IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 9, PP 52-58

Hybrid Approach For Securing Data

Amit Singh[1], Nayan Solanki[2], Prof. Foram Shah[3]
[1](Department of Computer Engineering, Atharva college of Engineering, India)
[2](Department of Computer Engineering, Atharva college of Engineering, India)
[3] (Department of Computer Engineering, Atharva college of Engineering, India)

Abstract: *During data transmission over the internet, it is important to transfer data in high security and high confidentiality, information security is the most important issue of data communication in networks and internet. To secure transferred information from intruders, it is important to convert information into the cryptic format. Different methods are used to ensure data security and confidentiality during transmissions like Steganography and cryptography. Proposed work improves information security through developing efficient compression of texts and encryption of texts by cryptography with steganography. The Proposed algorithm ensures the encryption and decryption using AES, compression and decompression by using LZW and RGB pixel shuffling with steganography. LSB method is used to insert data bits in LSB of RGB pixels of the cover image. In this Multi-threading use to retrieve information from image rapidly. Hence proposed system can reduce the data transmission time and cost. These algorithms are performed by using JAVA program.*
Keywords **–** AES, Cryptography, LSB, LZW, RGB, Steganography.

I. Introduction

On the internet nature of exchanging data, whether for business communication or social media, has changed from small text messages to different types of media files such as audio and video clips, various type of scientific and engineering photographic images, different kinds of an album, maps. Many of them contain confidential information which is always targeted for stilling information by industrial espionage hackers, the business competitor, adversaries, and personal data hackers.

Make multimedia data secure from unauthorized users access, destruction, modification, detection or distortion of the data while transferring over the internet. There are two well known methods for providing security protection from unauthorized users i.e. cryptography and steganography. Cryptography used to encrypt the data into random or meaningless characters which cannot be perceived by unauthorized users. Same way steganography also used to hide the data from attackers [1-8]. But the only difference between steganography and cryptography is, data is completely hidden into some other data instead of just changing the format of data which can easily attract intruders towards data because of their unlike nature [7][8].

Current steganography algorithms are having complexity problem in terms of time per data [1-8]. Nowadays steganography algorithm can hide data in equal length of image file for example it can hide 1Mb data with at least (or more than) 1Mb image file, it means that for extracting 1Mb data we have to download at least (or more than) 2Mb file (i.e.50% loss of data or more than 50% loss). Also, its cost for transmission is more and it takes more time for a complete transmission from sender to receiver.

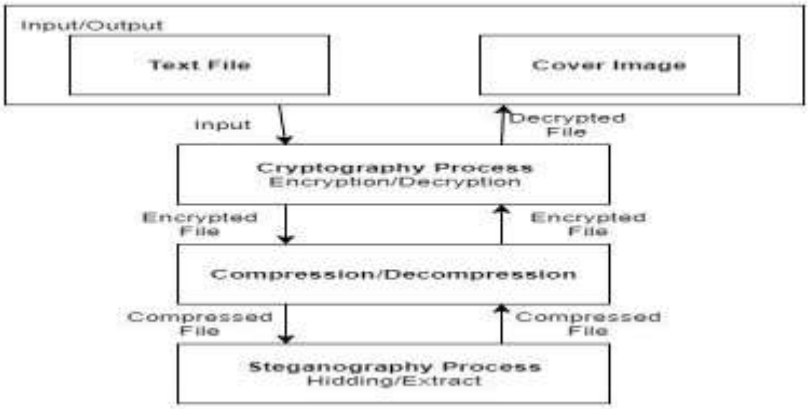

Fig.1: A General Steganographic Model

LZW compression scheme is used to optimize the size of secret data[10], it will enable a person to hide approx. two times more data in a cover-image, i.e. now we can store the double amount of data into the same image file[6][7]. This way we can reduce the cost and loss of data up to 50%. This approach is secure against the RS detection attack[6] and its stego-image is totally indistinguishable from the original image (cover image) by the human eye. We can save our decoding time by thread based[5] extracting data from stego-image at extraction time. This way we can reduce some amount of time from overall transmission time.

