ISSN No: - 2456 - 2165

A Novel Technique of CVC to improve the Security of Steganography

K. Sonika Priya[1], T. Madhavi Kumari[2]
[1]M. Tech student, [2] Associate Professor
Department of ECE, JNTUHCEH, Hyderabad, India
sonikapriya.saffron@gmail.com

Abstract- Steganography is a technique of hiding one message(secret) in another(cover) for secret communication. It is best way to conceal secret data without revealing its existence to the outsider. Today, this method is more in light than ever, hence increasing the informational security of Steganography is more than necessary to protect the secret information. In this paper we first do the cryptography of the image before embedding it in the cover image.

Keywords*-Steganography, Visual Cryptography, Chaotic Maps.*

I. INTRODUCTION

Cryptography is an art that applies complex mathematics and logic so as to design strong encryption methods to protect the secret data. Cryptography allows people to keep confidence in the electronic world. Cryptography of images has its own importance because of the increasing use of electronic signatures or e-signatures. Encryption Schemes over images have been drastically increased to meet the demand of secure image transmission over various medium such as Wired and Wireless Network. DES encryption standards show low efficiency over image encryption and have less impact on efficiency when the size of image is huge. Hence here image is encrypted using chaotic maps.

Steganography is the technique of communicating using hidden messages, often disguised within something else(such as an image) where one would not expect a message to be hidden in. Generally steganographic messages will appear ordinary at first glance: an image of a cat, a grocery list, an article or poem, etc. Hidden within these ordinary looking images or objects (in steganographic terms, the cover text/image) is the hidden message.

The difference between steganography and cryptography is that in cryptography, one can tell that a message has been encrypted(since he can see the encrypted form of the message), but he cannot decode the message without knowing the proper key. In steganography on the other hand, the message itself may not be difficult to extract, but most people would not detect the presence of the message. When combined, steganography and cryptography can provide two levels of security to the message.

II. LITERATURE SURVEY

A. Steganography

Today Steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Although it is related to cryptography, they are not similar. Steganography and cryptography are techniques used to protect information from third parties. Steganography alone is not perfect. Once the presence of hidden information is revealed or suspected, there is no use of Steganography. The strength of Steganography will increase by combining it with cryptography.

The techniques of Steganography have been categorized into

i. Spatial domain Steganography

It mainly includes LSB technique in which the least significant bit of the pixels of the cover image are replaced with bits of secret information. Spatial domain is frequently used because of its easy realization.

ii. Transform domain Steganography

The secret bits are embedded in the transform image of the cover image. Examples of transform domain Steganography are Discrete Cosine Transform, and Discrete Wavelet Transform.

Steganography is used in a wide range of applications such as defence organizations and intelligence agencies for safe circulation of secret data, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials.

B. Visual Cryptography

Visual Cryptography is an encryption technique that is used to encrypt images. In this two shares(which are also images) are produced. The original image can be obtained by overlaying these two transparent shares. One of the shares is called the encrypted image and the other share is called the key image. One image contains random pixels and the other image contains the secret information. It is not possible to retrieve the secret information from one of the

images. Both images are required to reveal the secret information. The technique was proposed by Naor and Shamir in 1994.

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks.

If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

In this paper we are using the Chaotic map as layer 1 which has true randomness. We encrypt the secret image with this chaotic map and hence we call it Chaotic Visual Cryptography(CVC).

C. Chaotic Maps

A chaotic map is a map exhibits some sort of chaotic behaviour. Maps may be parameterized by a discrete-time or a continuous-time parameter. Discrete maps usually take the form of iterated functions.

Chaotic sequences have many useful properties in security based applications. Firstly, they are easy to generate. Second, a chaotic signal is deterministic, not random, which allows us to regenerate it. This is fundamentally different from random sequences, since a random process is non-deterministic, and two successive realizations of a random process will give different sequences, even if their initial states are the same. But the output of the chaotic sequence is the same if the initial conditions are same. Third, a chaotic signal is extremely difficult to predict because of the high sensitivity of the secret key. A slight difference of the secret key will result in an entirely different chaotic sequence, which make it extremely difficult for attackers to regenerate it. Thus, the level of security is improved.

