Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 2, February 2013, pg.80 – 90

RESEARCH ARTICLE

Multi-Share Crypt-Stego Authentication System

Omprasad Deshmukh [1], *Shefali Sonavane* [2]
[1]Computer Science & Engineering, Walchand College of Engineering, Sangli
omprasaddeshmukh@gmail.com
[2]Computer Science & Engineering, Walchand College of Engineering, Sangli
shefali.sonavane@gmail.com

Abstract— It is very common to use text password for authentication. But text passwords are easy to forge. Hence, there is always a need to find more secure techniques for password authentication. This paper, presents a composite structure of Visual cryptography and Steganography with applications associated with QR (quick response) codes and banking applications. QR codes are the type of 2D barcode generally used by mobile phone user for instant access to web pages using hyperlink associated with that code. But, there is always a threat of tampering of QR code. In banking application, there is possibility of forging text passwords or fabricating frauds are common. Finding the scope in such area, it is believed that visual cryptography and Steganography can provide the better solution.

Indexed Terms: - Visual cryptography (VC); quick response (QR) codes; steganography; reversible data hiding; histogram modification; difference expansion.

I. INTRODUCTION

A. *Visual Cryptography*

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images .The way that the original image can be reveals only when both images are simultaneously available. The use of visual cryptography is explored to preserve the privacy of digital data (Image Passwords, QR code of the websites etc.).In this paper, visual cryptography for binary images used in QR code application and visual cryptography for colour images used in banking application.

B. *Steganography*

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Images are the most popular cover objects used for Steganography.The properties like robustness and embedding capacity should be carefully considered when designing a steganography algorithm.The reversible data hiding is new branch in steganography. In reversible data hiding techniques, at the encoder side data is hidden into cover image the output image looks same as that of original cover image. At the decoder side the hidden information as well as cover image should be perfectly recovered. In this paper, both histogram modification and difference expansion reversible data hiding techniques are used.

C. *Fusion Technique*

The multi-share crypt-stego authentication system uses both visual cryptography and steganography. There are two main components encoder and decoder. At the encoder side, key image is the input to visual cryptography stage which divides key image in to multiple shares. The output of visual cryptography stage is forwarded to steganography stage for hiding shares into cover image (stegoimage). At the decoder side, stegoimage is the input to reverse steganography stage for extraction of hidden shares. All output shares are forwarded to visual cryptography stage which overlaps all shares to generate key image. Then the output of decoder stage is checked with certain threshold to decide whether access is allowed or is denied for user.

II. LITERATURE SURVEY

Reversible data hiding is a newly developed branch in data hiding researches. The previous techniques only hide and extract data from host images but reversible data hiding gives us hidden data back as well as host image with perfect recovery [1]. The histogram based reversible data hiding techniques give minimum side information but less data capacity. The difference expansion techniques used for hiding data gives high data capacity but overhead of side information. So, difference expansion quad technique used to hide more data with less side information [2] [3].The histogram based difference expansion algorithm gives the high data capacity with the minimum side information.

The Visual cryptography scheme (VCS) is a secure method that encrypts a secret image by breaking it into shares. These shares provide authentication [4]. A visual cryptography scheme for a set P of n participants is a method to encode a secret image into n shadow images called shares, where each participant in P receives one share. Certain qualified subsets of participants can "visually" recover the secret image, but other, forbidden, sets of participants have no information on secrete image [5].A visual cryptography and 2D data matrix codes can be used for authentication of ID card and ID card owner information by encrypting confidential image into noise like secure shares[6]. A new k-n secrete sharing visual cryptography scheme for colour image where encryption of image is done using random number generator [7]. A (2, N) visual cryptography technique can be used in banking application [8].

III. PROPOSED TECHNIQUE

A. *Project Components*

1) The Encoder:

- Input the key image to visual cryptography stage.
- Divide the key image into multiple shares (for QR code application divide key image into two shares using visual cryptography for binary image and in banking application divide key image into multiple shares using visual cryptography for colour images).
- Hide share into cover images using reversible data hiding with histogram based difference expansion steganography techniques.