The general scheme for embedding data is depicted in Fig. 1. A message is embedded in a file by the stego-system encoder, which has as inputs the original cover, the secret message, and a key. Over a Communication channel, stego objects are transmitted to the receiver where the stego-system decoder uses the same key for processing given output. Following that same message given by the sender can be read .The Steganographic process can be represented using formulas[7]. The stego object is given by:

$I' = f(I,m,k)$

Where: I' is the stego object, I'' is the original object, m is the message and k is the key that the two parties share. The stego object may be subject to many distortions, which can be represented as a noise process n:

$I'' = I'+n(I')$

We want extracted signal *m at* the decoder end, we are considering signal I as unwanted signal. The signal which is embedded has to resist common distortions caused by the signal as shown in Figure 2. Two kinds of compression exist: the first one is *lossy* and another is *lossless*. Both methods have different results but they save storage space. Lossless compression permits exact reconstruction of the original message; therefore it is preferred when the original information must remain intact. Such compression schemes are the images saved as GIF (Graphic Interchange Format). Lossy compression, on the other hand, does not maintain the original's integrity. Such compression scheme is an image saved as JPEG (Joint Photographic Experts Group). The JPEG formats provide close approximations to high-quality digital photos but not an exact duplicate.

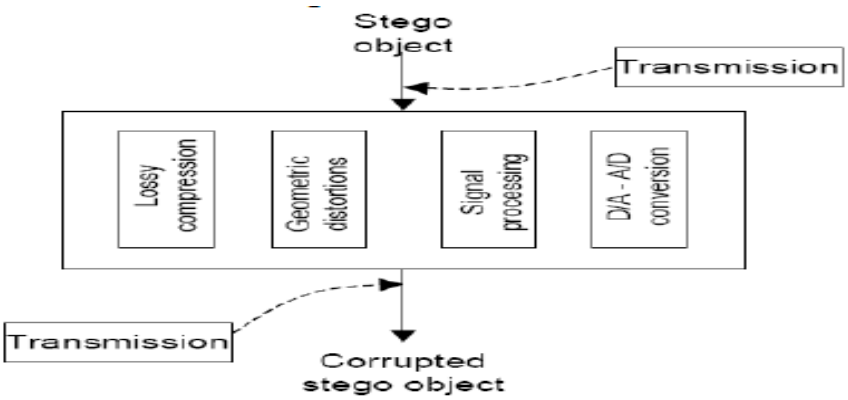

Fig.2: Common signal distortions over the transmission channel

II. Technology Used For Proposed Work

2.1 LSB insertion approach:

Least significant bit (LSB) insertion[2][3] is a common, simple approach to embedding information in a cover image [5]. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. An image is a set of pixels and each pixel have 3 bytes (i.e.24bits)[3][7].For example, if we want to hide any data which is represented into a binary number. Let's take 3 pixels i.e. each one have 24bits, as shown below

11010111 01101101 11111001
11010111 00111111 11011110
10011111 10110011 11110011

Let's take 9 bits data which we want to hide into above pixels by LSB insertion method which replaces all the least significant bits by given data. Our data is 111101111 which we will be embedding into above pixels.

1101011**1** 0110110**1** 1111100**1**
1101011**1** 0011111**0** 1101111**1**
1001111**1** 1011001**1** 1111001**1**

Here now we have successfully hidden 9 bits into image file but at a cost of only changing 1, or roughly 9%, of the LSBs. Similar methods can be applied to GIF images but the changes, as the reader might imagine, are more dramatic [2]. For more details refer [2][3].

