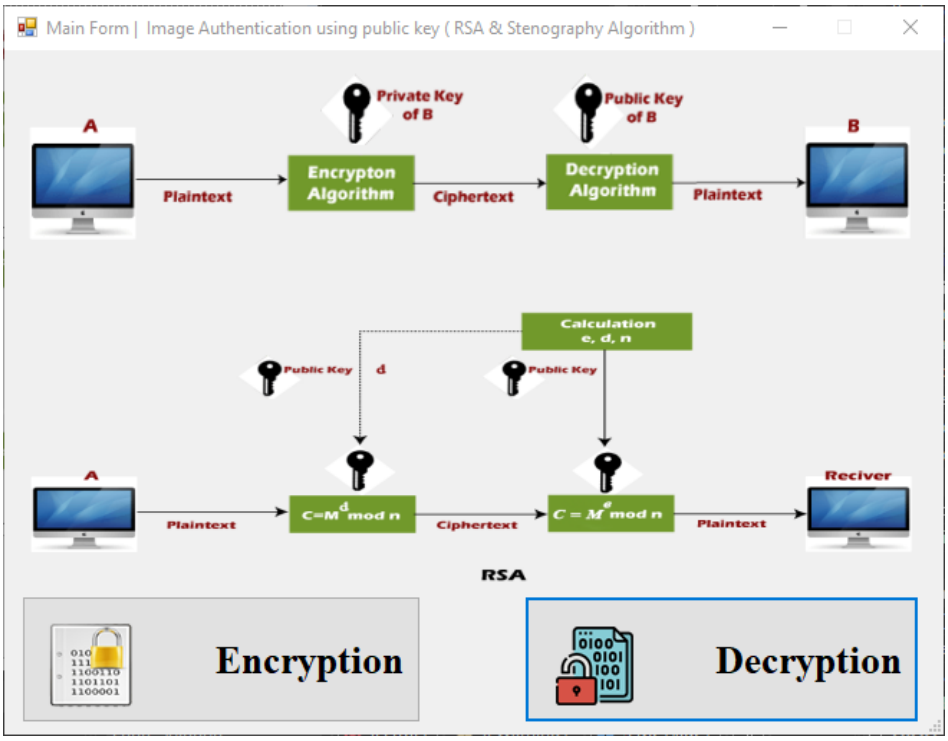

FIGURE 5. - The main form to display the main interface of the program

3. RESULTS AND DISCUSSION

Measuring the quality of encoding is a crucial step in the evaluation of data produced by a text hiding program in an image. The steganography LSB method is employed to assess this encoding quality. The text, which has undergone processing through the hash function method, is subsequently incorporated. The AES encryption algorithm is then applied, allowing for the addition or concealment of text within the file. The RSA algorithm is utilized to encrypt the image itself. During this step, in this study will analyze the image both before and after the encryption process to extract the outcomes and ascertain the alterations made to the image (see Figure 6 and Figure 7).

