IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 12, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012123 |

Combining Cryptography and Steganography for Data Hiding

Varad Ingale[1], Vasundhara Iyer[2], Varun Gujarathi[3], Varun Patil[4], Atharv Vanjari[5], Yogeshwari Rathod[6]

Department of Engineering Science and Humanities, Vishwakarma Institute of Technology, Pune, Maharashtra, India[1-6]

ABSTRACT:In this 21st Century, there is a need of high security of multimedia data. This secured system should provide confidentiality, authenticity, integrity, and non-repudiation in the network. The confidential details transferred through internet are hacked by phishing in an electronic communication world. So, Data Security is very much important. Cryptographic Algorithms are used extensively for information security. Steganography is used to hide their existence. Rivest-Shamir-Adleman (RSA) is an asymmetric cryptographic, highly secured algorithm. Since it is complex to compute, different methods are applied to increase the speed of an RSA algorithm. In this paper, a secrete text data is encrypted using RSA with modifications and then it is hidden in cover image using Least Significant bit.

KEYWORDS:Cryptography, Decryption, Encryption, LSB, RSA, Steganography

I. INTRODUCTION

The data communication through websites may include confidential data which might be obstructed. Also, there are many applications on the net and a lot of sites require users to fill forms that include confidential personal information like telephone numbers, addresses, and master card information. So, the users may have secret and secure transmissions for several reasons like protect their caution from hackers during it disregarded an open channel, that the confidentiality and data integrity are required to prevent unauthenticated access and use. Cryptography and steganography are the standard methods to protect transmissions. The standard methods for securing transmissions are cryptography and steganography. Cryptography and steganography are well-known and extensively used technologies for manipulating data to conceal personal information. Steganography, sometimes known as cover writing, is a means of converting a confidential method into a false communication. Cryptography or confidential matter can be a technique where a secret method is converted into ciphertext and sent to another one that then decrypts the ciphertext into plain text [2]; The information is hidden using the Steganography technique, which makes it impossible to view. We'll focus on expanding the method in this study, which uses both cryptography and Steganography to hide data. The goal of this study is to explain how to use image processing to combine cryptography with steganography. We offer a system that can conduct steganography and cryptography in a consistent amount of time. For data concealment, this study employs both encryption and steganography techniques. RSA is the most reliable and unique algorithm. In addition, it is the most well-known public-key execution approach. RSA is a symmetric key encryption technology that is often used to safeguard data where secrecy is a concern. It's an asymmetric cryptography algorithm, which means it employs both a public and a private key. A public key is disclosed openly, but a private secret is kept private and must not be shared with anybody.

II. RELATED WORK

[1] In this paper, AES algorithm is used for encryption of plain text and the key generated is used to decrypt the cipher text. For steganography traditional RDH algorithm is used to hide the cipher text into the cover image. The image for steganography is picked by the user. The Stego object generated will be transmitted through web. The user retrieves the cipher text from the stego object. Using the AES key, the cipher text is decrypted and the original text is obtained. In the extraction process the original message is extracted from the stego-image.

[2] The text file to be send to the receiver from a sender without disclosing it to others is first encrypted with modified RSA technique using public key. The encrypted text will be embedded in cover image randomly using pixel replacement technique based on the seed value generated. The resulting image is a stego image. This stego image is transmitted through network. At receiver it extracts the encrypted secrete text from the stego image. Then the encrypted text is decrypted using the private key.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012123 |

[3] In this paper both the hybrid cryptography and steganography has been applied, and a stego image has been generated. Here, the message is encrypted using AES. A hash value of the message is generated that is encrypted with the help of the public key of RSA to produce a digital signature. The digital signature received by the user is used to check if the message had been compromised. The cipher text is then embedded in an image using the LSB method of steganography.

[4] This method is involved with the method to secure the exchange of communication between two users. They are using the knowledge concealing technique which includes cowl image that is a secure way to hide the data. The sender first assigned the cryptography key on the image and then the knowledge concealing, a hidden key to further hide the data. Through this mechanism, the image is more secure because it uses two keys.

