Security Enhanced Visual Cryptography Scheme with Cheating Prevention Ability

Biltta P George
PG Student/ Department of CSE
Adi Shankara Institute of Engineering and Technology, Kalady
MG University, Kerala

Deepika M P
Asst. Prof / Department of CSE
Adi Shankara Institute of Engineering and Technology, Kalady
MG University, Kerala

Abstract—**Visual Cryptography (VC) is an encryption technique to encrypt a secret image into transparent shares such that stacking an enough number of shares reveals the secret image without any complex computation. In the existing visual cryptographic scheme the dealer or sender takes a secret image and encodes into shares. After encoding this shares are sent to participants. The receiver collects the shares and stack to get decoded secret image. here no verification is done. During share reconstruction phase the dishonest participant or dealer may submit fake shares instead of genuine shares. As a result fake image will be revealed. So effortless cheating is possible. To attain cheating prevention in VC a steganographic scheme is used to embed a secret message in each of the shares in random location during share generation phase called stego share. The security is enhanced by embedding each of these stego shares in cover work using LSB technique. At the time of recovery LSB extraction technique is required to decode the shares from cover and a message extraction technique is required to retrieve the text from share, which prevent cheating and check the originality of the share. And then use visual cryptography to reveal the original visual information by stacking the shares. The proposed visual cryptography scheme provides cheating prevention ability as well as improved security.**

Index terms - visual cryptography, cheating prevention, steganography, stego share

I. INTRODUCTION

Now a day the transmission of secret information through computer network has increased rapidly. So the security concerns of secret information have also grown proportionally. Confidentiality is probably the most common aspect of information security and need to protect valuable information from unauthorized access. It has become an inseparable issue as information technology which ruling the world now. In recent years there has been a rapid growth of information technology for human to communication on the internet. Since internet is public, anyone can easily read the information and perform successful transmissions without protection. In order to avoid sensitive information being illegally read or modified, the information must be encrypted before transmission. To protect information Cryptography plays an important role in this issue.

Cryptography & Steganography are the traditional method of providing security to the secret information. In 1994 Naor & Shamir [1] proposed a new method called as visual cryptography for providing security to the secret information. In VC Scheme the secret data splits into two or many shares, each of which individually cannot provide any information about the secret data. The secret data can be only retrieved when the desired numbers of shares are superimposed with one another. During decryption the shares are needed to be printed out in a transparency sheets/papers and needs to stack all or desired number of transparencies with each other that reveals the secret information. Therefore, it does not require any complex calculation as like other traditional cryptography schemes.

Steganography [3] is an art of hiding information inside another data. The main objective of steganography is to guard the contents of secret information. In this technique, secret information is communicated through unknown carrier data. The embedding of secret information is done in such a manner that the very existence of the secret information is invisible to any viewers. Carriers` data could be many forms such as images, audio, video, text any other data. In steganography, the image media are most popular as a carrier/cover data because of the existence of large number of redundant bits in it. The hidden information may be text, cipher text or any other digital form that represented as a bit stream can be embedded using steganography technique.

The Visual Cryptographic Schemes suffer from cheating where cheaters can submit false share during secret reconstruction. The cheating prevention ability is achieved in our scheme by checking the genuinty of the shares before secret reconstruction phase. The security is increased by using LSB technique [11].

II. RELATED WORK

A. *Visual Cryptography*

Visual cryptography was originally developed and established by Moni Naor and Adi Shamir in 1994 at the Eurocrypt conference [1].It involved breaking up the image in to 'k' shares so that only someone with all k shares could decrypt the image by superimposing each of the shares over each other. A share consists of m black and white sub-pixels. The structure can be described as an $n \times m$ Boolean matrix *S*. The structure of *S* can be described thus: $S = (s_{ij})\ m \times n$ where $s_{ij} = 1$ or 0.If the j^{th} *subpixel* of the ith share is black or white.

