IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11365

Securing Data Using Cryptography and LSB Image Steganography

Akshay Wagh[1], Prathamesh Tayade[2], Saurabh Wani[3], Shashwat Singh[4]

U.G. Student, Department of Computer Engineering, SSBT's College of Engineering and Technology, Bambhori, Jalgaon, India[1-4]

Abstract: Data Security is a challenging issue of data communications today that touches many areas including secure communication channels, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/ decryption methods to enhance data security. This paper describes a new method of encrypting original data parts with different strong cryptographic encryption algorithms and LSB Image Steganography to hide the decryption keys in an image. This encryption technique enhances the complexity in encryption algorithm at large extent. This paper becomes very special in few aspects, all of them are explained in a detailed way in the chapters.

Keywords: Cryptographic, Data Security, Decryption, Decryption Keys, Encryption, Information Technology, LSB Image Steganography

I. INTRODUCTION

The paper is so well organized as follows starting with and navigates in the order:

- Introduction
- Proposed methodology
- Cryptography and Steganography
- Results
- Conclusion
- Future Work

Digital communication witnesses a noticeable and continuous development in many applications in the Internet. Hence, secure communication sessions must be provided. The security of data transmitted across a global network has turned into a key factor on the network performance measures. So, the confidentiality and the integrity of data are needed to prevent eavesdroppers from accessing and using transmitted data. Steganography and Cryptography are two important techniques that are used to provide data security. Cryptography is the science of devising methods that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient. The aim is to develop a new approach to encrypting a message with multiple encryption methods and hiding required keys in an image, by taking advantage of combining cryptography and steganography.

II. PROPOSED METHODOLOGY

Here first the encryption part is discussed and the decryption is paid attention then.

A. *Encryption*

Step 1: Splitting the message into multiple parts and these files are then given as input to algorithm.

Step 2: Encrypting each split files by different algorithms which are selected randomly from list of encryption algorithms.

Step 3: The required keys (Encryption/Decryption keys) are then hided inside image Using LSB Image Steganography.

Step 4: The encrypted files and steganographic image are then zipped and sent as output.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11365

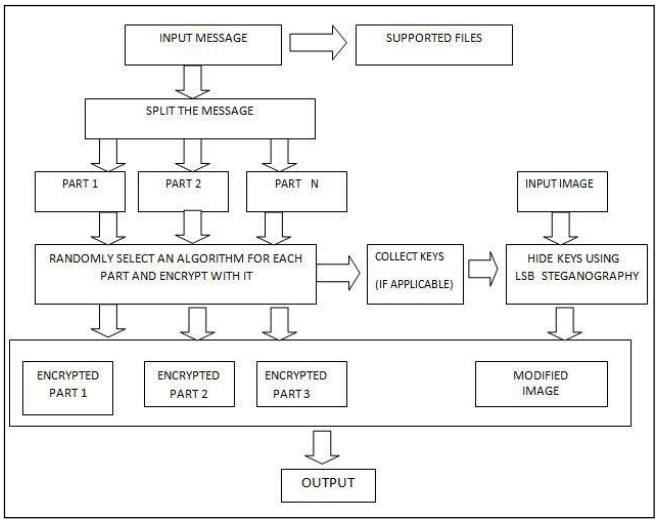


Fig.1 Encryption System

B. Decryption

Step 1: After extraction of zip file the (decryption) keys retrieved from steganographic image.

Step 2: All encrypted files decrypted using retrieved keys from Image.

Step 3: After generation of decrypted files, all encrypted files and Steganographic image deleted.

Step4 : Decrypted files merged together in proper sequence to get original file(message) as output.

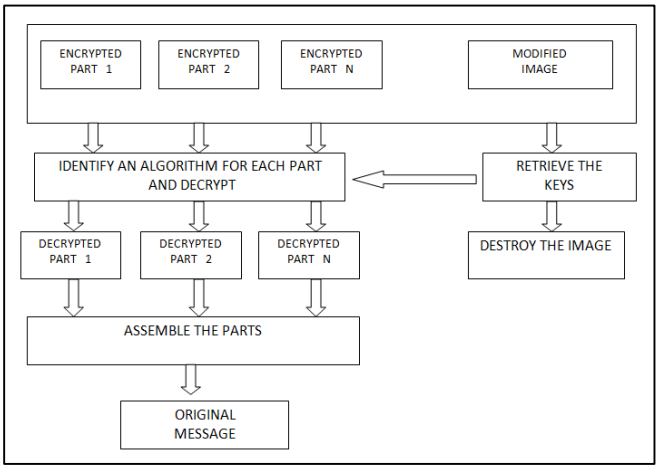


Fig.2 Decryption System

C. LSB Steganography

1) *Encoding*:

Step 1: Convert the message to its binary format.