FIGURE 6. - Original Image After Encryption Processing

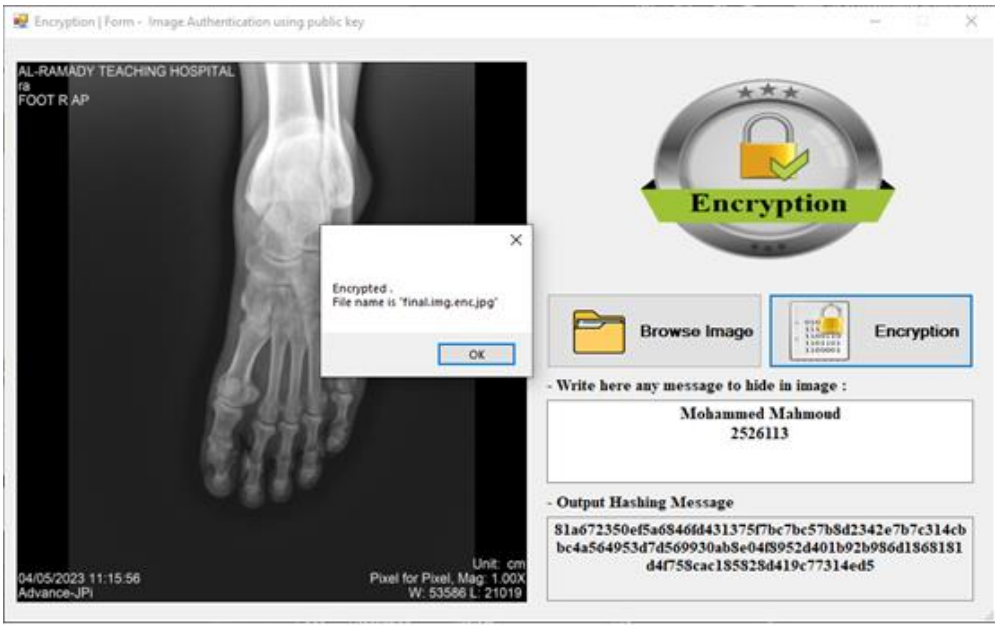

FIGURE 7. - Cipher Image before Encryption Processing

The process of image authentication utilizing public key cryptography contracts the privacy, reliability, and validity of concealed data within images. The software presents a thorough and secure method for concealing text within images through the utilization of LSB masking, hash functions, AES encryption, and RSA encryption. Using combining these technologies, the software guarantees the safeguarding and resistance to tampering of hidden data. To gain a greater understanding of the characteristics of encrypted data and validate its authenticity, histogram analysis and online minutiae extraction can be utilized as components of the image authentication procedure. Here is a step-by-step guide on how to implement these techniques.

The examination of data spreading and the understanding of its characteristics are accomplished through utilize of histogram analysis as a statistical method. This analysis creates a visual representation known as a histogram, which shows the frequency or quantity of data values within chosen time periods or bins. Graph analysis is greatly utilized in diverse sectors, covering data analysis, image processing, quality control, and finance. Examining the histogram of a ciphered image can submission an indication into the dispersal of pixel attributes. As a result of the encryption process, the histogram is able to exhibit a seemingly arbitrary pattern, making it difficult to discern from random noise. Thus, it is impossible that any significant insights or specifics regarding the concealed data or the initial image will be unveiled.

The process of public key authentication works to validate the integrity and genuineness of encoded images. Within the framework of RSA encryption, the private key can be utilized to affix a digital signature to the image. This digital signature functions as a mathematical representation of the image's substance, encrypted utilizing the private key. To determine the authenticity of the image, the corresponding public key is utilized to decipher the digital signature. A successful decryption that returns a matching digital signature confirms the image's integrity and authenticity.

Histogram analysis is a useful tool for visualizing and analyzing image content and potential alterations. It helps detect changes from encoding or steganography techniques before encoding utilizing RSA, AES, or steganography algorithms. Decrypting the image reverses the encoding process, allowing for restoration or retrieval of hidden data. Public key authentication methods like digital signatures ensure the integrity and authenticity of encoded images. Although not directly linked to public key authentication, histogram analysis can complement it. As shown in Figure 8, Figure 9 and Figure 10.