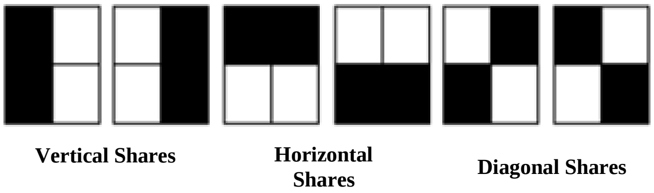


Figure-1: Pixel encoding in (2, 2) VCS

B. Cheating in Visual Cryptography[2]

Most cheating attacks in VC are known plaintext attacks where the cheaters know the secret image and are able to infer the blocks of victim's transparency based on the base matrices. It is observed that cheating is possible in (k, n) VC when k is smaller than n. There are two types of cheaters in VC. One is a malicious participant (MP) who is also a genuine participant, namely MP € P (Qualified participant) and the other is a malicious outsider (MO), where MP € P.

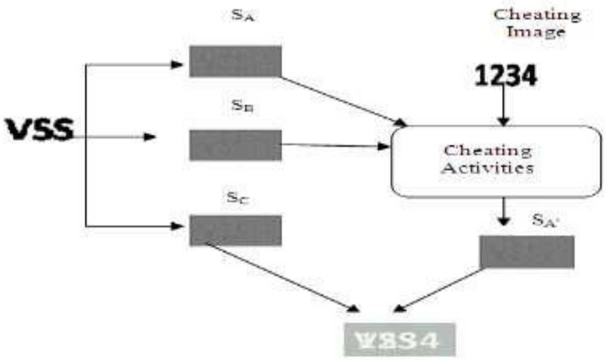


Figure-2: Cheating in Visual Cryptography

A cheating process against a VCS consists of the following two phases[4] :
1. Fake share construction phase: the cheater generates fake shares.
2. Image reconstruction phase: the fake image appears on the stacking of genuine shares and fake share.

Most of the Visual Cryptography schemes have the property of perfect blackness. Some of common ways how MO and MP cheat visual cryptography are[4]:

1) Cheating a VC by an MP
2) Cheating a VC by an MO
3) Cheating an EVCS by an MP

1. Cheating a VC by an MP (CA-1)

A qualified participant can also be a cheater, where the member creates a fake share image by using his original share images. By doing so, he will try to cheat the other genuine members because the fake share generated will be indistinguishable from the original share images and also the decoded output image will be different from the original secret image.

2. Cheating a VC by an MO (CA-2)

An ineligible member called as MO will create fake shares by using some random images as input and will try to decode the original image. The MO will try to create fake shares of different sizes because the size of the original share may vary.

3. Cheating an EVCS by an MP

The Qualified member creates the fake share from the genuine share by interchanging the black pixels by the white pixels which leads to less contrast of the recreated image. The less contrast in reconstructed image will be hard to see the image. The fake image in the stacking of the fake shares has enough contrast against the background since the fake image is recovered in perfect blackness.

In the case of cheating, honest participants who present their shares for recovering the secret image are not able to differentiate fake shares from genuine shares. A reconstructed image is a perfect image indistinguishable from the original. Figure 2.shows the whole cheating process and Table 1.shows how the cheaters create fake shares to change the decoded image

Pixel in secret image	**Pixel in Share S_A**	**Pixel in Share S_B**	**Pixel in Share S_C**	**Pixel in Cheating Image**	**Pixel in Share $S_{A'}$**	**Pixel in Share $S_{B'}$**
white	[100]	[100]	[100]	white	[100]	[100]
white	[100]	[100]	[100]	black	[010]	[001]

black	[100]	[010]	[001]	white	[001]	[001]
black	[100]	[010]	[001]	black	[100]	[010]

Table-1: Fake Share Pixel Creation for 2 out of 3 VC [2]