Step 2: Select a starting point randomly within the pixel matrix of image from which encoding of message will be done.

Step 3: Randomly select the pixel values (TRGB in case of PNG images).

Step 4: Traverse through each pixel of the image and do the following:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11365

a. Convert the pixel value to binary

b. Get the bit of the message to be embedded one by one

c. Create a variable temp If the message bit and the LSB of the pixel are same, set temp = 0

d. If the message bit and the LSB of the pixel are different, set temp = 1

e. This setting of temp can be done by taking XOR of message bit and the LSB of the pixel.

f. Update the pixel of output image to input image pixel value + temp Keep updating the output image till all the bits in the message are embedded Finally, write output image to local system.

Step 5: Return RSA encrypted Start Point and randomly selected pixel.

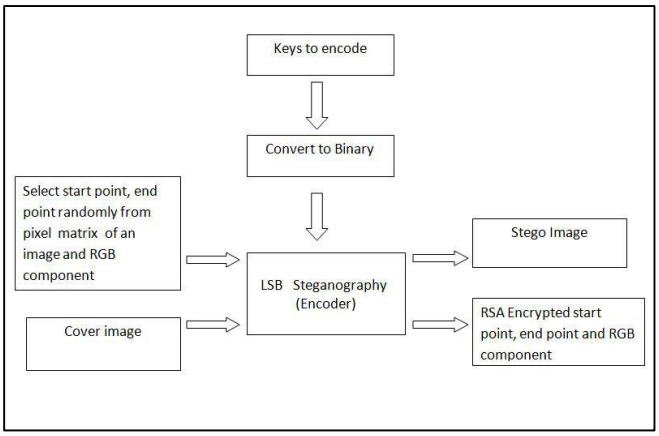


Fig.3 LSB Steganography – Encoder

2) *Decoding*:

Step 1: Decrypt Start point and pixel value from which decoding will start

Step 2: Traverse through each pixel of the image and do the following:

a. Get the last bit of selected pixel value and add to the Binary String

b. Repeat (a) till end point

Step 3: Group the bits of binary string as per the key size of given algorithms

Step 4: Make group of 8 bits within grouped string and convert into characters.

Step 5: Return Keys

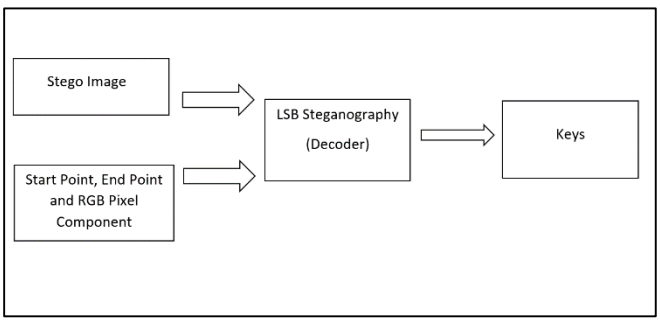


Fig.4 LSB Steganography – Decoder

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11365

III. CRYPTOGRAPHY AND STEGANOGRAPHY

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. This method is the art of secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext can be decrypted to the original plaintext. Without the knowledge of the key, nobody can retrieve the plaintext. Cryptography plays an essential role in many factors required for secure communication across an insecure channel, like: confidentiality, privacy, non-repudiation, key exchange, and authentication. Figure 1 shows the cryptography system [10]. There are two types of cryptographic schemes for securing the data. These schemes are often used to reach the objective: public-key cryptography, secret key cryptography, and hash functions. The length and type of the keys used depend on the type of encryption algorithm [10].

A. *Symmetric / Secret Key Cryptography*

The technique of Secret key encryption can also be known as the symmetric-key, shared key, single-key, and eventually private-key encryption. The technique of private key uses for all sides encryption and decryption secret data. The original information or plaintext is encrypted with a key by the sender side also the similarly key is used by the receiver to decrypt a message to obtain the plaintext. the key will be known only by a people who are authorized to the encryption/decryption.[12]

However, the technique affords the good security for transmission but there is a difficulty with the distribution of the key. if one stole or explore the key he can get whole data without any difficulty. An example of Symmetric-Key is DES Algorithm [12].