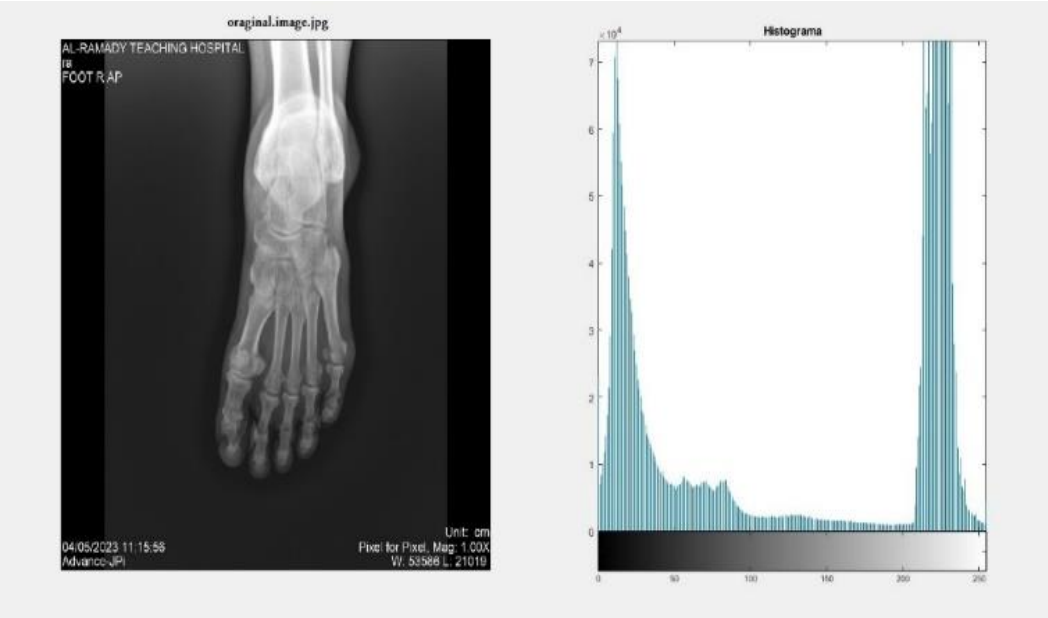

FIGURE 8. - Analyze the plain text file before the encryption process

Prior to initiating the encryption process, it is necessary to conduct a thorough examination of program samples extracted from the dataset. These samples are in the form of images, which are then subjected to a comprehensive histogram analysis. The results obtained from this analysis are visually represented in the image provided above.

In the realm of grayscale images, each pixel is allocated a distinct intensity value that spans from 0 to 255. A significant amount of insight regarding the overall brightness levels, contrast, and tonal distribution of the image can be gleaned from the examination of the histogram. This analysis entails studying the frequency distribution of the aforementioned intensity values. By delving into the histogram, one can ascertain the frequency at which each individual intensity value manifests within the image.

When examining histograms, it is crucial to note that this analysis is commonly performed on grayscale images or on specific color channels (such as red, green, and blue) within color images. Each color channel has the potential to possess its own unique histogram.