C. Cheating Prevention Schemes

Many studies focused on the cheating problems in VCS, and subsequently many cheating prevention visual cryptography schemes (CPVCS) have been suggested. Cheating prevention schemes of visual cryptography were briefly discussed in [12]. We classify the techniques in these CPVCSs as follows:

1. Make use of an online trusted authority who can verify the validity of the stacked shares [15],[17]
2. Generate extra verification shares to verify the validity of the stacked shares.[17],[4]
3. Expand the pixel expansion of the scheme to embed extra authentication information.[5]
4. Generate more than *n* shares to reduce the possibility that the cheaters can correctly guess the distribution of the victim's shares.[2]
5. Make use of the genetic algorithm to encrypt homogeneous secret images. [24]

By examining the above techniques, we found that the first technique is not practical in real applications, because the beauty of VCS is its simplicity, which is meant to be useful even when no computer network is available. The second technique requires the extra verification shares, which unsurprisingly increases the burden of the participants. The third and fourth techniques increase the pixel expansion and reduce the contrast of the original VCS [7].The fifth technique requires strong computational overhead and reduces the quality of the recovered secret image, where the secret image can only be a password.

III. PROPOSED SCHEME

In the proposed scheme a steganographic scheme is used for cheating prevention. Steganographic schemes are most commonly divided into two spatial domain technique and transform domain technique [9]. In the spatial domain, the secret message is embedded in the image pixels directly. In the frequency domain, however, the secret image is first transformed to frequency-domain, and then the message is embedded in the altered domain. In our proposed scheme spatial domain technique is used.

In this system mainly two modules are present. First one is encryption module. For encryption (n, n) visual secret sharing scheme is used. The input image is split in to 'n' shares and distributed among 'n' participants. Then a secret message is embedded into each share. As a result stego shares are generated. Every participant must be aware of this secret message which is used for authentication purpose. Then conceal these stego shares into cover image.

In the decryption module the receiver first take out the stego shares from cover work, check the embedding information within share for authentication then retrieve the secret information by stacking the share. If the extracted secret message is matched with that of the original message, the secret image will be revealed otherwise detection of the fake share is performed. In this system secrecy can be distributed among 'n' participants and all participants can verify the share by secret message but outsider cannot suspect about the message transmission as well as message sharing among group of people.

