**Engineering and Technology Journal e-ISSN: 2456-3358**

**Volume 10 Issue 04 April-2025, Page No.- 4424-4428**

**DOI: 10.47191/etj/v10i04.07, I.F. – 8.482**

**© 2025, ETJ**

# Digital Steganography and Cryptography Hybrid System Combining LSB and RSA Algorithms

**Khaled Balhaf[1], Nabil Ali Munassar[2], Alanood Ali Bagmeel[3], Madina Salem AL Hafeez[4], Fatima Mokhtar AL Gaafari[5], Adnan Swailem[6]**

[1,2]IT Department, Faculty of Engineering and Computing, University of Science and Technology & Aden, Yemen

[3,4,5,6]Department of Computer Science, Faculty of Applied and Health Sciences, Mahrah University of Science and Technology & Mahrah, Yemen

**ABSTRACT:** Given the significant increase in cyber threats, ensuring data security has become increasingly challenging in the digital era. To improve data confidentiality and integrity, this study proposes a hybrid security strategy that combines cryptographic encryption with data masking. The proposed solution adds a layer of security by integrating the Least Significant Bit (LSB) technique for data hiding with the RSA encryption algorithm, which ensures confidentiality. This combination notably reduces the risk of unauthorized access and decryption. Performance research illustrates the effectiveness of this method in protecting private information without affecting data storage and transmission. Throughout the experiment, the system has demonstrated its ability to withstand attacks.

**KEYWORDS:** Cybersecurity, Steganography, RSA algorithm, Hackers, Cryptography.

## I. INTRODUCTION

In the digital age, information security has emerged as a key concern. It is crucial to protect sensitive data's confidentiality and integrity while thwarting skilled hackers from accessing it. Steganography is the art of concealing; it is a method for encrypting digital media. To put it simply, confidentiality information must be protected by enclosing it in other information [3]. Although various media file formats such as GIF, JPG, and MP4 can be used, digital images are the most popular due to their widespread use on the Internet.

Comparably, the science of converting data into a secure format and protecting it is known as cryptography. Steganography, in contrast to cryptography, aims to keep people from even guessing the existence of the hidden information, not to stop them from knowing it [6]. Steganography and cryptography are two methods of concealing data that have different but similar uses. While cryptography uses encryption technologies to transform regular plaintext into encrypted, unintelligible text and vice versa, steganography prevents the detection of hidden signals. Steganography is typically used in conjunction with encryption. Steganography can also be used to disguise an encrypted file or communication, making the hidden message unintelligible even if the stego-image is decrypted. Therefore, steganography and cryptography working together can offer a strong basis for data protection [10].

Steganography and encryption have been employed for secret communication throughout history, albeit with more conventional methods like invisible ink. Nonetheless, the expansion of digital communications calls for the creation of safe digital techniques. Data is hidden via steganography in a "hidden medium." It is an effective tool that uses a variety of methods, including concealing information in audio, video, and photographs as well as hiding information from one image to another. Its contemporary uses have changed, leveraging advances in technology and artificial intelligence (the digital revolution) [5] [13]. A key principle of information security, confidentiality ensures that the content of the message is only accessible by the intended receiver. For sensitive communications, this is essential. Steganography is crucial for maintaining confidentiality because it covers the message's mere existence [5].

In this paper, we used a successful technique that combines the RSA (Rivest Shamir Adleman) and LSB (Least Significant Bit) algorithms in our unrelenting efforts to improve the security of sensitive data and shield it from growing threats. With several layers of security, this integration acts as an impenetrable fortress for secret data, making it very impossible for attackers to extract or even alter it. The background and related work are explained in part two of this study. Our methodology work is presented in section three, and our findings are then discussed. Finally, section five concludes and suggests future work.

