International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Secured Data Transmission Through Encrypted Images using Lossy Compression

S. Saradhapreethi (Author)
Dept. of Information Technology
KCG College of Technology
Chennai, Tamil Nadu, India

S. A. Sree Varsha (Author)
Dept. of Information Technology
KCG College of Technology
Chennai, Tamil Nadu, India

S. Subbulakshmi (Guide)
Assistant Professor
Dept. of Information Technology
KCG College of Technology
Chennai, Tamil Nadu, India

***Abstract*-- Image processing is a process of converting an image into a digital form where some operations are performed, in order to get an enhanced image or to extract some useful information from it. The aim of this paper is to overcome the limitation of adding limited additional data in an encrypted image. In the existing system, the encrypted image is compressed to least significant bits using data hiding key. As only LSB is compressed, only a sparse amount of space is created for accommodating additional data in which only limited amount of data can be added. Hence in order to add large amount of data, the amount of compression should be expanded so that large amount of space can be created. In this paper, we propose to use Lossy compression technique. As Lossy compression compresses large amount of data, a large amount of space can be created, which increases the capacity of adding the additional secret data. Also, this paper proposes to provide security to the file and keys separately through various methods.**

***Keywords*-- Image encryption, Lossy compression, Data hiding.**

I. INTRODUCTION

Over the past years, secret communication was done by the methods of cryptography. The disadvantage of these methods is that the pattern in which the data has been encrypted can easily be identified and hence this method provides a less or no security. In order to overcome this limitation, steganography was introduced. In recent times, the area steganography for secret communication plays an important role in wide areas. The objective of steganography technique is to hide a message into cover objects like images. Steganography method provides more security as compared to cryptography. As data hacking methods are developed each day, the security for these secret communications is being diminished. As a result only a limited amount of data can be sent securely to the destination. In this paper, more securityalgorithms are included. Hence, a large quantity of data can be hidden in the image, which overcomes the existing limitation.

II. EXISTING SYSTEM

The existing system uses both the methods of steganography and cryptography. Here the sender encrypts both the image and the data (which is to be sent) separately using AES algorithm. After encryption, 2 keys are generated, one for the image and the other for the data. The encrypted image is compressed using LSB technique. The encrypted data is then embedded into the compressed encrypted image which generates the 3rd key known as the "data-hiding key". Sender sends the file and the keys through mail system. Receiver can perform operations as per the respective keys present with him. If the receiver has data-hiding key and data key, then he will be able to decrypt only the data. Likewise if he has data-hiding key and image key, then he will be able to decrypt only the image. If receiver has all 3 keys then he will be able to decrypt both the image and the data.

III.PROBLEM DEFINITION

In the existing system, as only LSB is being compressed, only a sparse amount of space is created for accommodating additional data.Hence this method supports only for adding limited amount of additional data. In order to send large amount of data, a new system has to be developed.Another problem in the existing system is that, as both the steganographed file and credentials (keys) are being sent through the mail system. As hackers are increased day by day, it is easy for them to hack both the data files and hence secret details can be decrypted easily.

IV. PROPOSED SCHEME

In the proposed system, the data will be hidden in the image and is then sent to the destination. Here, unlike previous work, the entire image is compressed using Lossy compression technique. By this compression method a large amount of space will be created which can accommodate a large amount of data. After compression, the image is encrypted using AES technique with user-defined key for security. The same key is used for decryption. The data which has to be sent is also encrypted for more security purpose using AES technique where another user defined key is specified and this key is used for decrypting the data. This encrypted data is then embedded into the compressed encrypted image. During the embedding process, the sender will assign a separate data-hiding key which will be used for decryption at the receiver

end. The newly generated file is assigned with extension ".jpg". After the completion of the process, the sender sends the file to the receiver through IP address system and keys are sent privately using mail system. Hence, security is provided to the files and keys as both are sent through various methods to the receiver..

At the receiver end, the receiver will receive an encrypted image with hidden encrypted data. If the receiver has data-hiding and data decryption keys, then he can extract only the original secret data but he does not know the image content. Likewise, if the receiver has data-hiding key and the image decryption key, then he can extract an image similar to the original one but he cannot get the original secret data. If the receiver has all 3 keys i.e., the data-hiding key, image decryption key and the data decryption key, then he can extract both the original secret data and the image content similar to the original one. The maximum number of chances given to the receiver to decrypt the files is limited to three. If the receiver fails to decrypt any file within three chances, then the system will go into a non-responding state for few minutes. By the time a notification mail including the details of IP address, clock timing (failure time) is send to the admin regarding the failure at the receiver side. The admin will forward this mail to the sender and wait for the sender reply. The system admin have all authority like blocking and unblocking users. If the sender sends a favorable reply to the admin, then the system will restart and the receiver has to perform actions from the beginning.