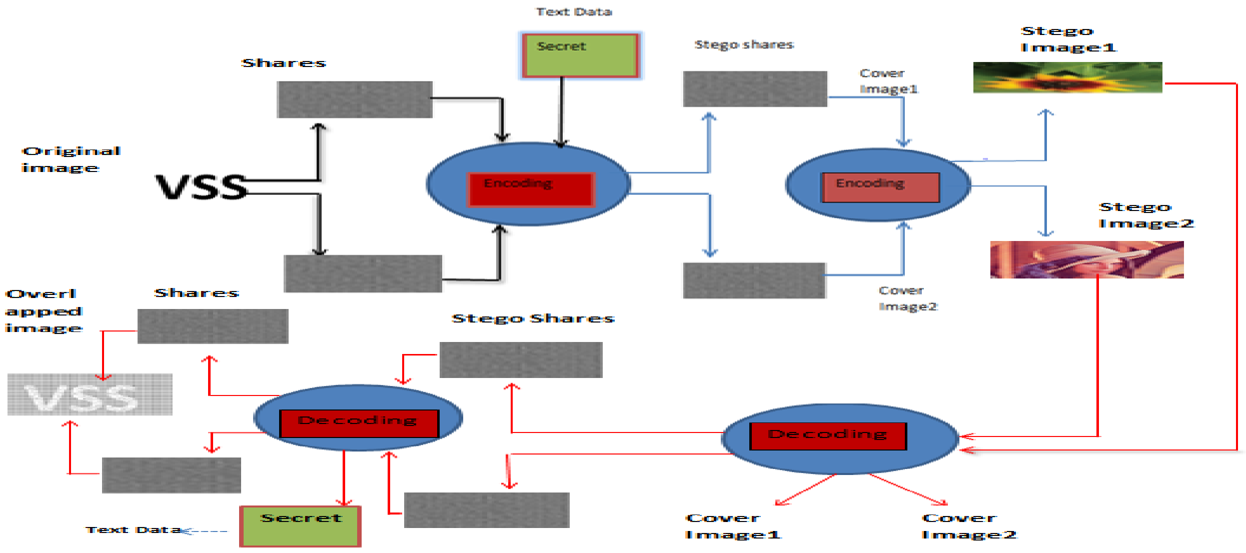


Figure -3: Proposed Encoding and Decoding Scheme

Algorithm1: Generation of shares using secret image

1. The share generation and distribution are performed by the dealer.
2. To generate shares of an image for members, we want to prepare two collections, K_0 and K_1, which consist of n x m Boolean matrices.
3. A row in a matrix K_0 and K_1 corresponds to m sub pixels of a pixel, where 0 denotes the white sub pixels and 1 denotes the black sub pixels.
4. For a white (or black) pixel in the image, we randomly choose a matrix M from K_0 (or K_1, respectively) and assign row i of M to the corresponding position of share Si, 1<= i<= n.
5. Each pixel of the original image will be encoded into n pixels, each of which consists of m sub pixels on each share. Since a matrix in K_0 and K_1 constitutes only one pixel for each share.

Algorithm2: Fake share Generation

1. For the fake share construction the inputs are the original share S1 and a fake image FI, which has the same size of secret image.
2. Assume that each pixel of S1 has X black and Y white sub-pixels.
3. For each white pixel of the fake image FI, copy the corresponding sub-pixels of the pixel in S1 to fake share FSI'.
4. For each black pixel of the fake image F, randomly assign X black and Y white sub-pixels to fake share FIS1, such that the pixel in the stacking of fake share FIS1‟ with original share S1 is perfect Black.
5. Generate fake share FS1'.

Algorithm3: Embedding secret message (Stego Shares Generation)

1. Input: Four shares S1, S2, S3, S4 and secret message SM.
2. Convert the ASCII value of each word in secret message in to corresponding binary values.
3. Calculate the locations at which the message is to be embedded within shares using pseudo random number generator (PRNG). PRNG (K) that means it generates a sequence of number which is depending on K.
4. Copy each location in the message (binary form) in to the corresponding locations in the shares. The dealer is the exact person who decides where embeds each word in the message within the shares.
5. Generate the four stego shares SS1,SS2,SS3,SS4

Algorithm4:Algorithm for adding cover images (LSB technique)

```
Input: cover image, Stego Shares (Shares+ Secret Message)
    Procedure:
    Step1: Consider the bit stream in the stego shares (Length L)
    Step2: Generate L number of pseudo random number using seed key
    Step3: Calculate the non-collide L pixel positions in the cover image
    Step4: while complete bit stream not embedded
      {
        Replace LSB of pixel denoted by i^th pixel position, with secret bit insert pixel into cover image
      }
    End
    Output: Stego-image (stego shares concealed in the cover image)
```

On the receiver side, first of all the pixel positions are calculated in the same way with the use of the same key. Then secret bit-stream is formed by the LSBs of these pixels. The Extraction algorithm is as below:

Algorithm 5: LSB Extraction Algorithm

```
Input: stego-image, key

  Procedure:
  Step1: Consider the bit stream in the stego shares (Length L)
  Step2: Generate L number of pseudo random number using seed key
  Step3: Calculate the non-collide L pixel positions in the cover image
  Step4: for i=1 to L
  {
    Get lsb of pixel denoted by i^th pixel position append this lsb into secret bit stream
  }
  Step5: Extract the stego shares from stego image
  End
  Output: stego shares
```

Algorithm6: Extraction of Secret message

1. Consider the 4 stego shares SS1,SS2,SS3,SS4 seed value K generate locations (these locations are same as the locations used for embedding messages)
2. Then using PRNG ,extract message embedded within the shares