2.2 LEMPEL –ZIV-WELCH(LZW) Algorithm:

Lempel-Ziv-Welch(LZW) compressor technique is one the best lossless compressor method. By compressing the data we can reduce size of data and because of its lossless behavior, we will get same data without any loss of information during decompression of data. For a better understanding of the work of Lempel-Ziv-Welch (LZW) compression algorithm refer [7][10].

2.2.1 Compression Algorithm

1. Build a table and store all possible strings in it
2. STRING = get input character
3. WHILE there are still input characters
4. DO CHARACTER = get input character
5. IF STRING+CHARACTER is in the string table then STRING = STRING + character
6. ELSEoutput the code for STRING
7. add STRING+CHARACTER to the string table
8. STRING = CHARACTER
9. END of IF
10. END of While
11. output the code for STRING

2.2.2 Decompression Algorithm

1. Build a table and store all possible strings in it
2. Read OLD_CODE
3. OLD_CODE = get translation of OLD_CODE
4. output OLD_CODE
5. CHARACTER = OLD_CODE
6. WHILE there are still input characters
7. DO Read NEW_CODE
8. IF NEW_CODE is not in the string table THEN
   STRING = OLD_CODE
   STRING = STRING+CHARACTER
9. ELSE
   STRING = get translation of NEW_CODE
10. END of IF

11. Output STRING
12. CHARACTER = first character in STRING
13. add OLD_CODE + CHARACTER to the string table
14. OLD_CODE = get translation of NEW_CODE
15. END of WHILE

III. Proposed System

The main objective of the proposed system is to secure data from the unauthorized user by putting multiple layers of security on data. All layers should be in proper order so that system will work smoothly. The proposed method is using LSB technique to hide the data or embedding data into an image file. And also cryptography use to make more complex to understand actual information for unauthorized users. To increase hiding capacity of data into image file we use Lempel-Ziv-Welch (LZW) compression technique. It increases the hiding capacity of an image by 50%. Now we can hide approx double data compare to the previous case. We are using a key which helps to improve prevention of unauthorized access of the system. Key helps sender to lock the stego-image during transmission. In this proposed system stego-image always contain a small code which will ask for a key to the user at extraction time, without right key user cannot extract information from stego-image. At the extraction time, the proposed method is using multi-threading technique to retrieving data rapidly. Depending on number multiple threads extraction time will decrease by half each time[5]. This way we can extract data comparatively in less time so that we can increase the efficiency of the proposed system.
Steps involve in proposed method and algorithms are given below,