V. WORKING OF PROPOSED SYSTEM

1. Registration

For the first time, the user will have to register for the system. The admin will provide the authority to the new user with the password. The user must login to perform any operation. The record of login session will be stored and maintained by the admin.

2. Image Compression

The user will input an image into the system or browse from the computer. The selected image is checked for its size and is then compressed using Lossy compression technique. The image is compressed at the ratio of 10:1.

3. Image Encryption

The compressed image is encrypted using AES algorithm where a key known as the "image decryption key" is defined by the sender which is used for decrypting the image at the receiver side.

4. Data Encryption

The user will input the required amount of secret data that he wants to send and is encrypted using AES algorithm where a key known as "data decryption key" is defined which is used for decrypting the data at the receiver end.

5. Data Embedding

The sender will embed/hide the encrypted data in the encrypted compressed image and assigns a data-hiding key which will be used for decryption at the receiver side. The generated file will be assigned with ".jpg" extensions.

6. File Sending

The sender will send the file with ".jpg" extension through IP address system and the credentials (keys) are sent privately through existing mail system.

7. Data Decryption

If the receiver has data-hiding and data decryption keys then he will be able to decrypt the data but not the image. After the decryption of data he will get the original secret message.

8. Image Decryption

At receiver end, if the user has data-hiding key and image decryption key then he will beable to decrypt only the image not the original secret data. The decrypted image will be similar to the original image.

9. Both Operations

If the receiver has all the 3 keys then he can perform all the operation like "Data decryption and extraction", "Image decryption".