Algorithm 7: Algorithm for checking shares

1. Consider the secret image SM[x][y] and 4 stego shares SS1,SS2, SS3,SS4.
2. Create a transformation matrix SM1[y][x] corresponding to the secret image SM[x][y]
3. Then message is extracted using algorithm-6,extract message SM'
4. Then generate a transformation matrix SM2[y][x] of SM'[x][y]
5. Check SM1[y][x]==SM2[y][x] if it is true make sure that all the shares are genuine
6. Otherwise the particular share is fake

IV. RESULTS AND DISCUSSIONS

In the proposed system a secret message is embedded within the original shares in some random location using PRNG, when the participants submit their shares a checking is done to check the secret embedded message. If the message is found to be matched then it is the original share and if it is not the same message found then the system confirm that it is a FS.

Distortion is measured by means of two parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The MSE is calculated by using the equation,

$$MSE=\frac{1}{MN}\sum_{i=1}^{m}\sum_{j=1}^{n}X_{i,j}\text{-}Y_{i,j}\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

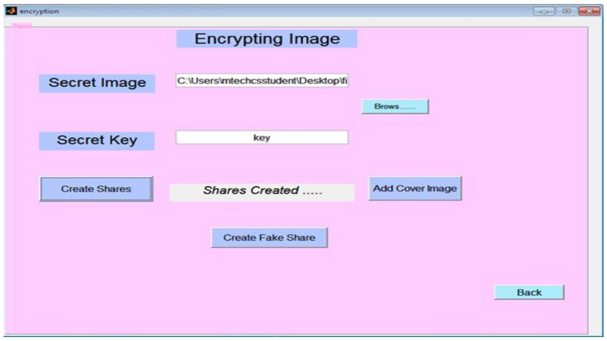
Where M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image $X_{i:j}$ represents the pixels in the original image and $Y_{i:j}$, represents the pixels of the stego-image.

The PSNR is calculated using the equation,

$$PSNR=10\log_{10}\left(\frac{I_{max}^{2}}{MSE}\right)dB\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Where I_{max} is the intensity value of each pixel which is equal to 255 for 8 bit gray scale images. Higher the values of PSNR better the image quality. Distortion Analysis of stego share gave the good results. The analysis in terms of PSNR of original share and stego share has given promising result. It has been found that the PSNR value of the proposed scheme is near to 70.

V. EXPERIMENTAL RESULTS



Secret Image: C:\Users\mtechcsstudent\Desktop\fi

Secret Key: key

Figure-4: Encryption Module(secret key is used as secret message)

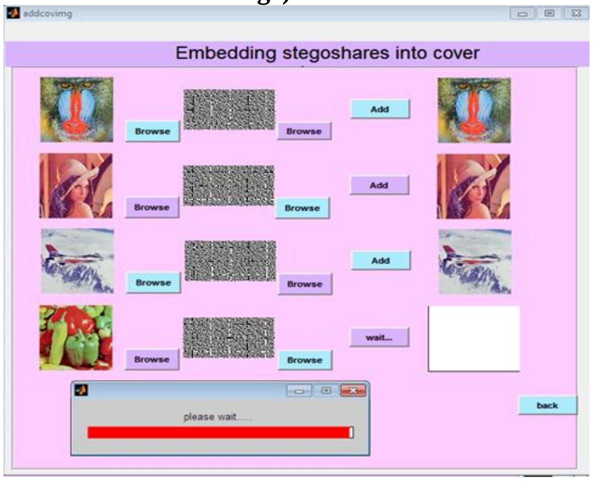
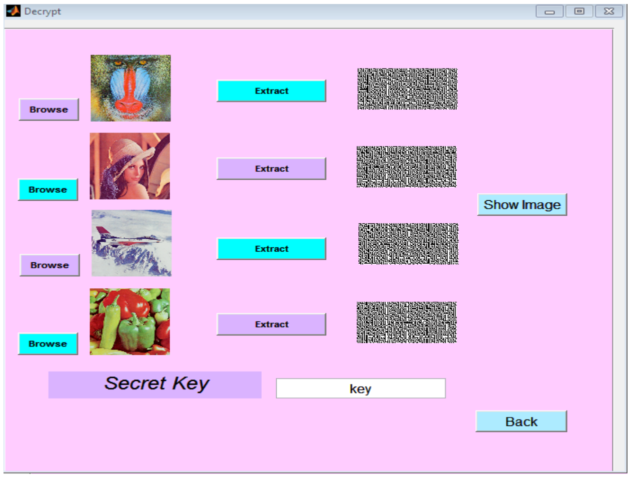


