A Novel Approach of Secure Communication: Encryption Based Compression Technique

[1]Mr. Aajam Sheikh, [2]Dr.Prashant Panse
[1]Research Scholar,[2]Associate Professor
,[2]Department of Information Technology, MITM, Indore, MP, India
***Email:** [1]aajam.it52@gmail.com*

DOI:https://doi.org/10.5281/zenodo.2011360

Abstract

Transmission of information through a problematic channel for communication assumes an essential job in the present period subsequently communication security over an overall system turning into a most rising point. Different advances have been acquainted with satisfy this need Cryptography and Steganography are two strategies in this period. Cryptography method distorts the information so that separated from proposed client nobody can get to it. Be that as it may, it is having an impediment that in this system message exist in encoded however noticeable shape. So malicious user keeps trying to decrypt that message and once it is decrypted it reveals its identity. Hence Steganography has been introduced to overcome the limitation of Cryptography. For secure communication various compression techniques are available which are described below.

***Keywords**: Steganography, Cryptography, Compression technique for secure communication, LSB.*

INTRODUCTION

Steganography found its existence long time ago. In past, Greek Historian Herodotus requests to tattoo the mystery message over the scalp of the slave and when the hairs were again developed, the slave was dispatched for the goal. Amid Second World War German found another strategy called Microdots. In this method Germans expected to diminish the span of a mystery message or picture except if and until the point when it moved toward becoming as a similar size of the composed period. Later this strategy was utilized, to shroud the mystery message on a wooden piece and afterward it was secured with wax. Also, the method was utilized as imperceptible ink. In this technique the secret message was written by a special kind of ink called invisible ink and the message was retrieved back when the paper got heated. This technique was also used by Britishers to take charge over India. They supposed to use drum of vaccination to hide themselves from Indian, in this way they collect their army in India and starts ruling over Indians [1].

Techniques for secure communication are described below:

1. Cryptography: Cryptography scramble -s the data to be communicated so that unauthorized receivers cannot see the information [6]. Cryptography uses a key for data encryption. The fact is that communication is taking place is known to everyone.
2. Steganography: Steganography transmi -ts data in such a way that a viewer cannot even detect the transmission of message is taking place and hence cannot try to decrypt it [1].
3. Watermarking: Digital Watermarking mostlyendow withavoidance from illicitreplica or claims the possession of digital media but it is not geared for communication [7].

RELATED WORKS

In "**Implementation of Steganography Using CES Technique**" the researcher proposed a procedure which utilizes the combination of cryptography and steganography for correspondence. CES system is used to trade the secret information between two ends. Information is first preprocessed before concealing it behind a cover picture. Preprocessing includes pressure of information which lessens its size o that a lot of information can be put away utilizing recurrence area based steganography. Finally this compressed data is hidden behind a g image using a secret key. In CES technique the data is first compressed and then altered with the help of a key. The modified text or cipher text is hidden behind 8th DCT coefficient of each row. But the data is hidden only the DCT coefficient of Blue component. The reason to hide the secret data behind blue component is its least visibility to human visual system. The advantage of this technique is that if intruders detect the presence of secret message then they cannot access the secret data because they will need secret key to decrypt it. And the size of the secret message does not change after embedding [15].

In "**Modified BPCS steganography using hybrid cryptography for improving data embedding capacity**" author proposed a procedure which utilizes hybrid cryptography of RSA and DES calculation for information encryption and pressure. In this technique changed BPCS (Bit Plane Complexity Segmentation) steganography is used which replaces all commotion regions with bit planes of the cover picture with mystery data. In this framework mystery data can be recuperated without having exceptional picture. In this technique the pressed message is introduced on noisy piece planes. At the recipient end got stego picture is rotted and again multifaceted nature of each territory is resolved and the noisiest area is used to isolate the mystery message for secure communication [16].