2) The Decoder:

- Input stegoimage to extraction stage i.e. reverse steganography technique.
- Retrieve the share from stegoimage using extraction technique.
- Pass shares to fusion step.
- Overlap the shares in fusion stage i.e. reverse visual cryptography technique to get the key image.
- Compare key image to original key image in comparison stage.
- Check the output of comparison step with certain threshold and then decide whether access allowed or denied for user.

Figure .1 and figure .2 gives block diagram of Encoder and Decoder in detail.

B. *Conceptual Framework*

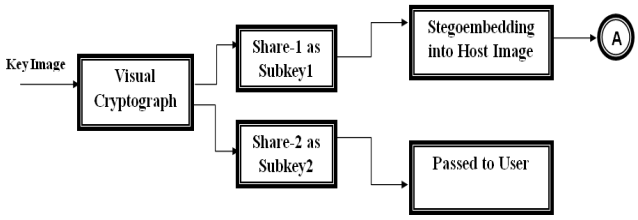

Fig. 1 Block diagram of Encoder

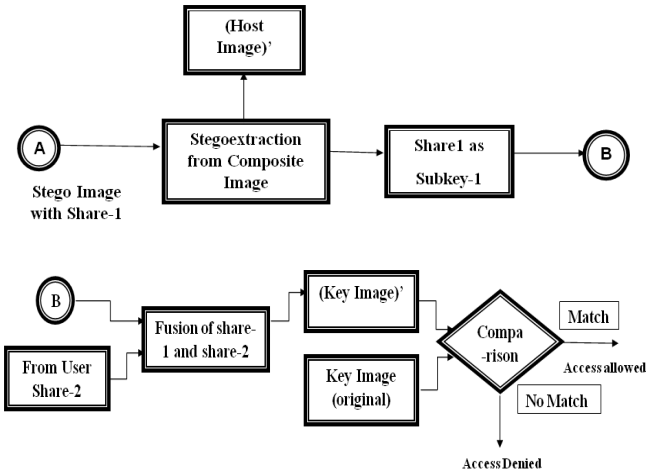

Fig. 2 Block diagram of Decoder

C. *Methodology*

In this paper, the combined approach of visual cryptography and steganography is used for protection of QR code from tampering and also is used for avoid the banking frauds.

QR code is generally observed on corner of poster or webpage. There is always a threat of tampering of original QR code with fake QR code. So instead of keeping QR code on corner of poster or webpage divide the QR code into two shares using VC for binary images and then hide one share in cover image i.e. our poster or webpage and pass another share to the user for further authentication. Apply the extraction techniques to extract hidden share and then pass that share to fusion technique. Only the intended user who has another share can access QR code by passing users share to fusion step. In fusion step after overlapping both shares the required QR code can be obtained. This technique hides QR codes presence on poster or webpage causing very little threat of tampering.

In banking application, the bank logo or key image is divided into multiple shares using visual cryptography for colour images. Then each share is hidden into bank customer image or cover image using steganography technique. Then at the time of access of particular joint account by multiple account holders extract each customer share using extraction technique of steganography and overlap the customer shares to get bank logo or key image. Then comparison can be made with certain threshold and then decision can be taken whether access is allowed or is denied. Depending on presence of number of customers the access permissions are given using k out of n visual cryptography schemas for colour images.

The algorithms used for visual cryptography methods are as follows

1) *Visual Cryptography for binary images:* There are two main steps of visual cryptography: share generation and extraction of original key image.

Algorithm of Share generation:

Step 1: Take the binary image (two tone image) as a key image.

Step 2: Divide the binary images in to two shares as shown in figure 3.