Here we are generating a chaotic map using a one dimensional logistic map. One dimensional Logistic map is described as

$$x_{k+1} = rx_k(1-x_k) \quad ....(1)$$

Where,

the system parameter r €[0, 4] and initial condition x €(0,1). The logistic map behaves randomly with r € (3.5699456, 4] where "(" and "["denotes to open and closed intervals .

Here r and x_0 are considered as keys for the Chaotic Visual Cryptography and their range is x €(0,1) and r € (3.5699456, 4].

III. PROPOSED METHOD

In the proposed method a chaotic sequence is used to generate one of the shares in visual cryptography with the objective of enhancing its resistance against attacks. We can produce this share with parameter "r" and initial condition "x_0", (r and x_0 are keys of the cryptographic algorithm) and reconstruct the secret image by combining this share to the one obtained from the stego image. In this paper, the Logistic map is used to generate the chaotic sequence. For embedding, the transform domain technique is used because it more robust to attacks.

A. At transmitting end

Step1: Input: Secret image, Keys "r" and "x_0" for generation of chaotic map

Output: Encrypted image;

Pixels of the chaotic share = C(i) mod 2; Encrypted image is produced by taking XOR operation between the chaotic map and the secret image

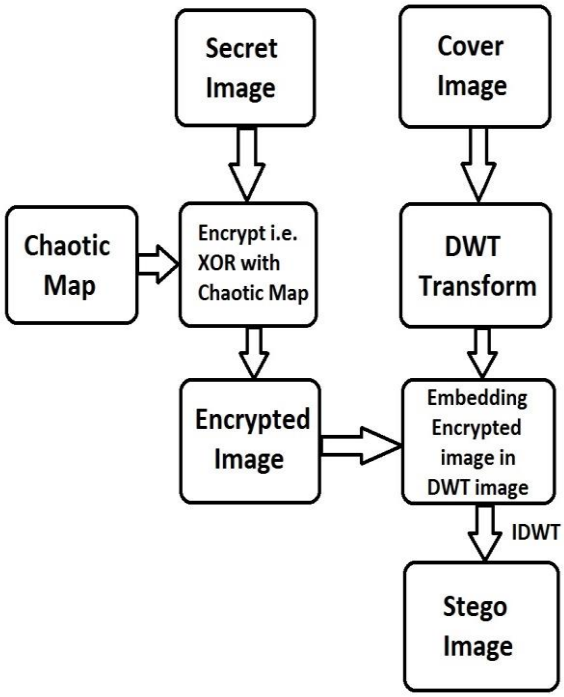

Fig.1(a) Secret Image Embedding

ISSN No: - 2456 - 2165

Step2: Input: Encrypted image, cover image;

Output: stego image;

Apply transform technique to the cover image; Encrypted image is embedded in transform coefficients of the cover image; The stego image is obtained by applying the inverse of that transform image;

B. Extraction

Step1: Input: stego image;

Output: Encrypted image;

Apply transform technique to the stego image; Encrypted image is extracted from the transform coefficients of the stego image;

Step2: Input: Encrypted image, Keys "r" and "x_0" for generation of chaotic map;

Output: secret image;

Chaotic map is produced by the chaotic sequence; The secrete image is produced by taking XOR operation between chaotic and complement shares;