3.1 Embedding Process:

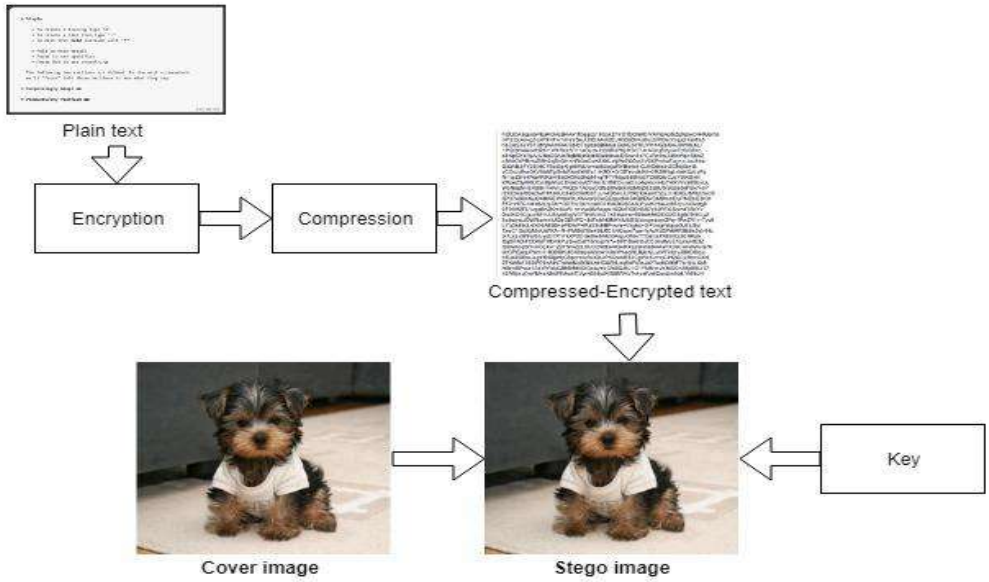

Fig.5: Embedding Process

Input: The text message and cover image represented by animated GIF/JPEG image.
Output:: The stego image represented by animated GIF/JPEG image.
Step 1: Read the text message.
Step 2: Encrypt the text message by using AES algorithm.
Step 3: Compress the encrypted message by using LZW compression algorithm.
Step 4: Extract all frames from the stegoimage (animated GIF/JPEG image) and convert them to a 256 color BMP images.
Step 5: For i=1 to no. of the bit in the LZW text code.
Step 6: For j=1 to no. of pixels in each frame.
Step 7: For k=1 to no. of image frames.

Step 8: Hide the LZW code bit in current pixel by using LSB algorithm.
Step 9: next k.
Step 10: next j.
Step 11: next i

3.2 Extracting Process:

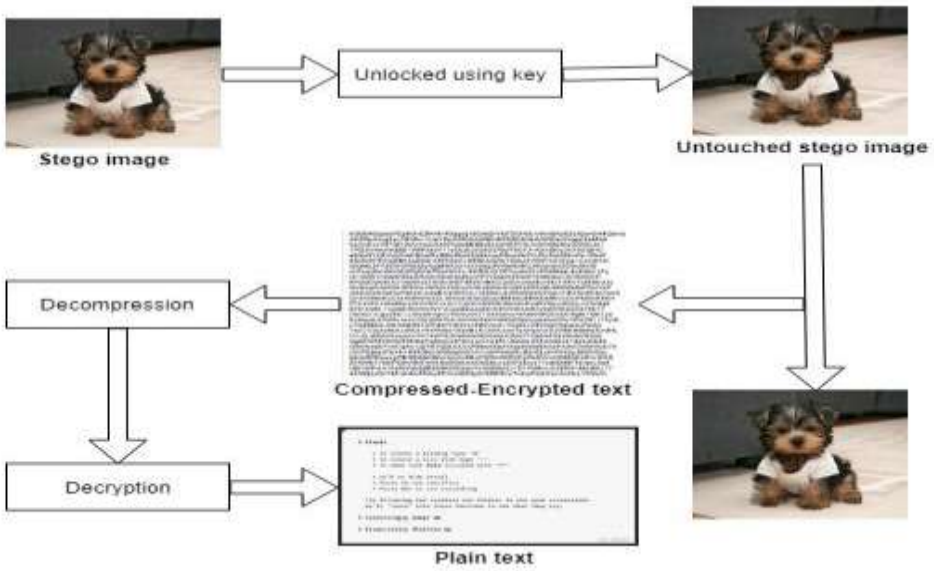

Fig.6: Extracting Process

Input: The stego image represented by animated GIF/JPEG image.
Output: The text message.
Step 1: Extract all frames from the stegoimage(animated GIF/JPEG image) and convert them to a 256 color BMP images.
Step 2: Sort the palette of all BMP images and reassign each
Step 3: For i=1 to no. of the bit in the LZW text code.
Step 4: For j=1 to no. of pixels in each frame.
Step 5: For k=1 to no. of image frames.
Step 6: Extract the LZW code bit from the current pixel by Using LSB algorithm.
Step 7: next k.
Step 8: next j.
Step 9: next i.
Step 10: Decrypt the decompressed text message by using AES algorithm.
Step 11: Decompress the LZW text code by using LZW Decompression algorithm.