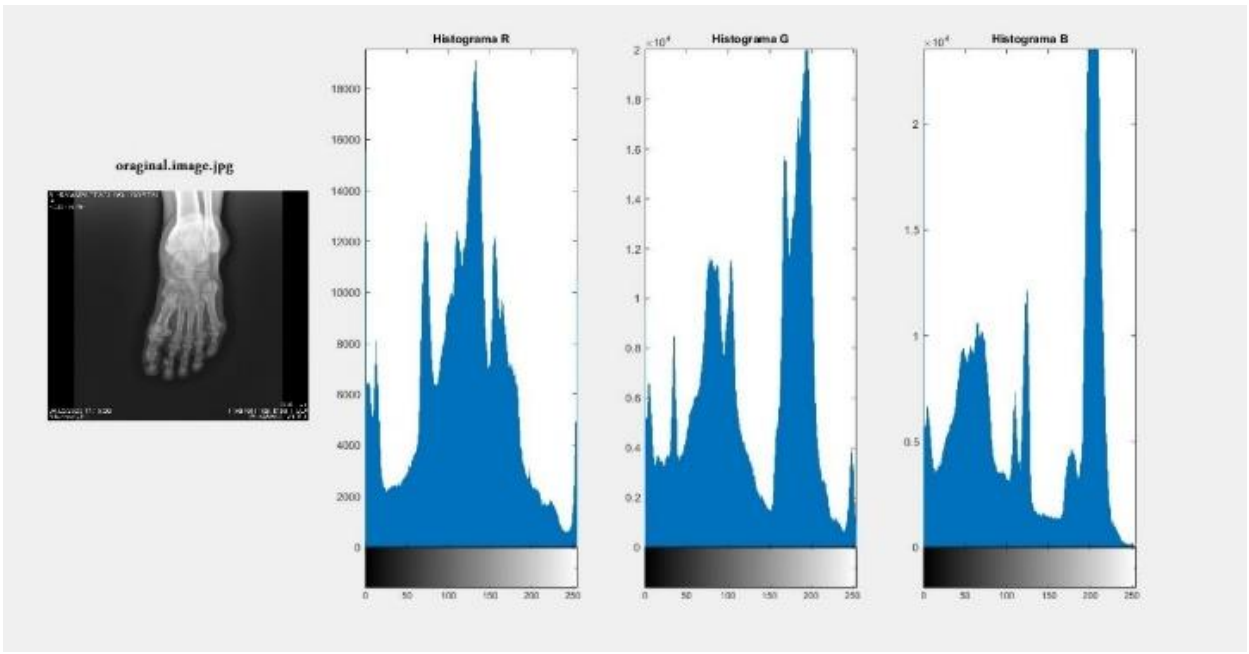

FIGURE 9. - Analysis of the plain text file before the encoding process using RGB channels histogram analysis

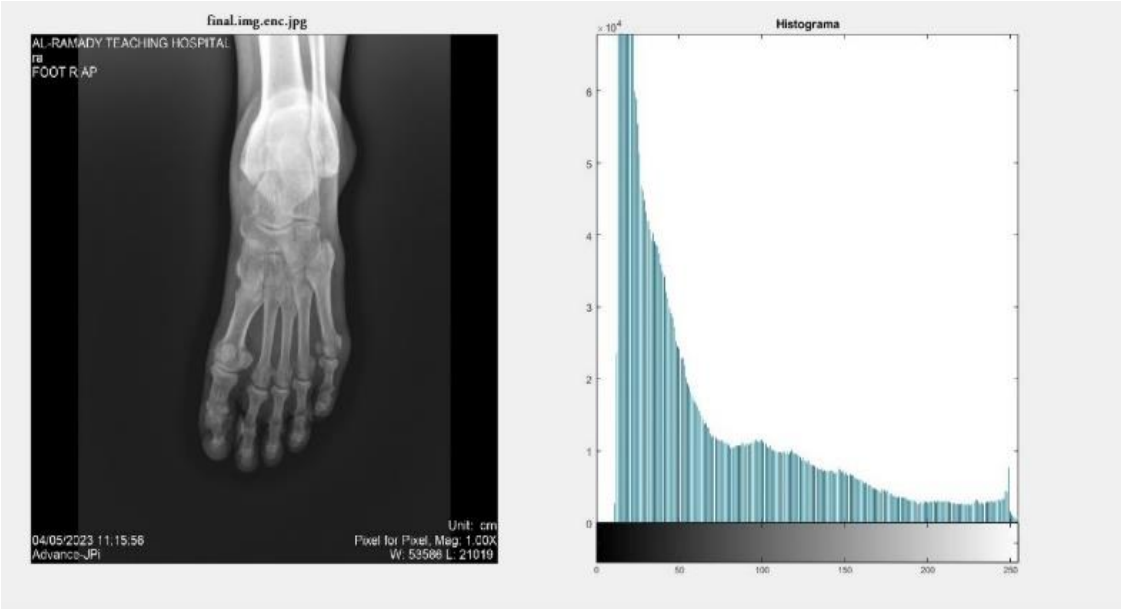

FIGURE 10. - Analysis of the ciphertext file after embedding the ciphertext and graph analysis of the file

