Advanced Steganographic Technique Based on Extended Visual Cryptography Scheme

Harshal S. Tekade[1], Prof. Baisa L. Gunjal[2]
[1](Amrutvahini College of Engineering,Computer Department,Savitribai Phule Pune University,India)
[2](Amrutvahini College of Engineering,Computer Department,Savitribai Phule Pune University,India)

ABSTRACT : *In steganography, a message is hidden in such a way that no one apart from the intended recipient knows of the existence of the message. It is an art of concealing using which we are sending secret message by hiding its content. Steganography is comprised of two algorithms: one for embedding data and one for extraction. Visual cryptography is a technique of secret sharing in which images are distributed as shares in such a faction that, when these share images are superimposed, a message hidden secretly in the image is revealed. In extended visual cryptography (EVC), the share images are constructed to contain meaningful cover images. Unique size of secret images, share images and recovered images is key requirement to improve quality in visual. That way we can maintain the perfect security of the original extended visual cryptography approach.As a part of project, secret text message is encrypted and hide behind the 2 cover images while sharing. At the receiver end message is re-constructed in image form and can be viewed by superimposing the two share images. The reconstructed image is in CAPTCHA form to provide enhanced security. Project is in JAVA Platform. The objectives of the project will be to improve certain image parameters such as Robustness, in order to block unauthorized use, Security of the hidden message and to maintain the Perceptual Quality of the image.*

Keywords *- Steganography, Cryptography, Visual Cryptography, hidden information, image processing, random grid*

I. INTRODUCTION

For secure data transmission over the internet various schemes are proposed like encryption, steganography, visual cryptography. These techniques manipulate information (secret messages) to hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect e-mail messages, credit card information, corporate data, etc.

Encryption [2] is process to convert information to meaningless text using key. Original message can be recovered in decryption phase. Various algorithms are proposed for this technique. These algorithms are mainly categorized in two sections: symmetric key and asymmetric key encryption. In our system we are using symmetric key algorithm [3].

Steganography [4] is the art and science of data communication discovered by Johnson and Jajodia, 1998. It has 2 phases: embedding and extraction. In embedding process, secret message is get hide within a cover image and the extraction process is the inverse of the embedding process, where the secret message is get extracted. Reversible Steganography or Lossless Steganography is the technique of Steganography to disguise information within a digital image in such a way that the cover image can be taken to its original state after extracting the hidden information.

Traditional VC and random grid visual secret sharing methods [5] produces meaningless share images which can create some management problems for those participating in many secret sharing projects because they have to keep track of many secret sharing images. Transmission of a meaningless image can arouse the suspicion of an outsider, who may realize that this image may carry some type of secret message. This attracts attention and could strengthen their desire to uncover the secret image, thus reducing the security of the share-image.

CAPTCHA [6] i.e. Completely Automated Public Turing test to tell Computers and Humans Apart is a technique to challenge the reasons test used to determine whether or not the user is human. Securely shared message is converted to CAPTCHA format to provide security against computerised detection/retrieval of message.

II. LITERATURE SURVEY

Naor and Shamir (1995) proposed a visual secret sharing method, namely visual cryptography (VC), which can encode a secret image into ’n’ noise-like shares [5]. The secret image can be decrypted by the human eye when any ’k’ or more shares are stacked in a sequence. The main advantage of this decryption process is that neither complex computations nor any knowledge about VC are needed. It is very simple and secured secret sharing method for the decoding of secret images when computer-resources are lacking. However, since VC uses a pixel expansion method to decompose the secret image, the sizes of share-images are larger than the original one. The drawbacks of this are wastage of storage space, image distortion and the share-images are difficult to carry.

A probabilistic method [7] is a general and systematic approach to address image quality issues without sophisticated codebook design. To avoid pixel expansion, a set of column vectors are designed to encrypt secret pixels rather than using the conventional VC-based approach. They begin by formulating a mathematical model for the VC construction problem to find the column vectors for the optimal VC construction. A simulated-annealing-based algorithm is proposed to solve the problem. A Visual secret sharing (VSS) scheme [8] which is a perfect secure method that protects a secret image by breaking it into shadow images (called shadows). As far as other threshold schemes are concerned, VSS scheme share can be easily captured by the human visual system without the knowledge of cryptography and cryptographic computations. However, the size of shadow will be expanded. Higher contrast or a smaller shadow size is the current working area VSS schemes.

Unlike in previous studies, multiple pixels are simultaneously encoded each time. Using halftone technique, the methods can be applied to encoding grey-level images [9]. These methods are based on two basis matrices and hence can satisfy the security and contrast conditions required by the VSS scheme. Hou adopted Itos method but utilized multiple successive pixels in the secret image as the unit of encryption. They generated smooth-looking shares of invariant size for gray-level secret images.