[5] In the proposed paper encryption is done by cryptography method to enhance the security level and a hybrid data compression algorithm increases the input data to be encrypted. For compressing the plain text Huffman coding algorithm has been used and cover image is compressed by Discrete wavelet transform DWT based that compacts the cover image through lossy compression to reduce the cover image dimensions. Then the encrypted data is compacted in the cover image.

III. METHODOLOGY

Algorithm

This system uses a mix of encryption and steganography algorithms. The RSA algorithm is used to generate keys, encrypt data, and decode data. The LSB (Least Significant Bit) technique was used in steganography to hide the encrypted data in the image, and the same process was used to extract the encrypted data from the stego image.

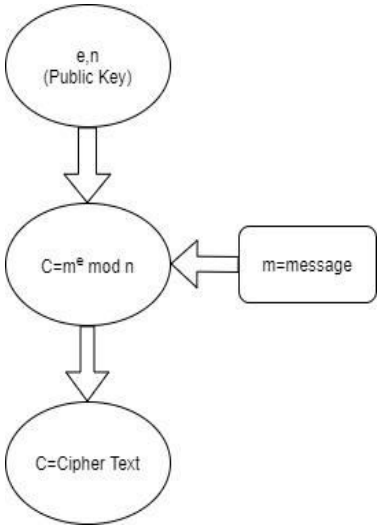


Fig. 1 Encryption process of RSA

To encrypt the message, Following are the steps:

1. The first step is to calculate (e;n) for public key generation
2. The second step is to accept the data in plain text format as input and encrypt the plain text using RSA to generate the cipher text as output.
3. The third stage accepts the output of the first stage as input and embeds it in the cover image using LSB so that the output is called stego image.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012123 |

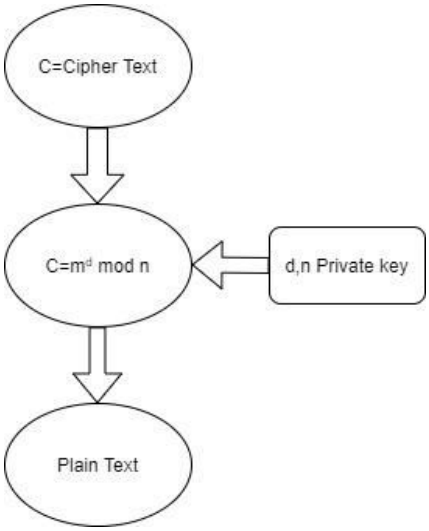


Fig. 2 Decryption process of RSA

To recover data from a Stego image, there are three steps:

1. The first step involves creating a private key such as an encryption key with the use of RSA key exchange.
2. The second step in retrieving the protected data is to extract the ciphertext from the stepper image.
3. The third step is to retrieve the secure data, that is, to decrypt the ciphertext text using the RSA algorithm.

Key Generation:
The keys of the RSA algorithm are generated as follows:
Step 1: Select two different random prime numbers p and q. Step 2: Calculate n = p q. n is used as a module for the private and public keys.
Step 3: Calculate f(n) = (p-1) (q-1). (f is the Euler total function).
Step 4: Choose an integer e such that 1 < e <f (p q), and gcd(e, f(n)) = 1
Step 5: Calculate d = e - 1 mode [f(n)]
Step 6: Publish the public encryption key: (e;n)
Step 7: Keep the secret private decryption key: (d; n) The keys for the RSA algorithm are generated in the following way:

LSB Algorithm:

LSB Algorithm LSB Steganography comprises of various methods like Text, Image, Audio and Video steganography but in this paper, we will focus on Image steganography.

Image Steganography Algorithm: - It is process in which Least Significant Bit of the pixel of cover image is replace with the Least Significant bits of the secret message.

For example: Suppose cover images has its first eight-pixel values as [01011010, 01100010, 10010011, 11000110, 11000101, 01010011, 00110110, 01100011]. Let‘s also assume the secret bits which we want to embed is 10110011, then immediately the secret bits are embedded through LSB algorithm, so now the pixel values changes for the image. That pixel values are: 01011011, 01100011, 10010010, 11000110, 11000100, 01010011, 00110110, 01100011. As you can notice that averagely half of the pixel are changed.