Figure-5: Embedding stego shares into cover work



Secret Key: key

Figure-6: Decryption Module

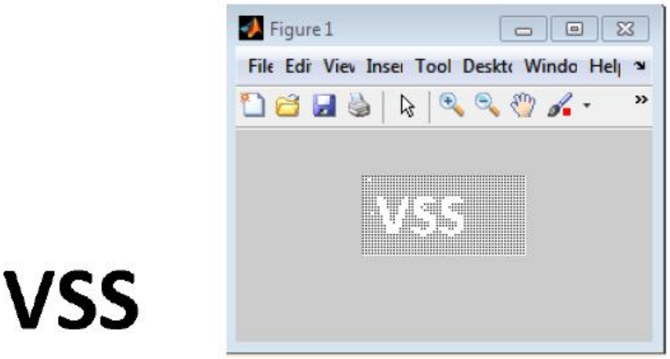
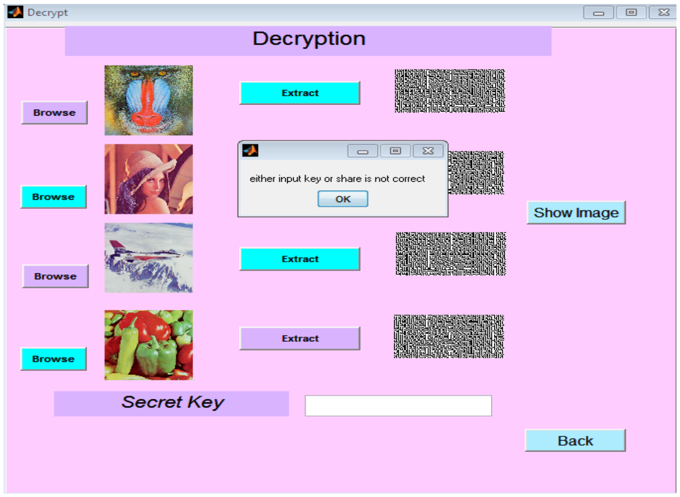
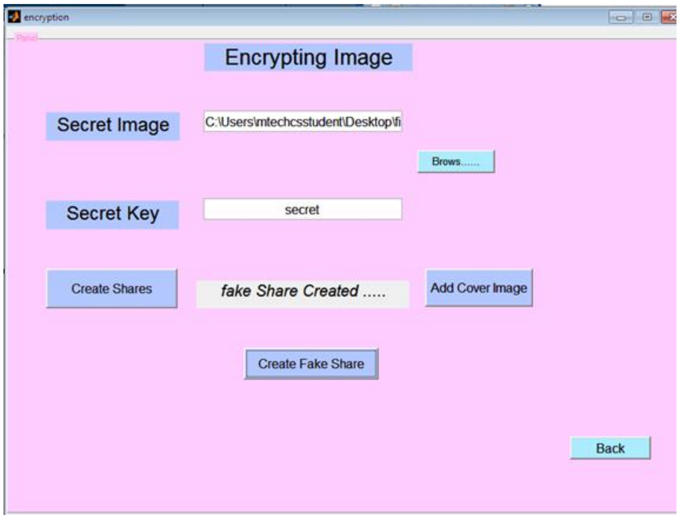


