Image Visual Cryptography By Using Haar Wavelet Based Decomposition

Ms. Pradnya S. Nagdive[1],
ME Scholar, CSIT Dept, H.V.P.M College of Engineering
Amravati, Maharashtra, India

Prof. Anjali B. Raut[2]
HOD, CSE Dept, H.V.P.M College of Engineering
Amravati, Maharashtra, India

Abstract— **To maintain the privacy and certainty of pictures may be a spirited space of analysis, with two totally different approaches being followed, the primary being encrypting the pictures through encoding algorithms using keys, the secondary approach involves hiding the data using data hiding algorithms to take care of the pictures secrecy. A content owner encrypts the first image using an encoding key, and an information-hider will embed further data into the encrypted image employing a data-hiding key although he doesn't recognize the first content. With an encrypted image containing further information, a receiver could initially decode it with the encoding key, then extract the embedded information and recover the first image with the data-hiding key.**

Index Terms—**Cover image, Information Concealing, Information extraction, Image encoding, Image decoding and Information recovery.**

I. Introduction

The security of information is presently one in every of the foremost pressing problems to that several researchers have paid plenty of attention. To achieve security two techniques are most widely used. These techniques are nothing but the Cryptography and Steganography.

Cryptography could be a technique for securing the key data. Sender encrypts the message with the help of key then sends it to the receiver. The receiver decrypts the message to obtain the private data. Cryptography focuses on keeping the content of the message secret.

Steganography is the practice of hiding information "in plain sight". This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer. Importantly, the transport layer – the carrier file - is not secret and can therefore be viewed by observers from whom the secret message itself should be concealed. The power of steganography is in hiding the secret message by obscurity, hiding its existence in a non-secret. while information concealing(also called as steganography) concentrates on keeping the existence of the message secret. The word steganography combines the Ancient Greek words *steganos* meaning "covered, concealed, or protected", and *graphein* meaning "writing". Information Concealing is another technique for secured communication. Information Concealing involves hiding the data thus it seems that no data is hidden at all. If an individual or more than one person views the object within which the information is hidden then he or she will have no idea that there is any hidden information, that's why the person will not attempt to decrypt the information. Information Concealing is the process of hiding a secret message within cover medium such as image, video, text, audio. Hidden image has many applications, especially in today's modern, high-tech world. Privacy and secrecy is a concern for most people on the internet. Hidden image allows for two parties to communicate secretly and covertly.

The strength of data hiding gets amplified if it combines with cryptography. The terminologies used in information concealing are cover-image, hidden image, secret message, secret key and embedding algorithm. Cover-image is the carrier of the message such as image, video or audio file. Cover-image carrying the embedded secret data is the hidden image. Secret message is the information that is to be hidden in a cover image. The secret key is used to embed the message depending on the hiding algorithm. The embedding algorithm is the way, which is used to embed the secret information in the cover image.

The security of the transformation of hidden data can be obtained by two ways: encoding and information concealing. A combination of these two techniques can be used to increase the data security. In encryption, the message is altered in such a way that no data can be disclosed if it is received by an attacker. Whereas in information concealing, the secret message is embedded into an image often called cover image, and then sent to the receiver who extracts the secret message from the cover image. When the secret message is embedded into cover image then it is called a hidden image. The visibility of this image should not be distinguishable from the cover image, so that it almost becomes impossible for the attacker to discover any embedded message.

II. Literature Survey

To study the concepts such as Visual Cryptography and Steganography we have referred following papers. Here we have described related papers and we thank to authors of these papers to provide knowledge about these concepts.