In "**An Enhanced Security Technique for Steganography Using DCT and RSA**" author proposed to utilize a blend of DCT based steganography strategy with RSA calculation. In this procedure one 8-bit dim scale picture is utilized as cover picture and another 8-bit dark picture is utilized as mystery message at that point by applying RSA calculation encryption is performed. In this strategy cover picture and mystery picture is partitioned into 8*8 square of pixels. At that point cover picture in spatial area is changed over into recurrence space DTC. Presently implanting is performed over mid DCT coefficient of cover picture after this by applying IDCT inserted picture is changed over into spatial area. At accepting end switch activity is performed to get the mystery picture [6].

In "**A Novel Steganography Algorithm for Hiding Text in Image Using Five Modulus Method**" All the non-multiple pixels of 5 give some remainder and are used to hide the secret message. The main advantage of this technique is that it keeps the size of the cover image constant. FMM consists of dividing an image into KXK pixel block, in bi-level grey image the value ranges from 0 to 255 hence if we can easily transform value in this range which is multiple of 5. It can not affect human visual system. So in order good result [11].

In "**A New Method inImage Steganography with Improved Image quality**" the secret message embedding is performed by using identical or similar bits between the secret message and pixel value of an image. This method is simple, fast and robust according to author and provide83% accurate results. In this method the picture is examined push by line and encoded into its double frame then again mystery message is additionally encoded into its twofold shape. At that point the extent of both cover picture and mystery message are checked. After that any one pixel of the cover picture is haphazardly chosen and its coordinating two by two bits are looked against mystery message bits. At the point when the indistinguishable match is discovered mystery message bit are inserted on cover picture with new qualities. Also, this area is recorded in paired table. Along these lines stego picture with mystery message is set up to transmit. This paper reasoned that this system give low picture quality debasement and make the mystery message more secure [10].

Different techniques have been implemented till now but these systems are having certain problems which are as follows:

- Unauthorized access of secret data over an unsecure channel.
- The existing system hides the secret message over the LSB of the smooth region. It can change the color o texture of the cover image which can draw the attention of anyone towards it.
- At the receiving end we need to send cover image as well as Stegoimage. Hence if the encryption is known to any one the n it is very easy for him toretrieve the secret message and breach the security of the system.
- One more problem with cover image is that up on embedding, it greatly increases the size of cover media which requires additional storage and as a result of which cost of storage increases.

PROPOSED TECHNIQUE

In the proposed work, implementation of LSB and edge based compression and encryption technique is performed in spatial domain. In edge based compression and encryption technique first either gray scale or color image is taken as input matrix and its edge is used to hide the secret message. Every pixel in a color image composed of three colors (channels) i.e. Red, Green and Blue. So, every pixel contains 24 bits (for 8-bit representation) where 8 bits for red component, 8 bits for green and 8 bits for blue component in a pixel.

In the projectedmethod for data embedding an edge is used to take the benefit of being unobserved because editing in edge areas cannot be easily observed by human visual system. Edge area may contain large number of secret bits as compared to smooth areas. Edge detection is the procedure of identifying the sharp changes in intensity of adjacent pixels. The point where discontinuity occurs in image is identified as edge.

For edge detection, canny edge detector is worn which is based on fixeddivergenceestimate of the partial derivatives. Before embedding, the covert data is compacted first by using LZW lossless compression technique. Data compression consists of taking a stream of symbols and transforming them into its corresponding ASCII codes. For effective compression, the resultant stream of codes is smaller than the original symbol. After compression, this compressed message is converted into cipher text by using RSA algorithm.

For decryption and encryption,RSA Technique is used, respectively. A plaintext message P is encrypted to cipher text C by
$C = P^e \mathrm{mod}\ n$
The plaintext is recovered by

$P = C^d \bmod n$

Below Figure is showing the architecture diagram of proposed technique. In this technique, first input image is taken from user and if this input image is gray scale image then directly its edges are determined by using Canny edge detector and if this image is color image then its Red, Green and Blue Components are calculated and then converted into gray scale format. Now on the individual component canny edge detector is applied to find their edges.