O. Kafri and E. Keren [10] proposes a method in which, each pixel of the image is treated as a grid, with a random variable used to encrypt the secret image. The biggest benefit of the RGVSS method for encryption is that it generates unexpanded share-images. Both traditional VC and RGVSS produced meaningless share-images. Such images produce management problems for those participating in many secret sharing projects because they have to keep track of many different share-images. Moreover, transmission of a meaningless image can arouse the suspicion of an outsider, who may realize that this image may carry some type of secret message. This attempt can be suspicious and attracts attention and probability increases to uncover the secret image by malicious user, thus reducing the security of the share-image.

An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS) [11]. A construction of EVCS which is realized by embedding random shares into meaningful covering shares, and they call it the embedded EVCS. It is the first applied the strategy of steganography to generate meaningful share-images in VC.

HVC construction methods [12] based on error diffusion are proposed. The secret image is embedded concurrently into binary share images while these shares are halftoned by error diffusion-the workhorse standard of halftoning algorithms. This works on the clarity of final stack image and it is dealing with halftone images designed to make the recovered stack-image less unclear.

III. PROPOSED SYSTEM

In this section, we introduce 3-tier architecture for our system.

The system can be categorized in 2 sections:

1) Sender section: This is user who what to send secret message behind the image using visual stereographic technique.

Steps:

a) Write Message to be sent.
b) Select 2 cover Images.
c) Divide message in 2 parts.
d) Encrypt message Using Blowfish Algorithm.
e) Hide message behind 2 cover images use DCT technique.
f) Send message to another user.
g) Share key for decryption using secured transaction method.

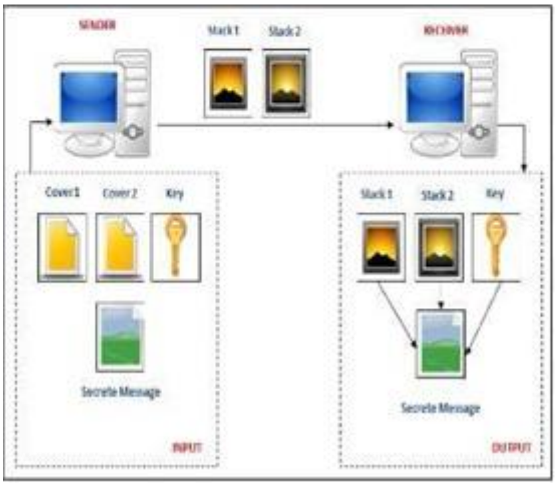

Fig. 1. System Architecture

2) Receiver section: This user receives the data and retrieve messages.

Steps:

a) Download 2 cover images.
b) Extract the encoded message.
c) Add key for decryption.
d) Decrypt data.
e) Apply random font, text size and deviation for each letter to generate CAPTCHA.
f) Generate original message (this message will be in buffer and cannot be accessed directly).
g) Encode this message in 3rd image.

h) Use 2 cover images with this 3rd image, to generate 2 stack images, using visual cryptography technique.
i) Overlap stack images.
j) Display secret message.

3.1 Encryption Technique:

For encryption we are using blowfish algorithm. Blowfish is a symmetric block cipher that can be used for encryption and safeguarding of data. It takes a variable-length key, from 32 to 448 bits, making it ideal for securing data. It is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. A Feistel network is a general method of transforming any function (usually called a Ffunction) into a permutation. The working of a Feistal Network is given below:

1) Split each block into halves
2) Right half becomes new left half
3) New right half is the final result when the left half is XORd with the result of applying f to the right half and the key.
4) Note that previous rounds can be derived even if the function f is not invertible.

Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

Strength of Blowfish technique: Strength of encryption algorithm is based on length of key. Normally 40-bit keys are used for encryption which can be cracked in short time span with computer with average configuration whereas 128-bit key would take one billions of computers to crack it. Blowfish is using 448-bit key which is 2.1 x (10) ^96 time stronger than 128-bit keys from security point of view. Though key is long enough, speed of algorithm is also impressive. Also this algorithm is free and not patented hence it can be clubbed into core product or project idea without permission or licence.

Blowfish Algorithm:

- Blowfish has 16 rounds.
- The input is a 64-bit data element, x.

Steps:

```
1) Divide x into two 32-bit halves: xL, xR.
2) For i = 1 to 16:
       xL = xL XOR Pi
       xR = F(xL) XOR xR
       Swap xL and xR
3) Swap xL and xR again to undo the last swap.
4) xR = xR XOR P17 and xL = xL XOR P18.
5) Recombine xL and xR to get the ciphertext.
```

3.2 DCT for Image Steganography:

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient even knows that a secret message has been sent. We perform steganography using DCT technique.