The verification of encoded images' authenticity and integrity is achieved through the use of public key authentication. In the process of RSA encryption, a digital signature can be affixed to the image by utilizing the private key. This digital signature functions as a mathematical representation of the image's content, encrypted with the private key. To authenticate the image, the appropriate public key can be employed to decrypt the digital signature. If the decrypted digital signature matches the signature calculated from the image's content, this confirms the image's integrity and authenticity. Prior to being encoded with RSA, AES, and steganography algorithms, metadata extraction can retrieve descriptive information from digital files. This extraction of metadata offers valuable insights about the image, Confidentiality, integrity, and authentication can be ensured by encoding the image. Decrypting the encoded image reverses the encoding process, allowing for the restoration of the original image or the retrieval of concealed data. Techniques such as digital signatures, which rely on public key authentication, can be employed to verify the integrity and authenticity of encoded images (see Figure 11).

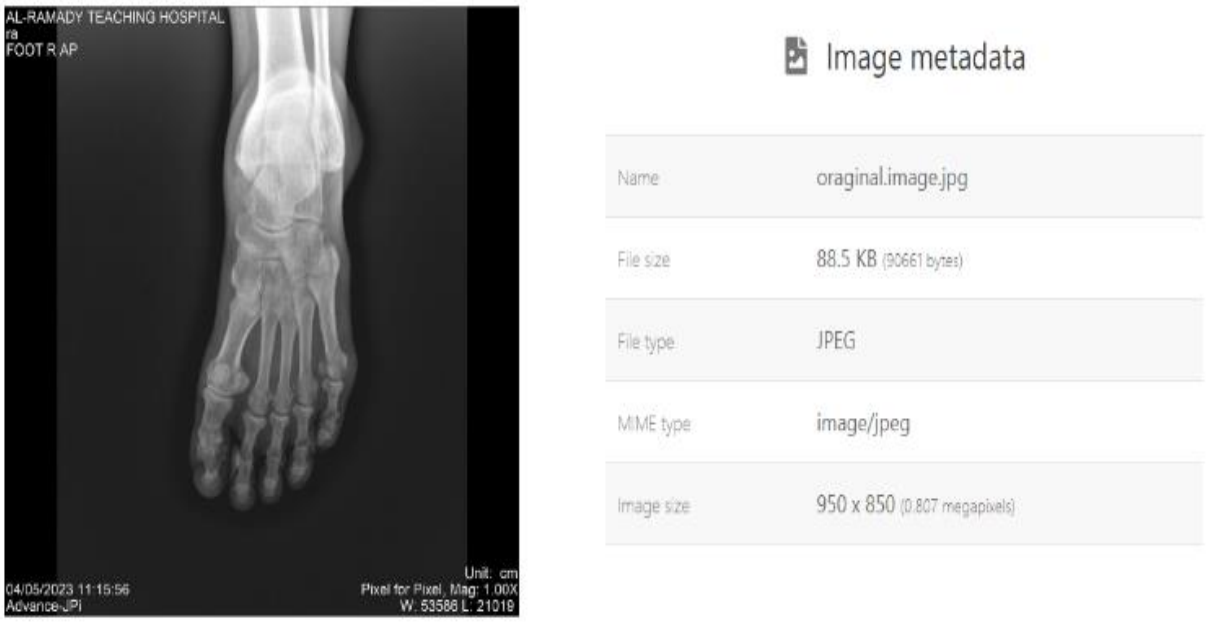

FIGURE 11. - Analysed the cipher text file using metadata extraction

4. CONCLUSION

This work proposed a good mechanism for securely embedding text within images through a combination of AES and RSA encryption. The proposed approach successfully ensures the confidentiality, integrity, and authenticity of the hidden data, making it highly suitable for critical applications like digital forensics and information security. Despite its strengths, this study acknowledges certain limitations, counting the computational intensity of the modified RSA algorithm, which may impact processing times for larger images. In addition, the potential threat of quantum computing to current encryption techniques highlights the need for ongoing research. Future work should focus on optimizing algorithm performance to enhance processing efficiency and exploring quantum-resistant encryption techniques.