B. *Asymmetric / Public Key Cryptography*

We can call this technique as asymmetric cryptosystem or public key cryptosystem, this technique use two keys which are mathematically associated, use separately for encrypting and decrypting the information.

In this technique, when we use the private key, there are no possibilities to obtain the data or simply discover the other key. all keys are needed for the technique to run. The key used for encryption is stored public therefore it's called public key, and the decryption key is stored secret and called private key. an example of Asymmetric-Key Algorithms is RSA [10].

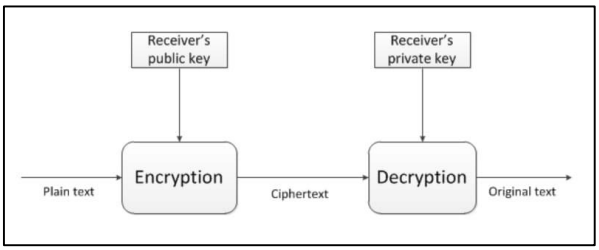


Fig.5 Asymmetric Key Cryptography

C. *Steganography*

Steganography can be defined as the science of hiding and communicating data through apparently reliable carriers in attempt to hide the existence of the data. So, there is no knowledge of the existence of the message in the first place. If a person views the cover which the information is hidden inside of he or she will have no clue that there is any covering data, in this way the individual won't endeavour to decode the data. Figure 2 shows the steganography system overview [10]. The secret information can be inserted into the cover media by the stego system encoder with using certain algorithm. A secret message can be plaintext, an image, ciphertext , or anything which can be represented in form of a bitstream. after the secret date is embedded in the cover object, the cover object will be called as a stego object also the stego object sends to the receiver by selecting the suitable channel, where decoder system is used with the same stego method for obtaining original information as the sender would like to transfer [10]. There are various types of steganography.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11365

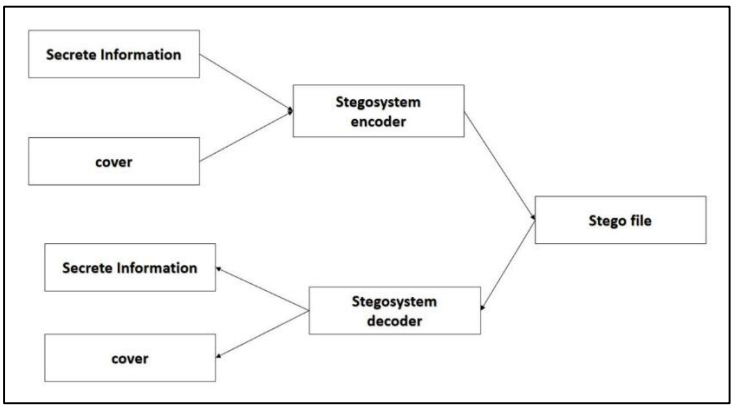
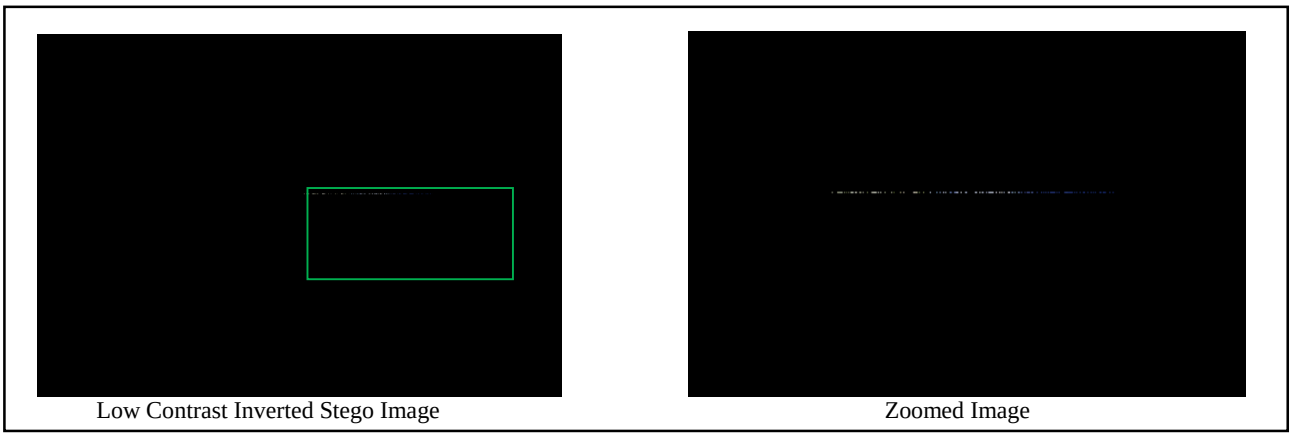