## II. RELATED WORK

### *A. Cryptography RSA algorithm*

The history of encryption is extensive and goes all the way back to ancient civilizations. Simple substitution ciphers and transposition algorithms were used in early encryption methods. For instance, Julius Caesar communicated with his generals using a straightforward substitution cipher. Addition- ally, the field of encryption underwent a revolution in the 1970s with the advent of public-key cryptography. In this method, two keys are used: a private key for decryption and a public key for encryption. This eliminated the need to share a secret key and allowed for the safe flow of information.

The RSA algorithm is considered one of the most widely used algorithms in the field of data security, and its emergence is due to [11]. This technique encrypts documents in a variety of ways that make it challenging for hackers to access or decode them. Numerous academics have attempted to enhance this algorithm's functionality and boost its effectiveness, including [15] [1]. Steganography and encryption have been the subject of much research. On the other hand, encryption aims to render data unreadable without the right key. The key exchange authentication technique makes use of the RSA algorithm. Diffie-Hellman is the basis for the key exchange procedure. In order to create shared keys used for data encryption and decryption, participants first interact using the Diffie-Hellman method [7].

RSA has successfully solved the problems of asymmetric encryption. The RSA algorithm implements two different types of keys as keys (public/private) but is associated with a wide range of applications. As a result, they obtained more secure and reliable data transmission results [2] [9].

### *B. Steganography LSB algorithm*

Steganography and encryption have been the subject of much research. Steganography concentrates on hiding the data's presence, whereas encryption aims to render it unread- able without the right key. Enhancing the least significant bit (LSB) technique to boost capacity, imperceptibility, and robustness has occupied a large amount of steganographic research.

A popular technique for protecting items, such as communications and sensitive data, is steganography. As a result, numerous experiments have attempted to increase steganography's effectiveness. The embedding matrix variation (EMD) approach, for instance, was suggested by Zhang and Wang

[14] and is a significant improvement over the LSB method since it lessens image distortion while data is being hidden. and the Optimized EMD (Opt-EMD) approach was presented by K. Lin et al. This method optimizes the concealing capacity by analyzing the link between the number of items in a set

(n) and the quantity of data that may be hidden inside the image [8]. Also, in 2020 Serdar Solak [12] introduced a hybrid image-hiding technology combining Enhanced Modified Signed (EMSD) and Least Significant Bit (LSB) methods. This algorithm uses a set of adjacent pixels with less significant bits in the cover image to hide information.

Nonetheless, new developments in this ever-evolving sector, including image comparison, are still being created. Over the years, there have been notable developments in the fields of steganography and cryptography, and both areas are still undergoing research and development. As technology continues to advance, new problems arise that call for creative answers. In this study, we combine the RSA algorithm and LSB stealth technology to achieve good security.

## III.METHODOLOGY

We suggested combining encryption technology with data hiding in another data set in order to achieve the goal of the study and guarantee strong data protection. The following steps are typically included in the suggested methodology:

- Encryption of Data The recipient's public key is used to encrypt the data that needs to be hidden, employing the RSA technique. This ensures that only the holder of the corresponding private key can decrypt the data.
- Steganographic Embedding The LSB steganography technique embeds encrypted data within a digital image. A high-quality image is chosen as the carrier to minimize potential distortion caused by the embedding process. The least significant bits (LSBs) that need to be altered to maintain image integrity are carefully selected during this method. Figure 1 illustrates this.
- Retrieval of data The encrypted data is extracted from the image using the LSB steganography process in order to recover the hidden data. The original data can be retrieved by decrypting the extracted data with the recipient's private key. The recipient's concealed data is retrieved, as shown in Figure 2.