FUNDING

None

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their efforts.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

[1] N. S. Mohammed, O. A. Dawood, A. M. Sagheer, and A. A. Nafea, "Secure Smart Contract Based on Blockchain to Prevent the Non-Repudiation Phenomenon," Baghdad Sci. J., vol. 21, no. 1, p. 234, 2024.

[2] A. A. Nafea, M. M. Hamdi, B. saad Abdulhakeem, A. T. Shakir, M. S. I. Alsumaidaie, and A. M. Shaban, "Detection Systems for Distributed Denial-of-Service (DDoS) Attack Based on Time Series: A Review," in 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), 2024, pp. 43–48.

[3] J. W. Cortada, All the facts: a history of information in the United States since 1870. Oxford University Press, 2016.

[4] N. M. Alfahad, S. A. Aliesawi, and F. S. Mubarek, "Enhancing AODV routing protocol based on direction and velocity for real-time urban scenario," J. Theor. Appl. Inf. Technol., 2018.

[5] A. K. Kareem, A. M. Shaban, A. A. Nafea, M. Aljanabi, S. A. S. Aliesawi, and M. Mal-Ani, "Detecting Routing Protocol Low Power and Lossy Network Attacks Using Machine Learning Techniques," in 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), 2024, pp. 57–62.

[6] A. Parekh, M. Antani, K. Suvarna, R. Mangrulkar, and M. Narvekar, "Multilayer symmetric and asymmetric technique for audiovisual cryptography," Multimed. Tools Appl., vol. 83, no. 11, pp. 31465–31503, 2024.

[7] S. Rahman et al., "A novel approach of image steganography for secure communication based on LSB substitution technique," Comput. Mater. Contin., vol. 64, no. 1, pp. 31–61, 2020.

[8] A. Arora, M. P. Singh, P. Thakral, and N. Jarwal, "Image steganography using enhanced LSB substitution technique," in 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2016, pp. 386–389.

[9] O. O. Amoo, F. Osasona, A. Atadoga, B. S. Ayinla, O. A. Farayola, and T. O. Abrahams, "Cybersecurity threats in the age of IoT: A review of protective measures," Int. J. Sci. Res. Arch., vol. 11, no. 1, pp. 1304–1310, 2024.

[10] F. J. Jaime, A. Muñoz, F. Rodríguez-Gómez, and A. Jerez-Calero, "Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare," Sensors, vol. 23, no. 21, p. 8944, 2023.

[11] A. S. Abdalkafor and S. A. Aliesawi, "Data aggregation techniques in wireless sensors networks (WSNs): Taxonomy and an accurate literature survey," in AIP Conference Proceedings, vol. 2400, no. 1,2022.

[12] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photonics, vol. 1, no. 3, pp. 589–636, 2009.

[13] A. A. Nafea, S. A. Alameri, R. R. Majeed, M. A. Khalaf, and M. M. AL-Ani, "A Short Review on Supervised Machine Learning and Deep Learning Techniques in Computer Vision," Babylonian J. Mach. Learn., vol. 2024, pp. 48–55, 2024.

[14] W. Diffie and M. E. Hellman, "New directions in cryptography," in Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman, 2022, pp. 365–390.

[15] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in Proceedings of the 2001 workshop on Multimedia and security: new challenges, 2001, pp. 27–30.

[16] R. Kumar and H. Singh, "Recent trends in text steganography with experimental study," Handb. Comput. Networks Cyber Secur. Princ. Paradig., pp. 849–872, 2020.
[17] J. Daemen, "The Rijndael block cipher," http//www. esat. kuleuven. ac. be/~rijmen/rijndael/, 1998.
[18] S. D. Galbraith, Mathematics of public key cryptography. Cambridge University Press, 2012.
[19] A. Jarzębowicz and P. Weichbroth, "A systematic literature review on implementing non-functional requirements in agile software development: Issues and facilitating practices," in Lean and Agile Software Development: 5th International Conference, LASD 2021, Virtual Event, January 23, 2021, Proceedings 5, 2021, pp. 91–110.