In 2011 Khalil Challita and Hikmat Farhat proposed two different approaches that help us achieve a higher level of secrecy and security, together with their limitations. The first method is about combining steganography and cryptography in such a way to make it harder for a steganalyst to retrieve the plaintext of a secret message from a stego-object if cryptanalysis were not used. The second method does not use any cryptographic techniques at all and relies solely on steganographic ones. These two steganographic techniques used to hide secret messages in stego objects that use the least significant bit method, together with known methods that stem from steganalysis on how to counter them. The first one does not modify the cover object and consists in sending a (possibly encrypted) vector that contains the different positions of the cover object that allow us to reconstruct the secret message from it. In this case, both the sender and the recipient should share a secret algorithm (or a key) on how to retrieve the secret message, given the cover object and the (secretly sent) vector. The originality of this paper lies in the second protocol that we called Multiple-Cover-Objects, where we suggest using more than one cover object to hide a secret message. Indeed, in order to recover the secret message, a steganalyst has to determine all the stego-objects and unravel the algorithm used to hide into them the secret message [1].

In 2012 Ravindra Gupta, Akanksha Jain, Gajendra Singh proposed a method that encodes the secret message in least significant bits of the original image, where the pixels values of the encrypted image are modified by the genetic algorithm to retain their statistic characters, thereby making the detection of secret of message difficult. Use of Genetic algorithm has compelled the system for enhancing the security. The proposed system hides data in a real image and achieve its detection after underwent to visual cryptography. The main aim of the proposed model is to design a feasible RS- resistance secure algorithm which combines the use of both steganography and visual cryptography for improving security, reliability and efficiency for secret message. The implementation shows that the proposed system has better resilient by considering the steganalysis [2].

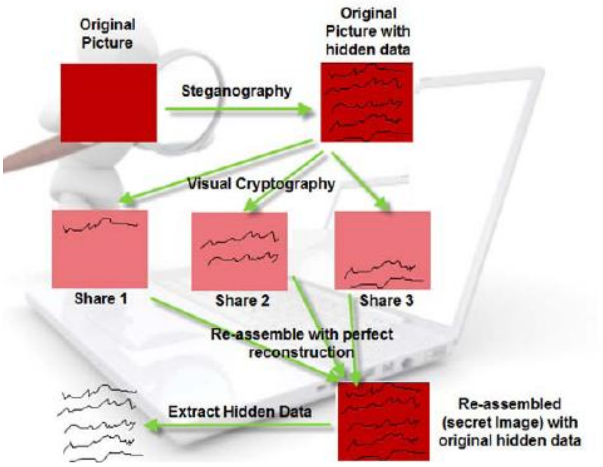
Original Picture
Original Picture with hidden data
Steganography
Visual Cryptography
Share 1
Share 2
Share 3
Re-assemble with perfect reconstruction
Extract Hidden Data
Re-assembled (secret Image) with original hidden data

Fig. 1 Proposed System

In 2013 Ajit Singh and Swati Malik proposed two layers of security i.e. cryptography and steganography which makes it difficult to detect the presence of hidden message. But in some cases if the eavesdropper has attacked the carrier of message then he will not be able to get the original message as all the relevant data here is in encrypted form. For cryptography Blowfish algorithm is used which is much better than AES and DES. In order to break blowfish algorithm he has to spend a lot of time and effort for trying several attacks and getting the original message. Although both of these techniques are easy to implement but there combination will provide much efficient and reliable security [3].

In 2013 Poonam Bidgar, Neha Shahare proposed Key based Visual Cryptography Scheme using Novel Secret Sharing Technique with Steganography. They are suggesting one new method in which a symmetric secret key is used to encrypt the image and then secret shares are generated from this image using Novel secret sharing technique with steganography. So, finally this method will produce meaningful shares and use of secret key will ensure the security of scheme. This scheme can become a reliable solution suitable for today’s authentication challenges.