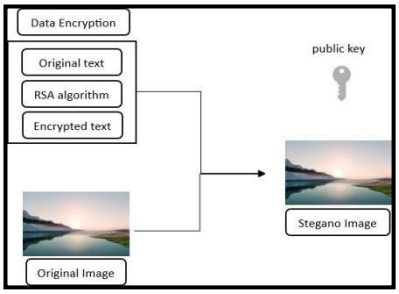



**Figure 1 Encryption and Steganography at sender**

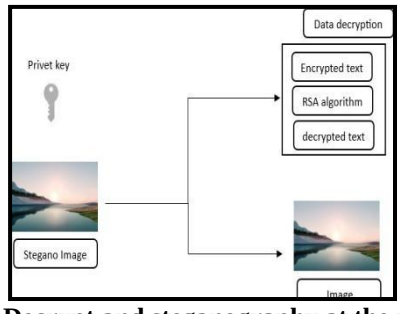



**Figure 2 Decrypt and steganography at the recipient**

Furthermore, Figure 3 illustrates our proposed system designed to accomplish the following objectives:

- Augmented Data Security: Implement dual layers of protection via encryption and steganography, thereby substantially complicating illegal access to the data.
- Preserved Image Quality: To make sure that the modifications are undetectable, use LSB steganography to reduce any negative effects on the carrier image's visual quality.
- Effective Transmission and Storage: By embedding concealed data into a digital image, you can enable the effective transmission and storage of that data.

To improve data security, this study combines the power of RSA encryption with the capacity to conceal information through the use of LSB stealth technology. It is anticipated to offer a practical way to safeguard private information in a range of applications. The system use case diagram is displayed in Figures 3 and 4.

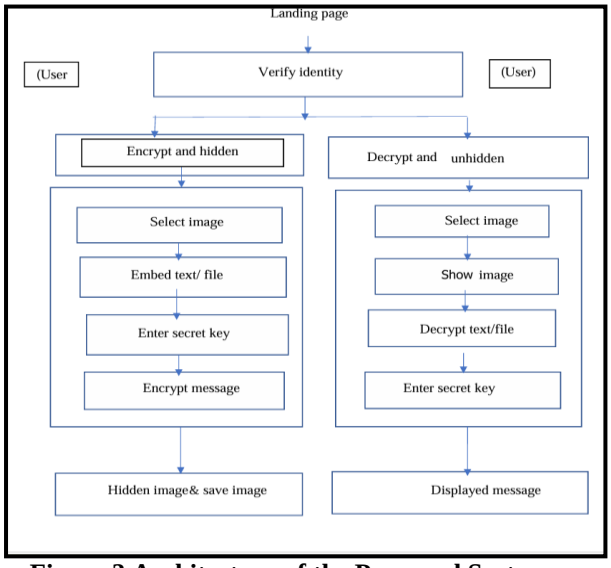



**Figure 3 Architecture of the Proposed System.**

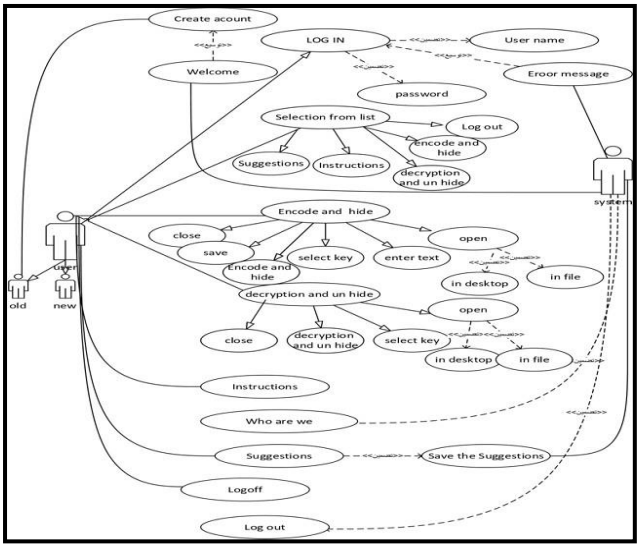



**Figure 4 Hybrid System Use Case Diagram**

## IV. RESULT AND DISCUSSION

The present study employed the RSA algorithm to encrypt text data, which was subsequently concealed within digital images using the LSB algorithm. The outcomes demonstrated that this method works well for reaching its objectives in terms of data security.