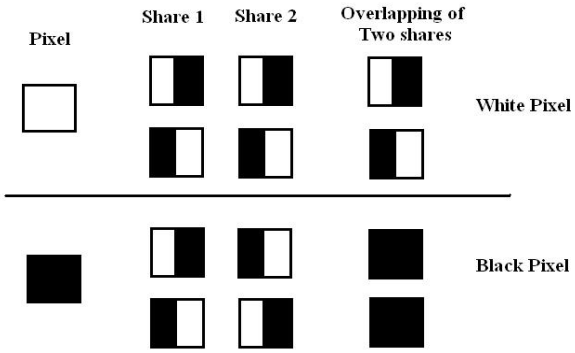

Fig. 3 Visual cryptography with 2 sub pixel construction [4]

Apply the same procedure for converting each pixel from original image into two sub pixels.

Algorithm for reconstruction of original image:

Step 1: Take the two shares (Shares are random noise images).

Step 2: Overlap the two shares to get the original image. Overlapping is simple OR operation or EX-OR operation

Figure 4 shows the block diagram of visual cryptography (2, 2) schema as follows

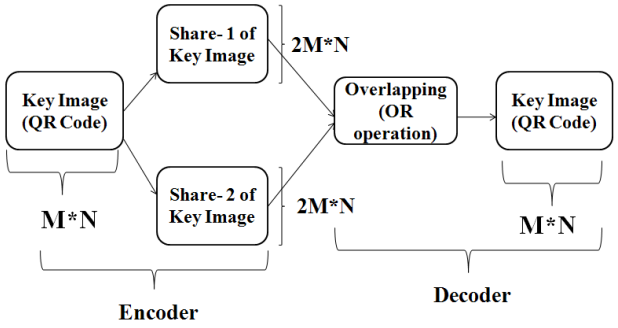

Fig. 4 Block diagram of visual cryptography (2, 2) schema

2) Visual Cryptography for colour images: [6]

Algorithm for share generation:

Step 1: Take the colour image (RGB image).

Step 2: Take the number of shares 'n' and minimum number of shares 'k' to be required to reconstruct the final image, 'k' must be less than or equal to 'n'

Step 3: Calculate reconstruction factor,

recons = (n-k) +1

Step 4: Select the one pixel from original image and convert it into 32 bit binary string

Step 5: take the 1st bit of binary string if it is 1 then in (n-k) +1 number of shares in that position of that pixel there will be 1. In the remaining shares in that position of pixel there will be 0. A random number generator is used to select (n-k) +1 number of shares. Repeat the same procedure for all bits in the 32 bit binary string to reproduce the pixel share.

Step 6: Apply the same procedure of all pixels as mentioned in step 5 to generate shares.

Algorithm for reconstruction of original image:

Step 1: Take any 'k' number of shares to generate original image.

Step 2: Take 1st pixel of each share then convert them into 32 bit binary string.

Step 3: Perform the OR operation on 32 bit string of all shares to get original image pixel. Repeat the same procedure for each pixel from share.

Step 4: Repeat the procedure mentioned in step 3 to get original image by overlapping all 'k' shares. Less than 'k' number of shares should not retrieve the original image.

The algorithms used in steganography method are as follows, the reversible data hiding algorithms used for steganography which gives perfect recovery of hidden data as well as cover image.

1) Histogram Modification: [1]

Embedding Procedure:
Step 1: Generate the Histogram of original image, Calculate
-Max Point
-Zero Point
Step 2: Select the range between max and zero points.
Step 3: Modify the gray values in selected range.
Step 4: Embed the information.

Extraction Procedure:

Step 1: Locate the selected range with side information
Step 2: Extract the hidden data relating to the original
- If the luminance value is equal to a, output bit '0' for the hidden information.
- If the luminance value is equal (a+1), output bit 1.
- For all the other luminance values, there's no output.
Step 3: Obtain the original image.

2) Difference Expansion: [1]

Embedding Procedure:
Step 1: Take the cover image.
Step 2: Take two consecutive pixels*(x, y)*. *x* and *y* are gray scale value of consecutive pixels. Then calculate,

$$l = \left\lfloor \frac{x+y}{2} \right\rfloor$$

$$h = x - y$$

l and h are lower and higher frequency bands.