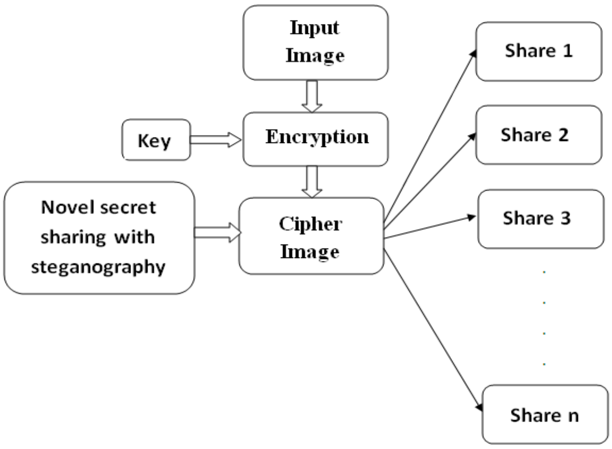

Fig.2 Encryption Process

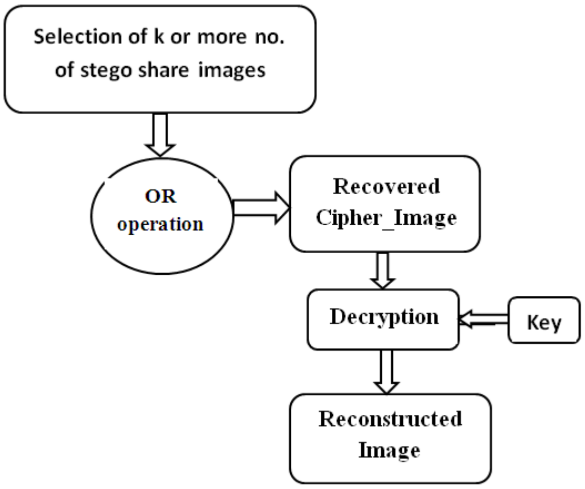

Fig.3 Decryption process

In this new proposed scheme, use of Symmetric key is suggested in first level of encryption process of secret image which will offer additional security. And then they are going to use novel secret sharing with steganography for the creation of shares of this encrypted image which will be meaningful shares instead of having noise like shares. So, because of meaningful shares attacker may fails to guess whether these images contain any secret information. Use of secret key makes it more secure and reliable [4].

In 2014 Rehana Begum R.D and Sharayu Pradeep invented a best approach for LSB based Steganography. The proposed system provides the best approach for secure data hiding and transmission over Networks using LSB based steganography with Genetic Algorithm (GA) and Visual Cryptography (VC). The system here encodes the secret message in least significant bits of the cover image so termed as stego image by using a secret key. Genetic Algorithm and Visual Cryptography has been used for enhancing the security. Genetic Algorithm is used to modify the pixel location of stego image which is another protection lock for the secret message and image and the detection of this is complex. Visual Cryptography is further used to encrypt the modified pixel image by breaking it into two shares based on a specific threshold, later those encrypted shares and the secret key is separately sent to others using Network Socket Programming. User who received the secret shares has to do the reverse process to retrieve the Image and the secret message by using the secret key [5].

In 2014 Siddaram Shetty, Minu P. Abraham proposed a new approach to encrypt a generated image share of Visual Cryptography using Public key Encryption. We used RSA algorithm in order to provide the double security of the document. Hence, shares of secret image are not exist in their actual form for third parties (those who try to create fake shares) to make alteration. The proposed scheme provides shares that are more secure and robust against number of attacks. This scheme also provides strong security for the handwritten text, documents and images that exists in the public network.

The proposed scheme is perfectly secure and very easy to implement with low computation cost. In our proposed scheme, first the secret image is taken and then it is divided into shares after converting it into binary image, then the shares of binary image are encrypted and decrypted using RSA algorithm, because of this even if the third party or intruder, once getting all the shares, he/she can’t get back the original secret image without availability of the private key. We can notice that there are many possible extensions exist as the visual quality & size of retrieved image. We can use following as some of the future extensions. 1. We can use colour image in place of binary image and then generate the shares using Visual Cryptography method. 2. Encrypted shares can be compressed in order to reduce the bandwidth requirement. We can implement this type of system in various fields like in Military, Defense, and other places where the confidentially of data should be must [6].