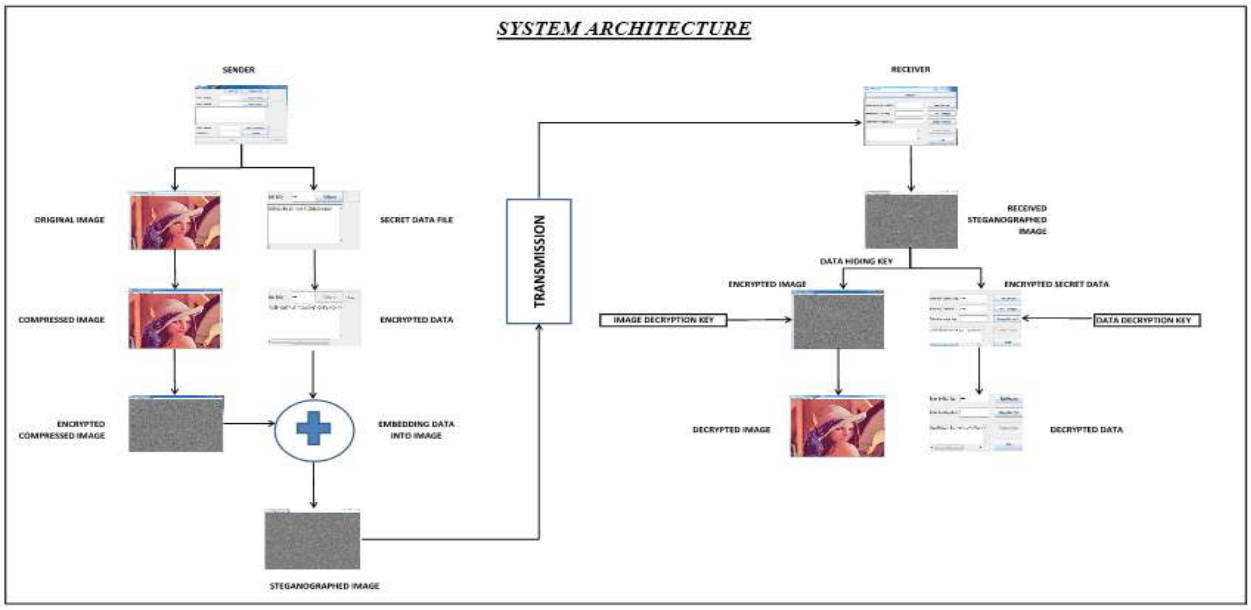


Figure: Work Flow Diagram- Sender Side

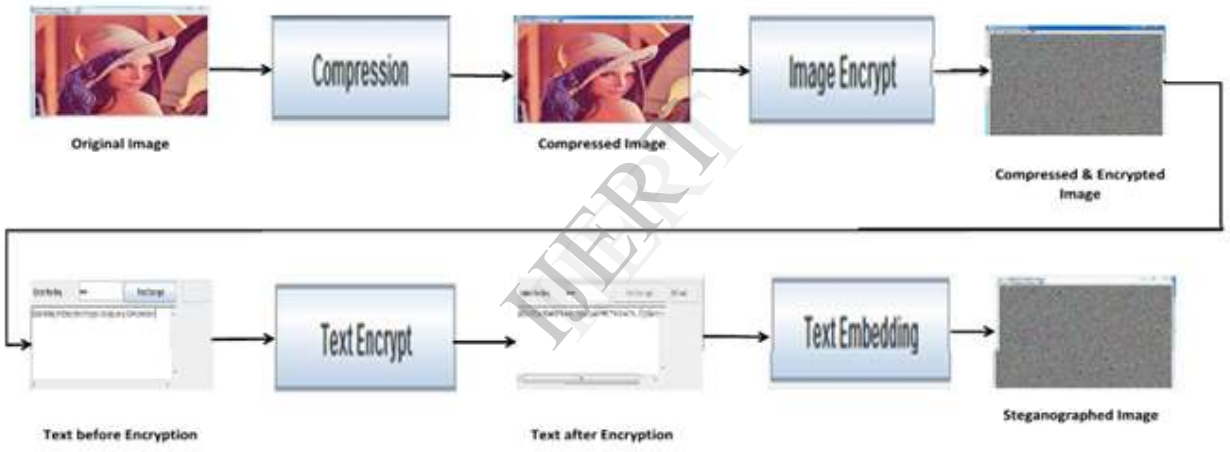
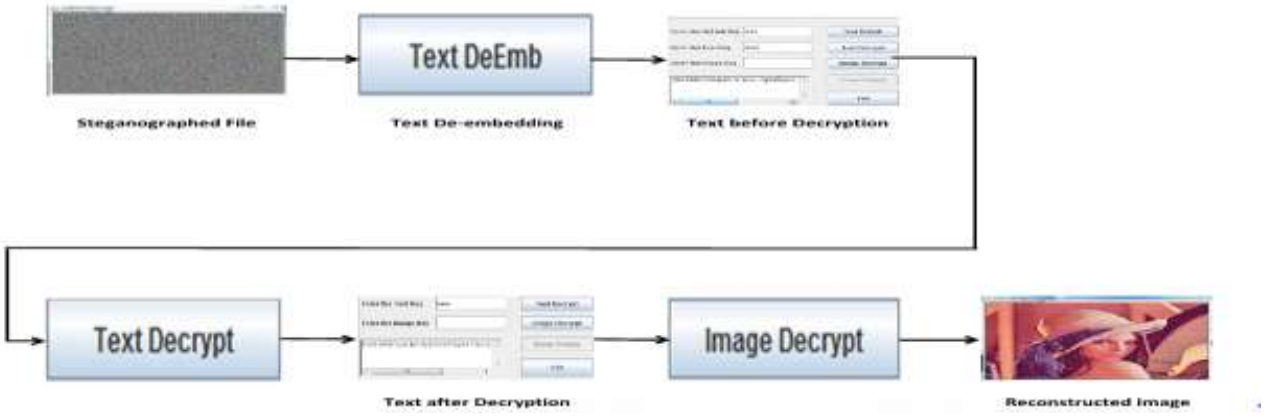


Figure: Work Flow Diagram-Receiver Side



VI. IMPLEMENTATION OF SYSTEM

1. Image Compression

In order to embed data into the image, we need some space. In order to create that space, the image is compressed using Lossy compression. In this method, samples of picture are taken, chopped into small segments, transformed into a new basis space, and quantized. The resulting quantized values are then entropy coded. This method compresses the image at the ratio of 10:1 which creates large space to

accommodate the required additional data. The following describes the steps followed during compression.

i) Quantization: This is the process of reducing information. In simpler terms, quantization is a method for optimally reducing a large number scale into a smaller one, and the transform-domain is a convenient representation of the image because the high-frequency coefficients, which contribute less to the over picture than other coefficients, are characteristically small-values with high compressibility. The quantized coefficients are then sequenced and losslessly packed into the output bitstream.

ii) Entropy encoding: Bit plane coding is used, the most significant bit plane is coded first. It involves arranging the image components in a "zigzag" order employing run-length encoding (RLE) algorithm that groups similar frequencies together, inserting length coding zeros, and then using Huffman coding on what is left.

2. Image & Data Encryption
The encryption technique proposed in this paper is AES algorithm. The AES algorithm operates on a 4x4 column-major order matrix which is known as "the state". The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, calledthe cipher key.