The Discrete Cosine Transform (DCT) transforms the image from spatial domain to frequency domain. It separates the image into spectral sub-bands with respect to its visual quality, i.e. high, middle and low frequency components. In DCT based techniques, DCT coefficients are obtained for the given carrier image. The secret data is embedded in the carrier image for DCT coefficients lower than the threshold value. To avoid visual distortion, embedding of secret information is avoided for DCT coefficient value 0.

DCT Algorithm:

A. Embedding Process:

Step 1: Select Carrier Image from the set.
Step 2: Find DCT coefficients of Carrier Image.
Step 3: Traverse through each pixel in Carrier Image till end of Secret Image.
Step 3.1: If DCT coefficient value is below Threshold then replace LSB(s) with MSB(s) of pixels in Secret Image.
Step 3.2: Insert 1 at that location in the key matrix.

B. Retrieval Process:

Step 1: Get the Stego Image.
Step 2: Traverse through each pixel in Stego-Image till end.
Step 2.1: Check the key matrix for that location.
Step 2.2: If it is 1, then extract LSB(s) from Stego Image.
Step 2.3: Otherwise move on to next pixel.
Step 3: Get Estimate of Secret Image.

The parameters required on receiver side for retrieval of secret image from stego image are:

- Number of bits replaced in carrier image.
- Number of bits stored for secret image data.
- Size of Secret Image.
- Key matrix.

These parameters are transmitted separately through predefined means. They are useful to retrieve the hidden secret information and without these parameters, extraction of secret image from given stego image is not possible.

3.3 Visual Steganography:

Whether the colour on the secret image is white or black, the pixels on the share-image will have X% chance of appearing black in the area corresponding to white in the cover-image; likewise, the pixels on the share-image will have Y% chance of appearing black in the area corresponding to black in the cover-image. Thus, no clues about the secret image are exposed in the share-image, and the pattern of the cover-image that emerges on that share-image has a contrast of (Y - X). The area in the stack-image corresponding to white in the secret image has Z % black pixels in the stacked image, while the area corresponding to black in the secret image can be stacked to have W% black pixels. Therefore the contrast in the stack-image is (W - Z), enough to reveal the secret pattern. The colour in the stack-image is only related to the colour of the secret image, not the cover-image, so the pattern of the secret image shows no outline of the cover-image.

In this technique, the black-appearing-probability is utilized to analyse changes in chromaticity in the share-image and the stack-image. An area with pixels assigned a higher probability of appearing black has a higher density of black pixels, making this area look darker. On the other hand, when the probability is low, the density of black pixels in this area is also low, and the area looks lighter. With these two different probabilities, we can produce light and dark contrast in the image, that is, show a black and white pattern.

Visual Secret Sharing Algorithm:

The user-friendly visual secret sharing algorithm:

INPUT: An LxH secret image P, two LxH cover-images C1 and C2, and probability parameters X,Y,Z and W, where 0<X <Y<=Z<W<=2X<=1.
OUTPUT: Two LxH share-images S1 and S2.
Step 1: Read the pixel colour of P (i, j), C1 (i, j) and C2 (i, j) sequentially, to judge what the combination is.
Step 2: Based on the combination, assign S1 and S2 an appropriate black-appearing-probability.
Step 3: Repeat steps 1 and 2 until all the pixels of P are encrypted.

3.4 Mathematical Representation:

Description:

S= I, O, F

I = I1, I2, I3, I4
I1 = Message to hide
I2 = Cover Image1
I3 = Cover Image 2
I4 = Key

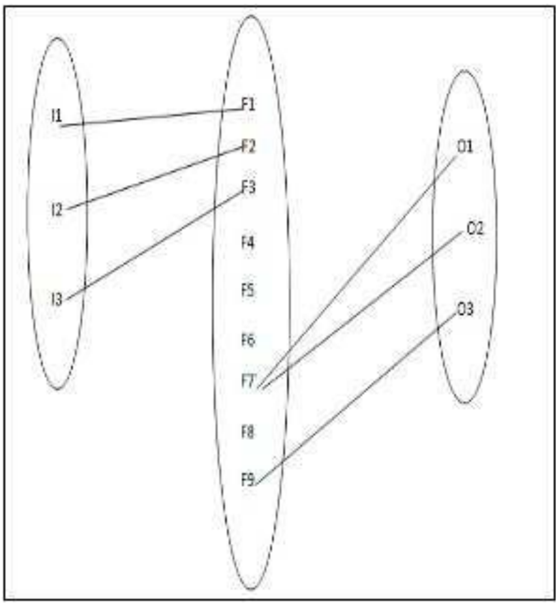

Fig. 2. Mathematical Representation

O = O1, O2, O3
O1 = Stack Image 1
O2 = Stack Image 2
O3 = Decrypted Message

F = F1, F2, F3, F4, F5, F6, F7, F8, F9
F1 = Encryption
F2 = Steganographic hiding
F3 = Image Resizing
F4 = Pixel Probability calculation
F5 = Chromaticity setting
F6 = Generation of stack image
F7 = Print stack image
F8 = Steganographic Message extraction
F9 = Decryption of Message