Step 3: For embedding one bit *b* where $b \in \{0,1\}$

- Keep lower frequency band same
- Change higher frequency band to

$$h' = 2.h + b$$

Step 4: For obtaining image containing the hidden information, the new pair *(x', y')* is calculated by

$$x' = l + \left\lfloor \frac{h'+1}{2} \right\rfloor$$

$$y' = l - \left\lfloor \frac{h'}{2} \right\rfloor$$

x' and *y'* must lie between 0 and 255.

Extraction Procedure:
Step 1: Take the stegoimage (image which contain hidden data).
Step 2: Derive the lower and higher frequency bands as follows

$$l' = \left\lfloor \frac{x' + y'}{2} \right\rfloor$$

$$h' = x' - y'$$

Step 3: Calculate the recovered pixel pair *(x", y")* by,

$$h'' = \left\lfloor \frac{h'}{2} \right\rfloor$$

$$x'' = l' + \left\lfloor \frac{h'' + 1}{2} \right\rfloor$$

$$y'' = l' - \left\lfloor \frac{h''}{2} \right\rfloor$$

Step 4: Finally obtain embedded bit by retrieving the least significant bit (LSB) from h*.

$$h^* = 2.h'' + b$$

Table I compares the histogram modification and difference expansion techniques,

Table- I
DIFFERENCE BETWEEN HISTOGRAM MODIFICATION AND DIFFERENCE EXPANSION

Parameter	**Histogram Modification**	**Difference Expansion (DE)**	
		DE-2	**DE-4**
1)Data Hiding Capacity	Low (Max occurrence of gray values)	High (0.5 bit/pixel)	High (0.75 bit/ pixel)
2)Location Map	Low 16 bit i.e. (Min, Max) pair	High (w*h)/2 Bits	High (w*h)/4 Bits

IV. APPLICATION

A. *QR Code application*

The block diagram of QR Code application is shown in fig 5.

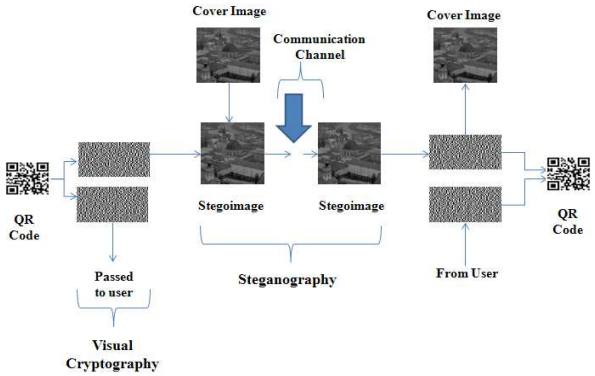

Fig. 5 Visual Cryptography and Steganography for QR code application

B. *Banking application*

The block diagram of banking application is shown in fig 6.

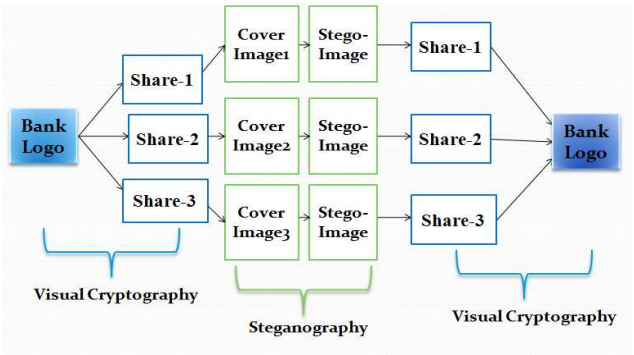

Fig. 6 Visual cryptography and Steganography for banking application

V. EXPERIMENTAL RESULTS

A. *Visual Cryptography*

1) Visual Cryptography for Binary Images:

Encryption Process

Source image: QR_code.jpg
Image size: 350, 350

Fig. 7 Source image (Binary image)

Number of shares: 2.

After applying share generation algorithm on source image following shares are obtained.