The main loop of AES technique performs the following functions:
1. SubBytes ( )
2. ShiftRows ( )
3. MixColumns( )
4. AddRoundKey( )

The AES algorithm is implemented as follows:
i) Key Expansion Round keys are derived from the cipher key using Rijndael's key schedule.

ii) Initial Round
AddRoundKey: each byte of the state is combined with the round key using bitwise XOR.

iii) Rounds
a. SubBytes: a non-linear substitution step where each byte is replaced with another according to a lookup table.

b. ShiftRows: a transposition step where each row of the state is shifted cyclically a certain number of steps.

c. MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.

d. AddRoundKey

iv) Final Round (no Mix Columns)
a. SubBytes
b. ShiftRows
c. AddRoundKey

3. Data Embedding
After the compression of image, the data and image is encrypted using AES algorithm. The compressed pixel of the image creates a large space to accommodate the additional data. The encrypted data will be embedded in the encrypted compressed image. The data is embedded into the space created by the compressed pixels of the image. After embedding the generated file is assigned with extension ".jpg".

4. De-embedding process
At the receiver end, the user will download the steganographed file with extension '.jpg'. Then the encrypted data is extracted from encrypted image using data-hiding key.

5. Image and Data Decryption
At the receiver end, the extracted encrypted data is decrypted using data decryption key. Similarly, the encrypted image is then decrypted using image decryption key. After this process, the image similar to the original image can be viewed.

VII. FEATURES

1. Addition of large data: As the entire image is compressed by Lossy compression, a large amount of space is created. Hence large amount of data can be hidden in the image.

2. Three keys for higher security: As individual keys are present for encryptions and embedding, the level of security of data is increased thus preventing the attacks on data during the transmission and these keys are sent privately to the receiver.

3. Protection of data at the receiver end: At the receiver end, the user is given three chances to perform any operation. If he fails i.e., if he enters a wrong key three times, then the system will go into a non-responding state for few minutes. Meanwhile, notification will be sent to the admin from receiver's mail.

4. Admin as main: The admin has all the authority to block or unblock users at any time if he feels something wrong. The admin maintains a database which contains the records of all the users and their activities.

VIII. PERFORMANCE MEASURES

Table-1. Compression Ratio

Size of Original Image(Bytes)	Size of compressed image (Bytes)	Size of Reconstructed image (Bytes)
69214	24246	32672
561276	61219	82228
777835	68748	91950
1516159	324708	440088
780831	95579	129983

Graph-1: Comparison of sizes between Original Image, Compressed Image & Reconstructed Image

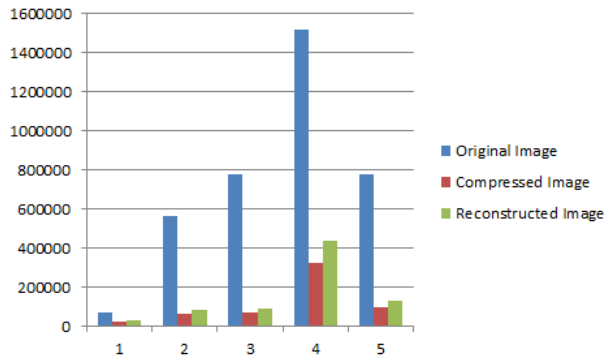


Table-2.Execution Time of Encryption of Image

File Size (Bytes)	Encryption Time
24246	3.51 sec
61219	6.443 sec
68748	6.559 sec
324708	40.498 sec
95579	6.989 sec

Table-3.Execution Time of Encryption of Data

File size	Encryption time
10 KB	0.047 sec
20 KB	1.102 sec
30 KB	3.213 sec
40 KB	4.433 sec
50 KB	6.892 sec

IX. CONCLUSION

In this paper, a novel scheme is proposed for secure transmission of large secret data files. The security level of data is increased by encrypting the data where the addition of large amount of data is made possible by compressing the entire image. This scheme prevents any third party access and also prevents the attack by the hackers as protection is provided for the keys.

FUTURE ENHANCEMENT

In future, we can use audio or video instead of image as cover for hiding the data. Also a comprehensive combination of image encryption and hiding of audio/video files compatible with Lossy compression deserves further investigation.

REFERENCES

1. Kadam, P.; Nawale, M.; Kandhare, A.; Patil, M., "Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique" IEEE Trans. Pattern Recognition, Informatics and Medical Engineering (PRIME)-2013, pp.312-316, February 2013
2. Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image" IEEE Trans. Inform. Forensics Security, vol. 7, no. 2, pp.826-832, April 2012.
3. Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image" IEEE signals processing letters, vol. 18, no. 4, pp.255-258, April 2011.
4. Deepthi Barbara Nickolas; Sindhuja.B; Sivasankar.A, "Enhancement of Data Hiding Process in Encrypted Image Using Advanced Encryption Standard" International Journal of Current Engineering and Technology, Vol.3, No.2 -June 2013
5. Poongodi. S; Kalavathi.B; Shanmugapriya.M, "Secure Transformation of Data in Encrypted Image Using Reversible Data hiding Technique" International Journal of Engineering Science and Innovative Technology (IJESIT), Vol.2, Issue.4 – July 2013