Encoding Algorithm:

• Take the path of cover image from the user.
• Secret message is taken as input by the user and then this secret message is converted into cipher text.
• Select cover image and hide the cipher text in image file using LSB algorithm.
• Finally Check the end of the message bit and stop the process

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012123 |

• Repeat till the whole message can be embedded in the image.

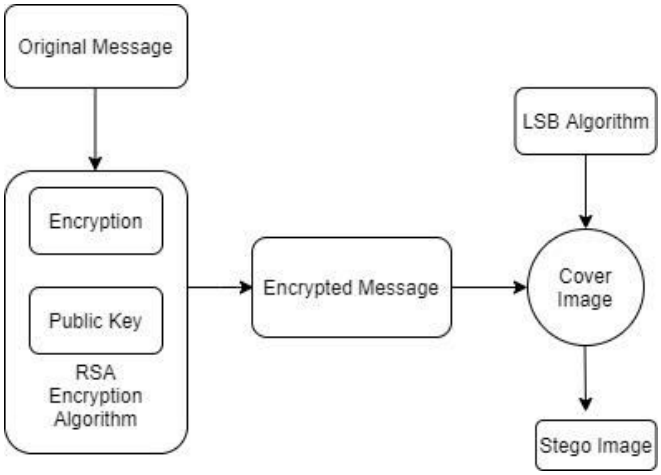


Fig. 3 Encryption process of system

Decoding Algorithm:

• Take the path of stego-image from the user.
• Extract the length of the hidden message by reading the LSB of each sample of image.
• Extract the cipher text by reading each sample.
• Convert ciphertext into hidden message.
• Display the hidden message.

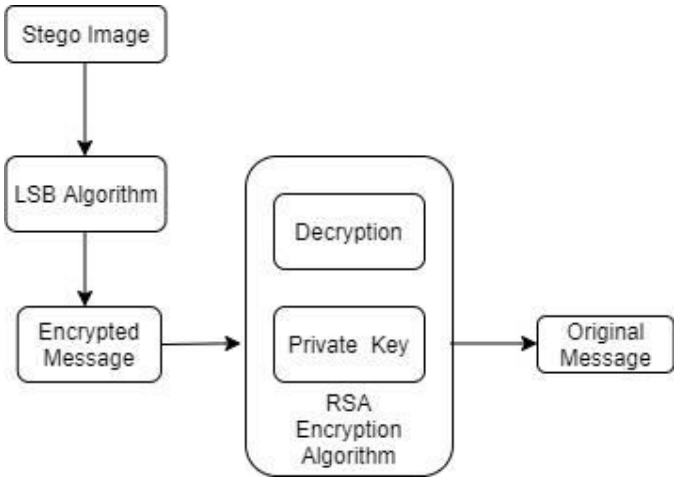


Fig. 4 Decryption process of the system

Performance Analysis

The ability of the proposed system to withstand statistical attacks and to also illustrate the robustness and security of the application are determined by calculating the PSNR.
The PSNR (Peak-Signal–to–Noise–Ratio) is the proportion of a signal's greatest potential strength to the power of the corrupting noise that influences the signal's representation. In steganographic applications, the PSNR is a parameter that is frequently used to measure, compute, and calibrate the quality of the stego picture. The signal in our system represents the actual image, while the noise represents the inaccuracy introduced by the steganographic techniques.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012123 |