Fig.6 Steganography System

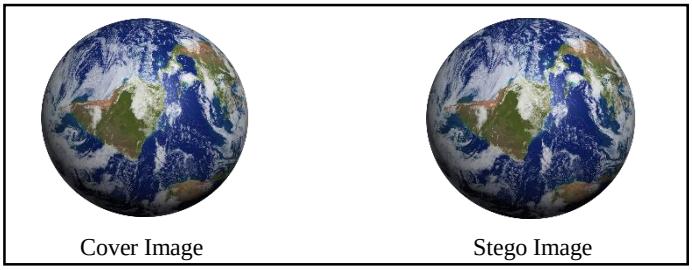
After converting the stego image into low contrast image in order to see the changed pixel values. It can be seen that the white dots show the modified pixels. this embedding starts from anywhere in the middle which makes it difficult for attackers to retrieve the keys.



Low Contrast Inverted Stego Image Zoomed Image

Fig.7 Modified Pixels in Stego Image

Cover image is used to store data and stego image is formed, even though there is message hidden in the stego image the difference between the two in unnoticeable.



Cover Image Stego Image

Fig.8 Cover Image vs. Stego Image

IV. RESULT AND ANALYSIS

After testing the system against some test cases, Results are shown below.

A. *Individual Algorithm Analysis:*

Selected encryption algorithms are evaluated against different file sizes and time taken is measured. Here, by using the algorithms RSA , DES and their time taken is computed and stated in the table below.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11365

The Average Encryption and Decryption time for 1KB file using RSA algorithm and encryption keys of size 128,196 and 256 bits is calculated by taking multiple samples is shown in table below.

Table I Average Encryption and Decryption Time for 1KB file using RSA

1 KB RSA ENCRYPTION + WRITING OVERHEAD			
	128	196	256
Average Time Required (in Seconds)	0.5480889797210693	0.6240232467651368	1.9380087852478027
RSA DECRYPTION + WRITING OVERHEAD			
	128	196	256
Average Time Required (in Seconds)	0.3266880512237549	0.636298656463623	1.0739824771881104

The Average Encryption and Decryption time for 10KB file using RSA algorithm and encryption keys of size 128,196 and 256 bits is calculated by taking multiple samples is shown in table below.

Table II Average Encryption and Decryption Time for 10KB file using RSA

10 KB RSA ENCRYPTION + WRITING OVERHEAD			
	128	196	256
Average Time Required (in Seconds)	5.600250244140625	9.626661586761475	23.01663222312927
RSA DECRYPTION + WRITING OVERHEAD			
	128	196	256
Average Time Required (in Seconds)	3.2889068126678467	6.569077253341675	16.20619034767151

The Average Encryption Time using DES algorithm for files of size 1KB, 10KB, 50KB, 100KB is calculated by considering multiple samples is shown in table below.

Table III Encryption Time For DES

DES ENCRYPTION	Average Time Required (in Seconds)
1 KB	0.21594715118408203
10 KB	2.0925791263580322
50 KB	10.705688238143921
100 KB	21.727703523635864

The Average Decryption Time using DES algorithm for files of size 1KB, 10KB, 50KB, 100KB is calculated by considering multiple samples is shown in table below.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11365

Table IV Decryption Time For DES

DES DECRYPTION	Average Time Required (in Seconds)
1 KB	0.3016495704650879
10 KB	3.039182424545288
50 KB	17.62427854537964
100 KB	52.01072859764099

B. *System Results:*

1) System Performance Evaluation:

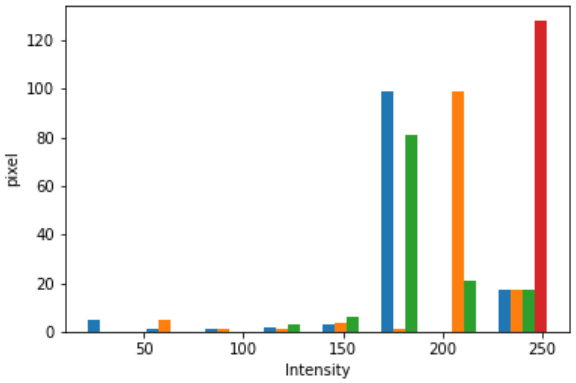
Here Complete system is tested against different sized files and and result are stated below.