Share 1 Share 2

Fig. 8 Encrypted shares

Decryption Process

Input shares: share1.jpg and share2.jpg
Image size: 350,700
Number of shares: 2

Output Results:
Output image size: 350,350

OR operation Ex-OR operation

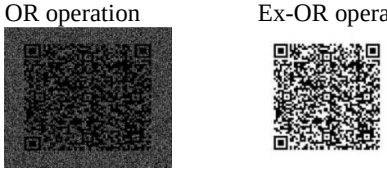

Fig. 9 Reconstructed images

2) Visual Cryptography for Colour Images:

Encryption Process

Source image: Sample.png

Image size: 256,256

Fig. 10 Source image (Colour image)

Number of shares: 8

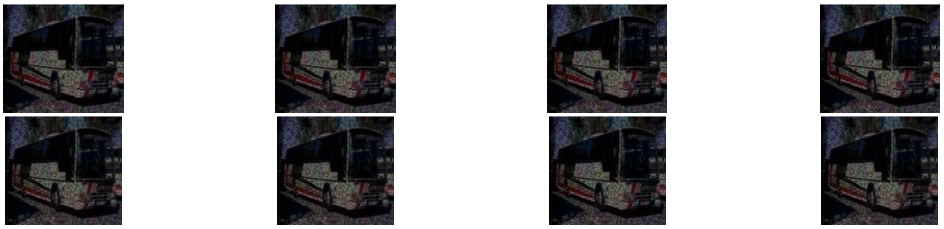

Fig. 11 Encrypted shares

Decryption Process
Input shares: share1.png, share2.png, share4.png, share5.png, share7.png, share 8.png
Number of shares: 8
Number of shares to be taken at a time: 6
Image size: 256,256

Output results:
Output image size: 256,256

Fig. 12 Reconstructed image with any 6 shares (PSNR>50dB)

Fig. 13 Reconstructed image with less than 6 shares (PSNR<30dB)

Quality measure parameter: MSE/PSNR (dB)
For binary image:
After overlapping two shares using EX-OR operation MSE=0
Advantage: Lossless recovery
Disadvantage: Can generate only two shares
For colour images:
PSNR of Recovered images α Number of shares
Advantage: Can generate multiple shares (>=2)
Disadvantage: Lossy recovery
The graph of Number of share Vs. PSNR (dB) for different colour image file format shown below,

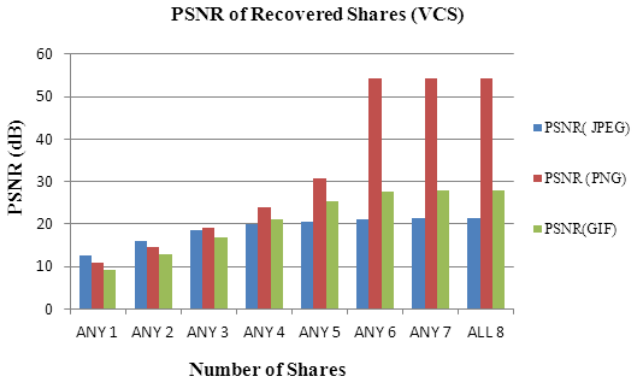

Fig. 14 Graph of Number of shares vs. PSNR (dB)

In above graph, k out of n visual cryptography schema for colour image is used. The visual cryptography schema is applied for different image formats like JPEG, PNG and GIF. So In case of 6 out of 8 visual cryptography, at least 6 numbers of shares out of 8 shares required to get high quality of original image shown in fig 12.Less than 6 number of shares could not recover the original image very well shown in fig 13.

B. *Steganography*

Quality measure parameter: Data Hide Capacity (bits) and Standard Deviation (SD) .Standard deviation is useful to divide sample set of test images into low detail, medium detail and high detail images.

1) Histogram Modifications:

Data Hide Capacity α Image Details (SD)

Advantage: Low location Map (Min, Max) pair 16 bit

Disadvantage: Low data hide capacity i.e. at most 12% of data hide capacity with respect to maximum achievable data hide capacity.