Text data that has been encrypted is very secure, thanks to the RSA method, which makes it difficult for unauthorized individuals to decrypt it. In other words, the letters were encrypted in a way that makes it challenging to decrypt them without the key. Stated otherwise, it is difficult to decrypt the letters without the key because they were encrypted. The LSB method not only conceals the data but also makes it possible for the encrypted data to be imperceptibly concealed inside digital images, making it challenging to identify the existence of hidden data. Thus, when we try to extract the text from the image, we will discover that it is encrypted, and not only is it hard to uncover the key, but it is also hard to determine whether or not the image contains concealed data. Using the following formulas, we evaluated several measures to determine whether a picture was affected by masking processes. These metrics included Mean Square Error (MSE), Signal-to-Noise Ratio (SNR), and Peak Signal-to-Noise Ratio (PSNR) [4]. Using the following equations.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(F_{ij} - G_{ij})^2$$

where M = Rows and N = columns**.**

$$SNR = 10log_{10}\frac{\sum_{i=1}^{n} W_i^2}{\sum_{i=1}^{n}(W_i - Q_i)^2}$$

Where W is the signal for the original image and Q a signal for the cover image.

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

The outcomes of our studies with the gray image when the English message was hidden are displayed in Table 1. Table 2 shows the results for the colour image. Table 3 shows the results for the colour image with Arabic text hidden. Our tests showed that, following masking, the effect on the image was invisible. The amount of the effect between the image before and after hiding is displayed in the 4th table. The experiments were executed on a laptop device:

- Hardware: Intel CPU core I5 with 8 GB RAM and memory bandwidth 14.40GB/s.
- Software: Windows 10 as an operating system, Microsoft Visual Studio 2015, C# programming.

**Table 1 Result (SNR, PSNR, AND MSE) For Grayscale Image With Different Text Sizes**

| IMAGES | IMG-SIZE | TXT-SIZE | SNR | PSNR | MSE |
|---|---|---|---|---|---|
| Image1 | 61.8 KB | 10 B | 44.72 | 72.78 | 0.034 |
| Image1 | 61.8 KB | 100 B | 41.79 | 69.85 | 0.0067 |
| Image1 | 61.8 KB | 6 KB | 37.93 | 65.98 | 0.0164 |

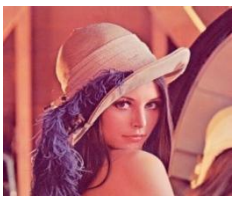
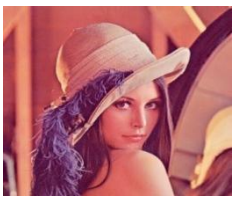
**Table 2 Result (SNR, PSNR, AND MSE) For Color Iimage With Different Text Sizes**

| IMAGES | IMG-SIZE | TXT-SIZE | SNR | PSNR | MSE |
|---|---|---|---|---|---|
| Image2 | 139 KB | 10 B | 22.43 | 54.99 | 0.206 |
| Image2 | 139 KB | 100 B | 19.75 | 52.32 | 0.34813 |
| Image2 | 139 KB | 12 KB | 16.11 | 48.67 | 0.8824 |

**Table 3 Result (SNR, PSNR, AND MSE) For Color Iimage With Different Arabic Text Sizes**

| IMAGES | IMG-SIZE | TXT-SIZE | SNR | PSNR | MSE |
|---|---|---|---|---|---|
| Image 3 | 88 KB | 10 B | 30.26 | 59.98 | 0.0653 |
| Image 3 | 88 KB | 200 B | 29.37 | 59.09 | 0.0802 |
| Image 3 | 88 KB | 5 KB | 26.8 | 57.83 | 0.0872 |

**Table 4 The Difference Between The Pictures Before And After Hiding**

| Images | BEFORE | AFTER |
|---|---|---|
| **Image 1** |  |  |
| **Image 2** |  |  |
| **Image 3** |  |  |

## V. CONCLUSIONS

Information security has become a major concern in the digital age. Ensuring the confidentiality and integrity of sensitive data while preventing skilled hackers from obtaining it is essential. Steganography, a technique for encrypting digital media, is the art of concealment. In other words, private information needs to be enclosed with other information to be protected.