IV. CONTRIBUTION

As per [1], two shared images are used to hide particular image. These shared images are sent to receiver directly. If these shared images are recovered by third untrustworthy party then original image can be traced. In this process direct shared image transfer to receiver generate security issue. Also as shared images are generated at sender side it generates halftone images which tends to lacking in image quality. Issues like image quality and security are handled effectively as part of contribution. As per contributed flow, text is hidden behind cover images. From security point of view this text is split into two parts and then encrypted. Both encrypted part of text is then hiding behind two shared images. These shared images are sent to receiver. Now though shared images are traced by untrustworthy party, process of recovery of original text is not possible. When expected receiver receives these shared images, he can extract hidden text out of it using decryption key. Extracted and decrypted text is then converted into CAPTCHA and using the concept of visual cryptography, this CAPTCHA is hidden behind two received shared images. Hence user can read this text by overlapping these shared images. This process achieves two level securities and image quality issue is solved because visual cryptography process is done at receivers end.

V. CONCLUSION

We provide secret sharing scheme by integrating text cryptography steganography and visual cryptographic technique. CAPTCHA technique is used to display secret message. Sender shares 2 meaning full images. A message is hidden in these images. The embedding and extraction process is not at all a time consuming process. Our project generates user friendly GUI to deal with this technique. Generated stack images are easy to manage and carry from sender to receiver using any electronic media. Our technique provides more security, robustness. Random grid technique provides pixel non-expanding benefits. Image quality is improved than previously proposed techniques using sharpness and edge detection technique.

In future we will implement this technique on natural coloured images rather than halftone images and will work on improvement of image quality of extracted secret message.

VI. Acknowledgements

I avail this opportunity to thank all those people who helped me in making this paper and the project. I would like to express my respect, deep gratitude and regards to Prof. B. L. Gunjal for her support that helped and enlightened me in every possible way. I am indebted to her for bringing order to this report out of the chaos that was many times presented to them.

REFERENCES

[1] Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin, Visual cryptography Random-grid-based Visual Cryptography Schemes, in *IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 1 part 2,* 2014, pp. 733-744.

[2] Monika Agrawal and Pradeep Mishra, A Modified approach for Symmetric Key Cryptography Based on Blowfish Algorithm, in *International Journal of Engineering and advanced Technology (IJEAT), vol. 1, no. 6,* 2012.

[3] MD Asif Mushtaque, Shahnawaz Hussai, Harsh Dhiman, Shivangi , Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity, in *International Journal of Engineering Research and Technology (IJERT) vol. 3, no. 4 part 2,* 2014.

[4] Suchitra. B and Priya. M, Raju.J , Image Steganography Based On DCT Algorithm for Data Hiding, in *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) , vol. 2, no. 11 ,* 2013.

[5] Moni Naor and Adi Shamir Visual Cryptography, *Lecture Notes in Computer Science Volume 950, pp 1-12,* 1995.

[6] Luis von Ahn, Manuel Blum, Nicholas J. Hopper and John Langford, CAPTCHA: Using Hard AI Problems for Security, *Watson Research Center, Yorktown Heights NY 10598,* USA.

[7] R. Ito, H. Kuwakado, and H. Tanaka, Image size invariant visual cryptography, IEICE Transactions on Fundamentals of Electronics, *Communications and Computer Sciences, vol. E82-A, no. 10,* 1999, *pp. 2172- 2177*.

[8] C. N. Yang, New visual secret sharing schemes using probabilistic Pattern Recognition, *Letters, vol. 25, no. 4,* 2004, pp. 481-494.

[9] S. F. Tu and Y. C. Hou, Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images, *Imaging Science Journal, vol. 55, no. 2,* 2007, pp. 90-101,.

[10] O. Kafri and E. Keren, Encryption of pictures and shapes by random grids, *Optics Letters, vol. 12, no. 6,* June 1987, pp. 377-379.

[11] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Extended schemes for visual cryptography, *Theoretical Computer Science, vol. 250,* 2001, pp. 143-161.

[12] Z. Wang, G. R. Arce, and G. D. Crescenzo, Halftone visual cryptography via error diffusion, *IEEE Transactions on Information Forensics and Security, vol. 4, no. 3,* 2009, pp. 383-396.