Figure-7: Input image &Resultant Image



either input key or share is not correct

Figure-8: Authentication

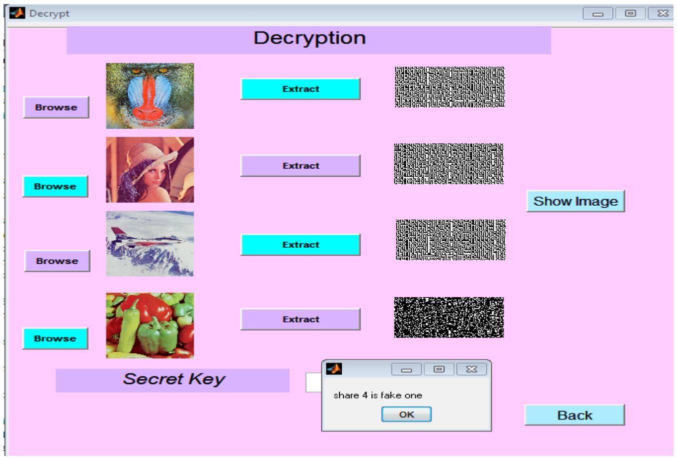


Secret Image: C:\Users\mtechcsstudent\Desktop\fi

Secret Key: secret

fake Share Created .....

Figure-9: Fake share creation



share 4 is fake one

Figure-10: Fake share detection

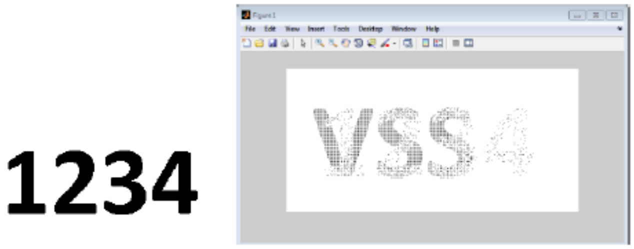


Figure-11: Input for fake share creation& Generated fake image

VI.CONCLUSION

In this research work, we have developed a security enhanced visual cryptography scheme with cheating prevention ability. The Proposed scheme is provably secure against the Horng's cheating activities CA-1, CA-2.The security is enhanced in this scheme by using a steganographic scheme by embedding a secret message within the shares then it is concealed into the cover image thereby decreasing the chance of hacking the secret image. The main disadvantage of this scheme is the pixel expansion. But the quality of recovered image is good for viewing. Pixel expansion is cannot be further reduced because the message embedding capacity is depends on pixel expansion.

REFERENCES

[1]. Moni Naor and Adi Shamir, Visual cryptography. In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12

[2]. .G.Horng, T.H.Chen ,D.S.Tsai, Cheating in visual cryptography, Des Codes Cryptogr.38(2)(2006)219236.

[3]. C.C. Thien, J.C. Lin, A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, Pattern Recognition 36 (11)

(2003)2875_2881K.

[4]. C.M.Hu, W.G. Tzeng , Cheating prevention in visual cryptography,IEEETrans.ImageProcess.16(1)(2007)36_45.

[5]. Zhu BS, Wu JK, Kankanhalli MS (2003) Print signatures for document authentication. In: Proceedings of ACM conference on computer and communications security. 145–153

[6]. Blundo C, Santis A, Stinson DR (1999) On the contrast in visual cryptographyschemes.J.Cryptol,12(4):261–289.

[7]. Yang CN, Chen TS (2007) Extended visual secret sharing schemes:improving the shadow image quality. Int J Pattern Recognit Artif Intell 21(5):879–898.

[8]. Jana, B. ; Mallick, M. ; Chowdhuri, P. ; Mondal, S.K., _Cheating prevention in Visual Cryptography using steganographic scheme_ , International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, 706 _ 712

[9]. Jana, B. ; Mondal, S.K. ; Jana, S. ; Giri, D., "Cheating prevention in Visual Cryptographic Schemes using message embedding: A hardware based practical approach International Conference on Issues and Challenges in Intelligent Computing Techniques(ICICT), 2014, 319 _ 324

[10]. R.De Prisco, A.De Santis, Cheating immune threshold visual secret sharing, Comput.J.53 (2010)1485–1496.