To strengthen the security of sensitive data and protect it from ever-increasing threats, we employed a successful method in this study that combines the RSA (Rivest Shamir Adleman) and LSB (Least Significant Bit) algorithms. This integration serves as an impenetrable fortress for sensitive data, preventing attackers from extracting or even altering it, thanks to multiple security levels.

As a result, we can state that this activity has improved our safety and security. The effectiveness of the two algorithms was tested, and the findings demonstrated that they operate with high efficiency in terms of encryption, concealment, and retrieval time. Overall, it can be concluded that the encryption and concealment method employed in this study offers a secure and efficient means of encrypting text data and transferring it undetectably within digital photographs.

Information security has undergone a paradigm change with the combination of RSA and LSB approaches. We have created a novel approach that offers previously unheard-of levels of protection for sensitive data by fusing the advantages of steganography and encryption. In the future, we will extend the study to involve improving user privacy and giving consumers total control over their personal data.

## REFERENCES


1. Rim Ali Salah Al-Ardhi and Mohammed Fadhl Abdullah. Enhancing parallel implementation of rsa algorithm using openmp. Journal of Science and Technology, 29(2):52–56, 2024
2. A Al-Lehiebe. Ciphered text hiding in an image using rsa algorithm. J. Of College of Education for Women, 26(3), 2015.
3. Walter Bender, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. Techniques for data hiding. IBM systems journal, 35(3.4):313–336, 1996.
4. Xintao Duan, Kai Jia, Baoxia Li, Daidou Guo, En Zhang, and Chuan Qin. Reversible image steganography scheme based on a u-net structure. Ieee Access, 7:9314–9323, 2019.
5. Akande Adenike Folashade, Olubokola Adekola, Femi Temitope John- son, and Oladayo Joseph Elugbadebo. Hide-it: An enhance secure least significant bit image steganographic system using dual encryption techniques. 2024.
6. Mohammad Hashim et al. Hiding encryption text by dna using exploiting modification direction algorithm. AL-Rafidain Journal of Computer Sciences and Mathematics, 15(1):147–158, 2021.
7. JH Hong and CW Wu. Rsa public key crypto-processor core design and hierarchical system test using ieee 1149 family. National Tsing- Hua University, Taiwan, Doctoral dissertation, 2000.
8. Kai Yung Lin, Wien Hong, Jeanne Chen, Tung Shou Chen, and Wen Chin Chiang. Data hiding by exploiting modification direction technique using optimal pixel grouping. In 2010 2nd International

conference on education technology and computer, volume 3, pages V3– 121. IEEE, 2010.

9. Taleb Samad Obaid. Study a public key in rsa algorithm. European Journal of Engineering and Technology Research, 5(4):395–398, 2020.
10. Aditya Raj. Hiding secret data in audio, video, image, text steganography using least significant bit algorithm.
11. Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communica- tions of the ACM, 21(2):120–126, 1978.
12. Serdar Solak. High embedding capacity data hiding technique based on emsd and lsb substitution algorithms. IEEE Access, 8:166513–166524, 2020.
13. Murat Uzun and Serdar Solak. Advancing data privacy in color images through pixel-specific data hiding techniques. Computers and Electrical Engineering, 118:109442, 2024.
14. Xinpeng Zhang and Shuozhong Wang. Efficient steganographic embed- ding by exploiting modification direction. IEEE Communications letters, 10(11):781–783, 2006.
15. Xin Zhou and Xiaofei Tang. Research and implementation of rsa algorithm for encryption and decryption. In Proceedings of 2011 6th international forum on strategic technology, volume 2, pages 1118– 1121. IEEE, 2011.