Table V Encryption and Decryption Time for Proposed System

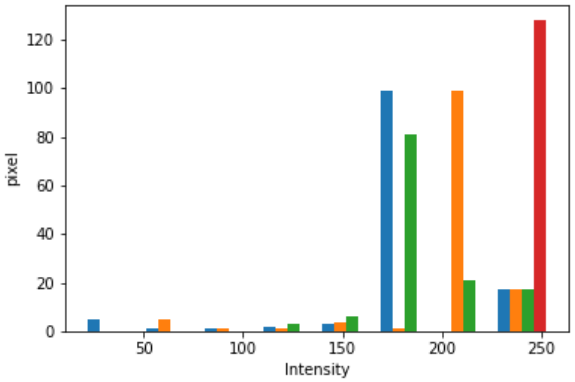
Proposed System Time key size 128 bits		
File Size	Encryption Time Required (in Seconds)	Decryption Time Required (in Seconds)
1 KB	1.9102466106414795	0.3911890983581543
10 KB	7.5593485832214355	5.201308012008667
50 KB	16.681638956069946	16.095878839492798
100 KB	34.6966769695282	31.173506259918213

2) LSB Steganography:

Here is the histogram of pixel values of cover image and stego Image of pixels, which will be changed after performing encoding.



Cover Image RGB Component Histogram



Stego Image RGB Component Histogram

Fig.9 RGB Component Histogram of Cover and Stego Image

V. CONCLUSION

After analysing the result, it is found that

1. RSA and DES combined gives great amount of security considering the time complexity.
2. Combination of cryptography and steganography provides more security compared to traditional approaches.
3. Change in cover image after performing LSB steganography is very negligible and cannot be identified without performing extreme analysis.
4. The randomness while selecting the encoding start point and pixel component, makes it difficult to detect the message inside the image.
5. This study proposes a new security approach that messages cannot be retrieved easily from the image by any intruder or hackers in the communication process.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11365

VI. FUTURE WORK

The future enhancement of this study is to incorporate different steganography (audio and video steganography along with image steganography) to enable it to support most of the file types (for encryption). By incorporating different encryption algorithms will make this encryption method more secure. Improvisation in key management will cause this system more robust another future enhancement will be to optimize the time complexity and to optimize space complexity to avoid excess memory usage.

REFERENCES

[1] M. H. Rajyaguru, "Crystography-combination of cryptography and steganography with rapidly changing keys," International Journal of Emerging Technology and Advanced Engineering, ISSN, pp. 2250–2459, 2012.
[2] D. Seth, L. Ramanathan, and A. Pandey, "Security enhancement: Combining cryptography and steganography," International Journal of Computer Applications (0975–8887) Volume, 2010.
[3] P. R. Ekatpure and R. N. Benkar, "A comparative study of steganography & cryptography," 2013.
[4] J. V. Karthik and B. V. Reddy, "Authentication of secret information in image stenography," International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58, 2014.
[5] M. K. I. Rahmani and N. P. Kamiya Arora, "A crypto-steganography: A survey," International Journal of Advanced Computer Science and Application, vol. 5, pp. 149–154, 2014.
[6] H. Abdulzahra, R. AHMAD, and N. M. NOOR, "Combining cryptography and steganography for data hiding in images," ACACOS, Applied Computational Science, pp. 978–960, 2014.
[7] C. P. Shukla, R. S. Chadha, and A. Kumar, "Enhance security in steganography with cryptography," 2014.
[8] M. K. I. Rahmani and M. A. K. G. M. Mudgal, "Study of cryptography and steganography system," 2015.
[9] P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz, "An improved level of security for dna steganography using hyperelliptic curve cryptography," Wireless Personal Communications, pp. 1–22, 2016.
[10] P. Kumar and V. K. Sharma, "Information security based on steganography & cryptography techniques: A review," International Journal, vol. 4, no. 10, 2014.
[11] Al-Shaaby, Ahmed & Al-Kharobi, Talal. (2017). Cryptography and Steganography: New Approach. Transactions on Networks and Communications. 5. 10.14738/tnc.56.3914.
[12] H. Sharma, K. K. Sharma, and S. Chauhan, "Steganography techniques using cryptography-a review paper," 2014.
[13] A. Dhamija and V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015, pp. 346–351.
[14] J. K. Saini and H. K. Verma, "A hybrid approach for image security by combining encryption and steganography," in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. IEEE, 2013, pp. 607–611.
[15] N. Khan and K. S. Gorde, "Data security by video steganography and cryptography techniques," 2015.