[11]. Chi- Kwong Chan, L.M. Cheng.(2004),-Hiding data in images by Simple LSB Substitution-,Pattern Recognition 37pp.464-474

[12]. Biltta P George, Deepika M P, “Cheating Prevention Schemes for Visual Cryptography”, International Journal of Engineering Research & Technology, vol. 4 Issue 07, July2015.

[13]. C.S Tasai, H.C.Wang, H.C Wu,C.H.M Wang ,”A Cheating Preventing Visual Cryptography Scheme By Referring The Special Position”, International Journal Of Innovative Computing ,Information And Control volume 7 , N Umber7(A),July 2011.

[14]. Aarti, Harsh K Verma, Pushpendra K Rajput ,” Ideal Contrast Secret Sharing Scheme through Meaningful Shares with Enveloping Digital Watermarking using Bit Plane based(k,n)-VCS”, International Journal of Computer Applications Volume 46,No.9,May2012.

[15]. Bin YU, Jin-Yuan LU, Li-Guo FANG,” A Co-cheating Prevention Visual Cryptography Scheme”, Third International Conference on Information and Computing, 2010

[16]. Shuo-Fang Hsu ; Yu-Jie Chang;Ran-Zan Wang; Yeuan-Kuen Lee; Shih-Yu Huang, “Verifiable Visual Cryptography” Sixth International Conference on Genetic and Evolutionary Computing (ICGEC), 2012,464 –467

[17]. Yanng,C., Laih,C.: Some new types of visual secret sharing schemes,vol.III,pp.260-268(December 1999).

[18]. H. Yang And A. C. Kot, ”Binary Image Authentication With Tampering Localization by Embedding Cryptographic Signature And Block Identifier, ”IEEE Signal Processing Letters, Vol.13, No. 12,Pp. 741-744,Dec.2006

[19]. Shamir, A. 1979. How to Share a Secret. Communications of the ACM.22:612-613.

[20]. H. Yan, Z. Gan and K. Chen, .A Cheater Detectable Visual Cryptography Scheme,. *Journal of Shanghai Jiaotong University*, vol. 38, no. 1,2004.

[21]. T.Rabin,Robust sharing of secrets when the dealer is honest or cheating,J.ACM41(6)(1994)1089–1109.

[22]. M. Tompa, H.Woll, How to share a secret with cheaters,J.Cryptology1(3)(1989)133–138.

[23]. Y. C. Chen, D. S. Tsai, G. Horng, A new authentication based cheating prevention scheme in Naor–Shamir’s visualcryptography,J.Vis.Commun.ImageRepresent.23(8)(2012)1225–1233.

[24]. D.S.Tsai ,T.H.Chen ,G.Horng ,A cheating prevention scheme for binary visual cryptography with homogeneous secret images ,Pattern Recogn .40(8) (2007) 2356–2366

Authors Profile

Ms. Biltta P George received the B Tech. degree in Computer Science & Engineering from the Mar Baselios Institute of Engineering and Technology (MBITS) Nellimattom, M.G University, Kerala, India, in 2013. Currently doing **M.Tech.** in computer science and engineering in Adi Shankara Institute of Engineering and Technology, Kalady, MG University, Kerala, India. Her research interest includes Security, Visual Cryptography and Cryptography**.**

Mrs. Deepika M P working at Adi Shankara institute of Engineering and Technology, kalady as Assistant Professor in Information Technology Department. Received her **B. Tech** and **M. Tech** from **CUSAT.**Currently doing **PhD.** in Visual Cryptography in Cochin University of Science and Technology **(CUSAT)**, Kochi, Kerala, India