IV. Experimental Results

The peak signal-to-noise ratio (PSNR) is a value which indicates or evaluate the stego-image quality. Larger the value of PSNR indicates less distinguish between cover image and stego-image and stego-image is more invisible to the human eye.
The PSNR is defined as bellows:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\,dB \quad \ldots(1)$$

$$MSE = \left(\frac{1}{M\ x\ N}\right)\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(\alpha_{ij} - \beta_{ij})^2 \quad \ldots(2)$$

Where α_{ij} and β_{ij} are the pixels of cover image and stego-image respectively at the coordinate is (i,j).
And also proposed system overcome the RS detection of stego-image which is less alteration in pixel values which indicates the good quality of stego-image.

Two images are shown in Fig.7 which explain the embedding process of data. Here we obtained stego-image which exactly looks like cover image. And also stego-image is a lock with the key provided by the user which is directly transferred to the receiver through mail-in an encrypted format. To use that key, user needs to first decrypt that key and then use for the extraction process.

Fig.7: Embedding Data

In Fig.8 there is two column, in that first column contain stego-image which requires the key, provided by the sender through the mail, for extraction of information from the stego image. And in another half of column shows the acceptance of key for completing the extraction process.

Fig.8: Extracting Data

V. Conclusion

Using above system, retrieval of the hidden message from image becomes more complex because text messages are compressed using LZW which makes processing difficulties for the intruder. another advantage of the system is that, for any observer, it becomes difficult to recognize difference between original image and image with hidden text message compared to other approaches. Here the lossless compression method used in the image and in the embedded text result to extract the text without any changes in the message. Other cryptographic algorithms, compressions methods can be used with the proposed system in future to improve performance.

References

[1] Aishwarya Baby, Hema Krishnan, "Combined Strength of Steganography and Cryptography- A literature survey", *International Journal of Advanced Research in Computer Science*, Volume 8, No. 3, March-April 2017, Kerala, India.

[2] Richard Apau,Clement Adomako,"Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones", *International Journal of Advanced Research in Computer Science*,Vol.164,No.1,April 2017,Kumasi-Ghana.

[3] Assist.lec. May H.Abood, "An efficient Cryptography using Hash-LSB Steganography with RC4 and pixel shuffling encryption algorithms", *in Proc. Annual Conference on new trends in information and communications technology applications(NTICT 2017*), 7-9 March 2017, Baghdad, Iraq.

[4] M. Mary Shanthi Rani, K. Rosemary Euphrasia, "Data Security through QR code encryption and steganography". *Advanced Computing: An International Journal (ACIJ)*, Vol.7, No.1/2, March 2016, Tamil Nadu, India.

[5] Mr. A. Balasubramani, Dr. Chdv. Subba Rao, "Sliced images and encryption techniques in steganography using multi-threading for fast retrieval*", International Journal of Applied Engineering Research ISSN 0973-4562* Volume 11, Number 9 (2016) pp 6504-6509, Andhra Pradesh, India.

[6] Dilpreet Kaur, Harsh Kumar Verma, Ravindra Kumar Singh, "A Hybrid Approach of Image Steganography",*International Conference on Computing, Communication and Automation (ICCCA2016)*

[7] Intisar Majeed Saleh, Hanaa Merzah, "Efficient data hiding system using LZW cryptography and GIF image steganography", *International Journal of Technical Research and Applications*, Volume 3, Issue 2(Mar-Apr 2015), pp. 28-32, Baghdad, Iraq.

[8] Vipul Shanna, Madhusudan "Two new approaches for image steganography using cryptography", *Third International Conference on Image Information Processing*, 2015, Srinagar, J&K, India.

[9] Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security",*Global Journal of Computer Science and Technology Network, Web & Security*,Volume 13 Issue 15 Version 1.0 Year 2013,IITM,India

[10] The Scientist's and Engineer's Guide to Digital Signal Processing ch27/Data Compression/LZW Compression. [http://www.dspguide.com/ch27/5.htm].Accessed March 6, 2018.