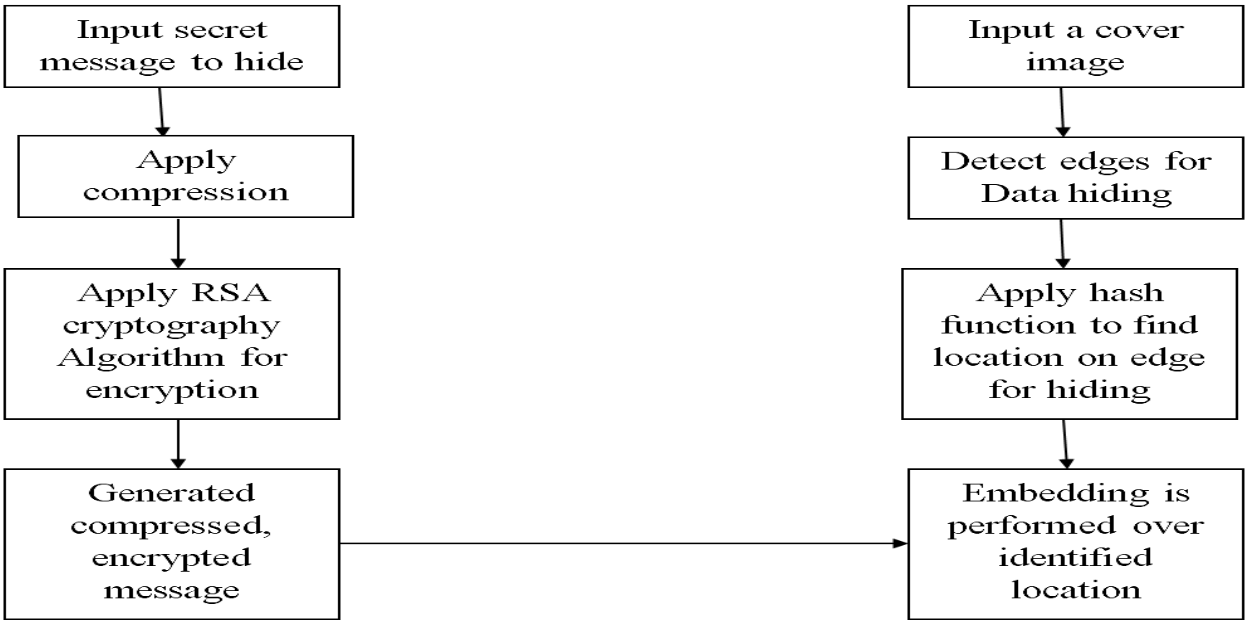

Input secret message to hide
Apply compression
Apply RSA cryptography Algorithm for encryption
Generated compressed, encrypted message
Input a cover image
Detect edges for Data hiding
Apply hash function to find location on edge for hiding
Embedding is performed over identified location

Fig:1.*Architecture to embed the secret message behind any cover image*

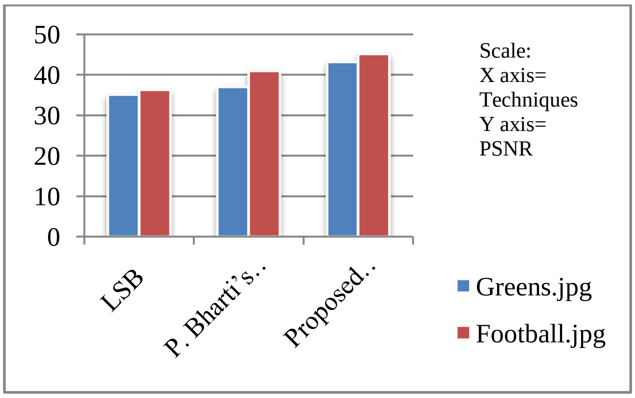
This edge is used to hide the secret message because edge is that place in an image that causes very less distortions in image after embedding. At the other end LZW algorithm is applied over the secret message for lossless compression and after compression RSA encryption algorithm is applied to encrypt the secret data. After successive compression and encryption, secret message is embedded at the location identified by the hash function on the edge of the image. In this way stego image is generated which is dispatched to the intended user. At the receiving end secret message is retrieved again by using the same key with the help of which encryption is performed.

Following table shows the results based on above discussed technique and it is showing much better results than previously implemented techniques.