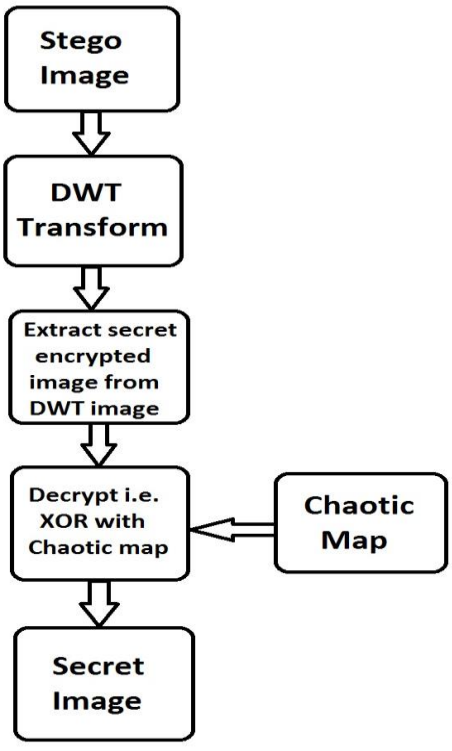

Fig.1(b) Secret Message Extraction

IV. RESULTS AND ANALYSIS

The following image shows the images at different stages of the algorithm. Resizing of the secret image is done so that it can be embedded in the secret Image. The keys used for chaotic map are x=0.5 and r=3.968

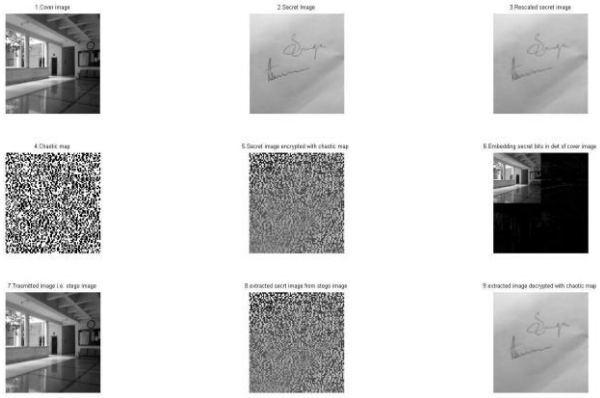

Fig.2 Result of the DWT Algorithm. Both Encryption and Decryption.

The following is the analysis used to rate the performance of steganographic and cryptographic techniques

A. Imperceptibility

Imperceptibility is usually calculated by Peak Signal-to-Noise Ratio (PSNR). When the difference between the cover image and stego image is small, PSNR increases.

For the images used in the above result the PSNR values for LSB method and DWT method are as follows
LSB PSNR=51.1583dB
DWT PSNR=33.2524dB

B. Capacity

Capacity of the steganographic algorithm is determined by the number of secret bits that can be embedded in each cover pixel. With increase in the capacity the PSNR value decreases. Decrease in PSNR value means more deviation of the stego image from the cover image. Hence capacity should be chosen keeping in mind the PSNR value. The following tables show the PSNR values for different capacities for LSB and DWT methods.

Table 1(a) Capacity and PSNR for LSB method

Capacity	PSNR(dB)
1-bit	51.1583
2-bits	43.2518
3-bits	36.0362
4-bits	29.5564
5-bits	23.176
6-bits	16.6384
7-bits	10.9777
8-bits	6.7171

ISSN No: - 2456 - 2165

Table 1(b) Capacity and PSNR for DWT method

Capacity	PSNR(dB)
1-bit	33.2524
2-bits	32.85
3-bits	31.3667
4-bits	27.8797
5-bits	22.7513
6-bits	16.4887
7-bits	11.1473
8-bits	6.6747

C. Histogram analysis

Histogram analysis is one of the important criteria in security analysis. If the histogram of the image being more uniform, the security for the encrypted message is more guaranteed.

For the chaotic map generated using x_0=0.5 and r=3.9 the number of white pixels and black pixels is shown below. Which means the histogram is nearly uniform.

White Pixels	Black Pixels
14628	10972

The histogram of enrypted image is as follows.