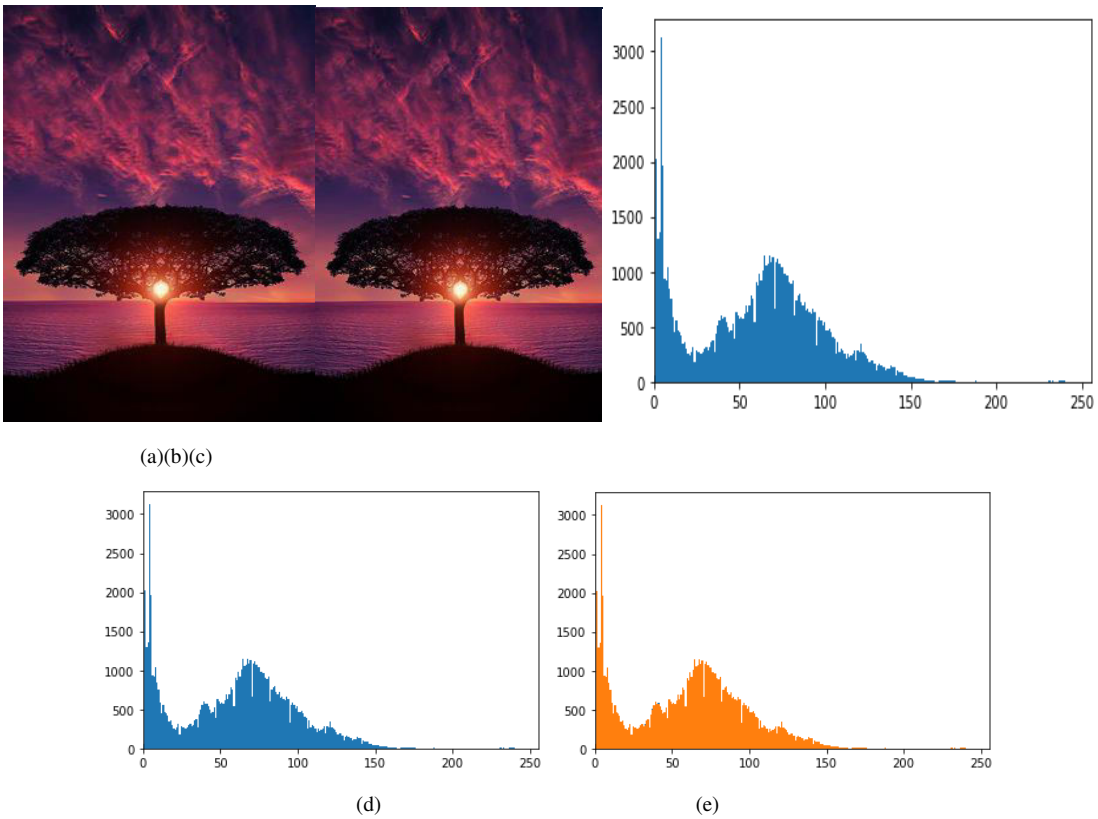
The Mean Square Error is frequently used to calculate the PSNR (MSE). The MSE is calculated using two M*N monochrome pictures I and K, one of which is a noisy approximation of the other. PSNR and MSE are calculated using the following scientific formulas:

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

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(O(i,j) - D(i,j))^2$$

IV. EXPERIMENTAL RESULTS

In the performance analysis of LSB, the technique to calculate PSNR and MSE values is to be executed on a cover image. The following figures show the cover image along with the stego image. The PSNR and MSE values have been calculated for the original and stego image and their comparison along with their histogram is shown in test cases below.



(a)(b)(c)

(d) (e)

Fig.5.Test 1 (a) Original cover image (b) Stego Image (c) Histogram of original image (d) Histogram of stego image (e) Comparison of histograms of images

The PSNR Value between original image Fig. 5. (a) and stego image Fig. 5. (b) is 62.25821290795001.
The MSE Value between original image Fig. 5. (a) and stego image Fig. 5. (b) is 0.038659752564779694.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 12, December 2021 ||