Table:1.*Comparison results of Various Steganography Techniques*

Image	LSB	P.Bharti’s Technique	Proposed Technique
Green’s.jpg	35.1	37	43.1
Football.jpg	36.3	41	45.1

The above table shows the comparison of various spatial domain techniques and clearly shows the improvement of results. This can be better understood by bar graph shows below.



***Graph: 1.** comparison graph of various spatial domain techniques*

CONCLUSION

In plannedprocedure, the assemblage of Cryptography and Steganography is used to boost the protection without drawing notice of anybody. Steganography hide the subsistence of the surreptitious message while Cryptography encrypts and decrypts the furtive message. A combination of both these techniques does not expose the uniqueness of the secret message over an unsecure conduit. If the smooth regions of the cover image were used then it may cause visible distortions hence to remove this drawback edge area is used for hiding.Because of this if the foe recognizes the nearness of concealed information behind the cover picture and prevails to get it, he needs to apply loads of endeavors on it to recoup the first message which is preposterous insofar as correct encryption key isn't accessible. In awry key cryptography the mystery message is encoded by utilizing recipient's open key and at the less than desirable end the mystery message is decoded by utilizing collector's private key. The information is covered up in the edge by discovering area utilizing hash work in this manner an enormous measure of compacted information can be put away there with a few changes in unique and Stego picture. It makes the procedure more powerful and secure.

REFERENCES

1. PritamKumari, Chetna Kumar, Preeyanshi, Jaya Bhushan, “Data Security Using Image Steganography And Weighing Its Techniques,” in international Journal Of Scientific & Technology Research Volume 2, Issue 11, November 2013,pp. 238-241.
2. M. Prasad, "Basic Concepts of communication," 24 December 2012. [Online]. [Accessed Admin at max Embedded IT University, Vellore].
3. J. G. Daugman, "The communication Vision Homepage," Carnegie Mellon University. [Online]. Available: http://www-2.cs.cmu.edu/_cil/vision.html.
4. http://expertedge.aje.com/2012/05/21/figures-and-file-types-the-basics.
5. Rina Mishra, DeepikaDongre, “A research review on data security rationale,” in national conference on national conference on Innovative trends in engineering sciences & management 2014.
6. Shahana T, “An Enhanced Security Technique for Steganography Using DCT and RSA,” in international Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 7, July 2013,pp. 943-949.
7. RamadhanMstafa, Christian Bach, “Information Hiding in Images Using

Steganography Techniques," in ASEE Northeast Section Conference 2013.

9. Islam, Md. Baharul Islam,"A Novel Approach for Image Steganography Using Dynamic Substitution and Secret Key," in American Journal of Engineering Research (AJER), Volume-02, Issue-09, pp-118-126.
10. Dr.S.Vijayarani, Mrs.M.Vinupriya, "Performance Analysis of Canny and Sobel Edge Detection Algorithms in Image Mining," in International Journal of Innovative Research in Computer and Communication Engineering,Vol. 1, Issue 8, October 2013, pp. 1760-1767.
11. Uvika,SumeetKaur, "A Comprehensive Review On Different Edge Detection Techniques," in An International Journal of Engineering Sciences ISSN: 2229-6913 Issue July 2012, Vol. 6, pp. 162-169.
12. SnehaArora, SanyamAnand, "A Proposed Method for Image
8. Saeed Ahmed Sohag, Dr. Md. Kabirul

   Steganography Using Edge Detection," in International Journal of Emerging Technology and Advanced Engineering,Volume 3, Issue 2, February 2013,pp. 296-297.
13. Tara Bansal, RuchikaLamba, "Steganography Using Various Quantization Techniques: A Review," in International Journal of Advanced Research in Computer Science and Software Engineering, July- 2013, pp. 26-30.

Cite as:
Mr. Aajam Sheikh, & Dr.Prashant Panse. (2018). A Novel Approach of Secure Communication: Encryption Based Compression Technique. Journal of Electronics and Communication Systems, 3(3), 32–37. http://doi.org/10.5281/zenodo.2011360