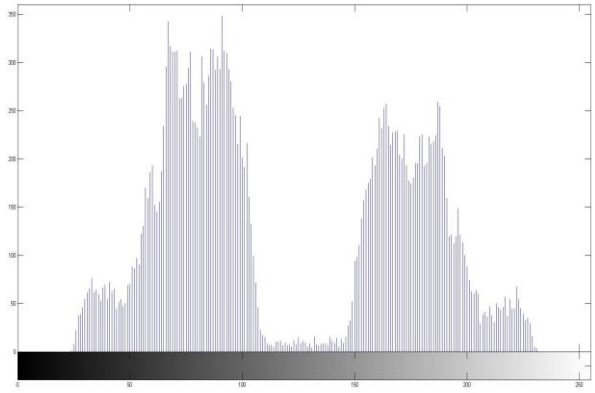

Fig.3 Histogram of encrypted Image

D. Correlation Coefficient

Correlation coefficient indicates the statistical relationship between two images. Whatever the correlation coefficient values of pixels getting near to zero, the resistant of algorithm against the statistical attacks is increased.
The correlation coefficient for the secret image used and the encrypted image is 0.0544 which means the secret image is not at all related to encrypted image and the information is safe.

E. Key space

To have a secure encryption method, the key space should be large enough to make the brute-force attack infeasible. For the chaotic map to behave randomly the initial conditions x and r should be in the range of x €(0,1) and r € (3.5699456, 4]. If the key size is taken as 128 bits each then considering their range the key space will be $2^{127+126}=2^{253}$ which is enough to avoid brute force attacks from today's computers.

F. Key sensitivity

Key sensitivity is one of the important criteria in image encryption algorithms. First the secret image is encrypted using two keys r and x_0. Now a very small change is made to r and x_0 and the encrypted image is decrypted using this. It was observed that a small change in the keys led to a significant change in the decrypted image. The following image shows the key sensitivity of the algorithm.

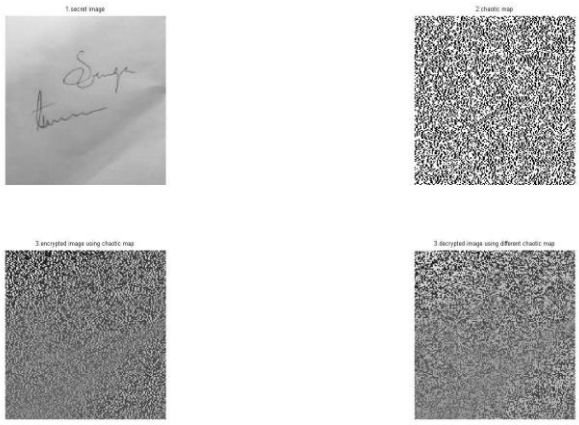

Fig.4 (3) is the secret image encrypted with x=0.4 and r=3.956 and (4) is the decrypted image using x=0.400001 and r=3.95600001

V. CONCLUSION

The proposed algorithm hides one secret image into another innocent-looking image. The innocent-looking image draws less attention from the attackers. Also, a chaotic visual cryptography algorithm is proposed to generate one share based chaotic sequence and another share produced by the taking an XOR between the chaotic share and the secret message. Since the employed chaotic system has high sensitivity to its keys, no one can easily guess these parameters, even by using a brute force attack accessing to a strong processor. Using Chaotic visual cryptography increases the security level of Steganography. The proposed scheme all in all is an easy and robust method.

REFERENCES

[1] Melika Mostaghim , Reza Boostani, *" CVC: Chaotic Visual Cryptography to Enhance Steganography"* Information Security and Cryptology (ISCISC), 2014

[2] Himanshu Sharma , Neeraj Kumar, Govind Kumar Jha, *"Enhancement of security in Visual Cryptography system using Cover Image share embedded security algorithm*

ISSN No: - 2456 - 2165

(CISEA)" International Conference on Computer & Communication Technology (ICCCT)-2011.

[3] J.K. Mandal, S. Ghatak, *" Secret Image / Message Transmission through Meaningful Shares using (2, 2) Visual Cryptography (SITMSVC)"* IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.

[4] Saravanan Chandran, Koushik Bhattacharyya, *" Performance Analysis of LSB, DCT, and DWT for Digital Watermarking Application using Steganography"* International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) - 2015.

[5] M. Naor and A. Shamir, *"Visual Cryptography"*, In Proceedings of Advances in Cryptology-Eurocrypt, Springer-Verlag, pp. 1–12, 1995.