In 2014 Biswapati lana, Partha Chowdhuri, Madhumita Mallick, Shyamal Kumar Mondal proposed a Steganographic Scheme to Prevent Cheating in Visual Cryptography. Here a steganographic approach is proposed to detect fake share and then revealed secret image from original share. Our attacks are to reveal fake images which cheat honest participants.

To achieve cheating prevention in VC they have proposed a steganographic scheme to embed a secret message in each of the shares in random location during share generation phase called stego share. Before stacking receiver can extract hidden message from stego share for cheacking authentication of shares. In this method no verification share is required to prevent cheating in VC [7].

III. Proposed Methodology

In the proposed method, we used two algorithms which are as follows

A. Data Hiding
B. Data Extraction

Data Hiding Algorithm is used for hiding data in the image. For hiding data, 5 bits (LSB) out of 8 bits of each R, G, and B channel are used. Overall we used 15 bits out of 24 bits (ie. 1 pixel) for data hiding.

Data Extraction Algorithm is used for extracting data from the image .For extracting data the key by using which we hide data must be required because without key we can’t extract data from the image.

A. Data Hiding

1. Select an Image
2. Split an Image into segments.
3. Select an image segments.

4. Select Secrete data for hiding.
5. Encrypt data with Shifting method
6. Split data into segments.
7. Apply Higher LSB Method for replacing pixels bits with encrypted data bits by taking one image segment & secret data segment.
8. Repeat Step 3 & Step 7 until all encrypted data segments are not hidden within image segment.
9. Generate and select key OR Add own key
10. Encrypt image segments.
11. Join Segments (Level 2)
12. Join Segments (Level 1)
13. Join Segments (Level 0)
14. Stop

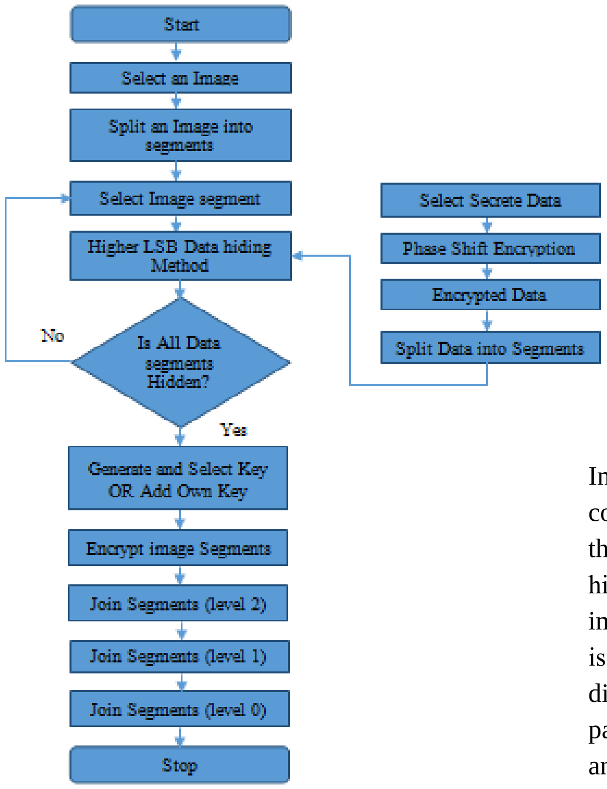

Fig.4 Flow diagram for Data Hiding

B. Data Extraction

1. Select a Stego Image.
2. Split stego Image.
3. Generate and Select Key OR Use Previous Key
4. Decrypt Image Segments
5. Apply Higher LSB Extraction algorithm.
6. Extract data bits from 1 to 5 LSB color pixels bits using Stego Key.
7. Decrypt Data using Phase Shift Decryption
8. Assemble Data.
9. Stop