| DOI:10.15680/IJIRSET.2021.1012123 |

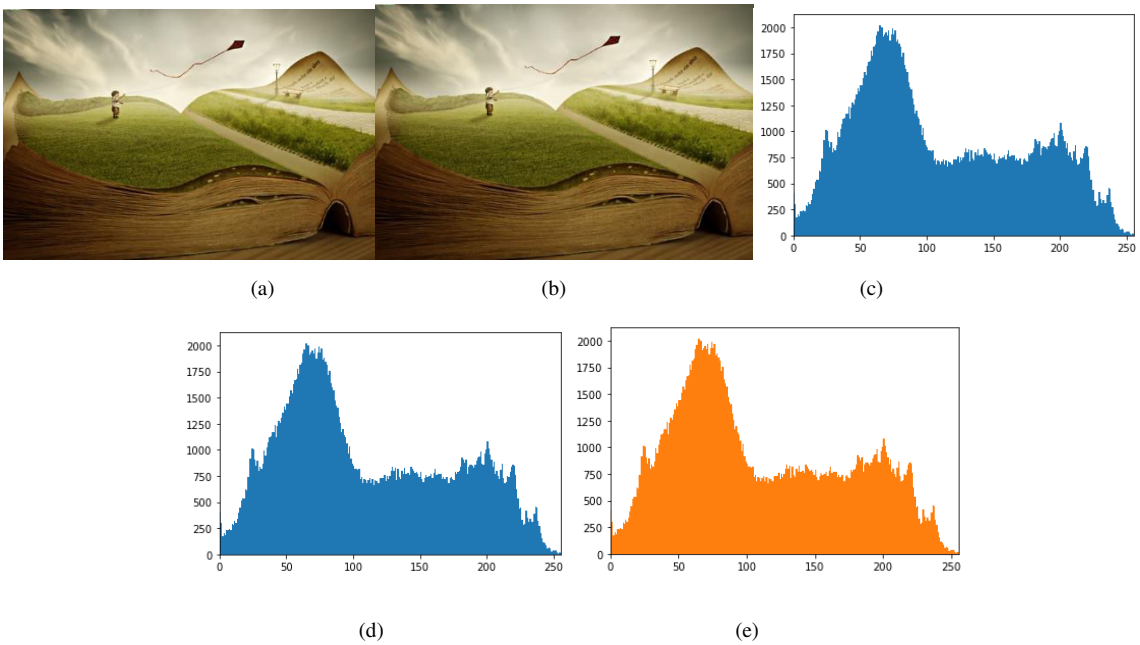


Fig.6.Test 2 (a) Original cover image (b) Stego Image (c) Histogram of original image (d) Histogram of stego image (e) Comparison of histograms of images

The PSNR Value between original image Fig. 6. (a) and stego image Fig. 6. (b)is 79.31131009773475.
The MSE Value between original image Fig. 6. (a) and stego image Fig. 6. (b) is 0.000761990138951143.

VI. CONCLUSION

To hide confidential information, cryptography and steganography can be effectively used. The steganographic method aims to hide information resistant to external attacks and should not reveal the secret information that the cover image is carrying. In this project, we have used LSB Algorithm as a Steganographic method. Along with the RSA algorithm, the over system becomes more secure.

REFERENCES

[1] N. Rashmi and K. Jyothi, "An improved method for reversible data hiding steganography combined with cryptography," 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 81-84, doi: 10.1109/ICISC.2018.8398946.
[2] M. Ganavi and S. Prabhudeva, "A Secure Data Transmission using Modified RSA and Random Pixel Replacement Steganography," 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), 2018, pp. 1-7, doi: 10.1109/ICCTCT.2018.8550848.
[3] C. Biswas, U. D. Gupta and M. M. Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography," 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 2019, pp. 1-5, doi: 10.1109/ECACE.2019.8679136.
[4] T. Naqash, A. Iqbal and S. H. Shah, "Review on Safe Reversible Image Data Hiding," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0929-0932, doi: 10.1109/CCWC.2019.8666536.
[5] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," in IEEE Access, vol. 9, pp. 31805-31815, 2021, doi: 10.1109/ACCESS.2021.3060317.
[6] Richard Apau and Clement Adomako. Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones. *International Journal of Computer Applications* 164(1):13-22, April 2017.
[7] Ms.Shridevishetti, Mrs.Anuja S, 2015, A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ICESMART – 2015 (Volume 3 – Issue 19)
[8] Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh, "Steganography in images using lsb technique", Volume 5 Issue 1 - January 2015

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details