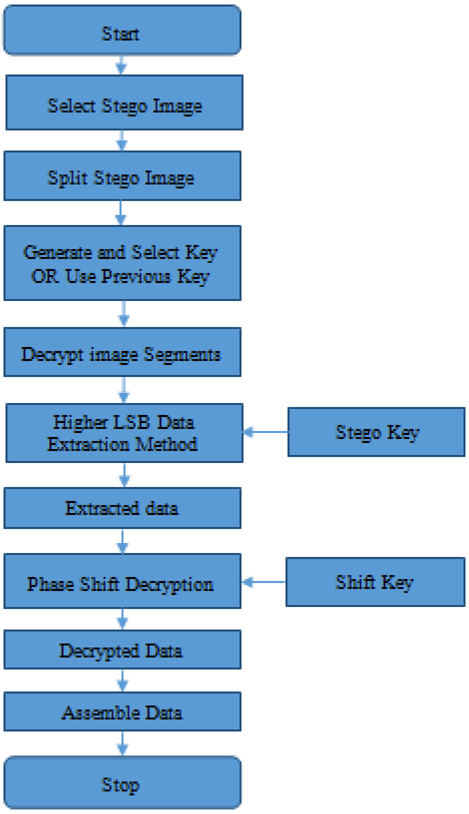

Fig. 5 Flow diagram for Data Extraction

IV. CONCLUSION

In this way, we have presented a new method by using the combination of visual cryptography and steganography. In this method, if hacker has got the image in which data is hidden, he can't recognize the presence of message in the image due to steganography and if he recognized that message is present in the image, he can't retrieve the message because different keys known to only owner are used to hide different parts of message and also that message is convert into an another form that is not understandable to hacker, this is done by using visual cryptography.

ACKNOWLEDGMENT

I would like to thank my guide for motivating me to do research in this domain and also guiding me in proper way.

REFERENCES

[1] Khalil Challita and Hikmat Farhat "Combining Steganography and Cryptography: New Directions" International Journal on New Computer Architectures and Their Applications (IJNCAA), ISSN 2220-9085, 2011

[2] Ravindra Gupta, Akanksha Jain, Gajendra Singh " Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012

[3] Ajit Singh and Swati Malik "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in

Computer Science and Software Engineering,Volume 3, Issue 5, May 2013

[4] Poonam Bidgar, Neha Shahare "Key based Visual Cryptography Scheme using Novel Secret Sharing Technique with Steganography" IOSR Journal of Electronics and Communication Engineering e-ISSN: 2278-2834, Volume 8, Issue 2 (Nov. - Dec. 2013)

[5] Rehana Begum R.D and Sharayu Pradeep "Best Approach for LSB Based Steganography Using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission over Networks" International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 6, June 2014

[6] Siddaram Shetty, Minu P. Abraham "A Proposal to Secure Visual Cryptographic Shares of Secret Image using RSA" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 12, December 2014

[7] Biswapati lana, Partha Chowdhuri, Madhumita Mallick, Shyamal Kumar Mondal "Cheating Prevention in Visual Cryptography using Steganographic Scheme" IEEE Conference 2014

[8] Mehdi Hussain and Mureed Hussain" A Survey of Image Steganography Techniques" International Journal of Advanced Science and Technology Vol. 54, May, 2013

[9] Mr. Deepak S. Bhiogade, Prof. Shaikh Phiroj Chhaware" Steganography and Visual Cryptography for Secured Data Hiding" International Conference on Industrial Automation and Computing (ICIAC),13th April 2014

[10] Shaveta Mahajan, Arpinder Singh" A Review of Methods and Approach for Secure Stegnography" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),Volume 2, Issue 10, October 2012, ISSN: 2277 128X

[11] Pradeep Kumar Saraswat and Dr. R. K. Gupta "A Review of Digital Image Steganography" Journal of Pure and Applied Science & Technology Vol. 2(1), Jan 2012, pp. 98-106