2) Difference Expansion:

Data Hide Capacity α 1/Image Details (SD)

Advantage: High data hide capacity i.e. 98% of data hide capacity with respect to maximum achievable data hide capacity.

Disadvantage: High location map.

The experimental results after applying the histogram modification and difference expansion are shown below,

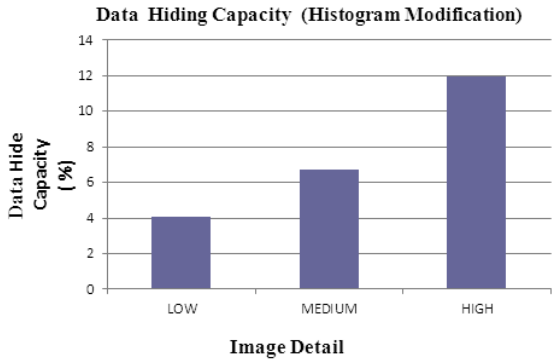

Fig. 15 Graph of Image Details vs. Data Hide capacity (Histogram Modification)

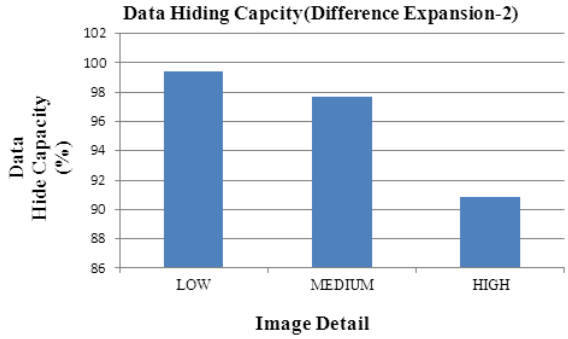

Fig. 16 Graph of Image Details vs. Data Hide capacity (Difference Expansion -2)

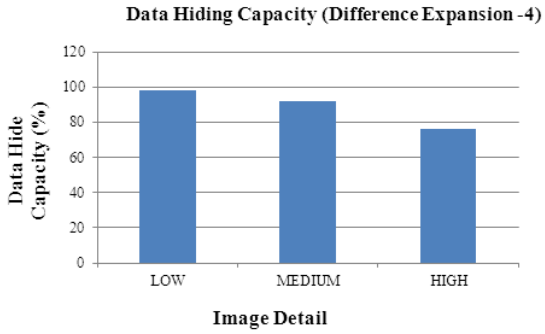

Fig. 17 Graph of Image Details vs. Data Hide capacity (Difference Expansion -4)

Graph shown in figure 16 & 17 indicates that, even for low detail images, the data hiding capacity is maximum, which is normally unexpected observation for any conventional steganographic technique.

VI. CONCLUSION

In this paper, a multi-share crypt-stego authentication system is implemented. The combined technique of visual cryptography and steganography is used in QR code and in banking as case applications. The combined technique of cryptography and steganography gives multi-level security. This multi-level security can be applied in future for similar parallel applications. The advantage of both the techniques discussed can be concentrated and extended to improve upon the results depending on the end application requirements supporting security, authentication and authorization.

REFERENCES

[1] Hsiang-Cheh Huang, Senior Member, IEEE, Feng-ChengChang, Member, IEEE, and Wai-Chi Fang, Fellow, IEEE, "Reversible data hiding with histogram based difference expansion for QR code applications," *IEEE Transactions on Consumer Electronics*, vol.57, no.2, pp. 779-787, May 2011.

[2] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, "A novel difference expansion transform for reversible data embedding," *IEEE Trans. Information Forensics and Security*, vol. 3, no. 3, pp. 456-465, Sep. 2008.

[3] J. Tian., "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technology*, vol.13, no.8, pp. 890–896, Aug.2003.

[4] Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S., "An overview of visual cryptography," *International Journal of Computational Intelligence Techniques, ISSN: 0976–0466 & E-ISSN: 0976–047* vol. 1, Issue 1, pp.32-37, 2010.

[5] JagdeepVerma, Dr.VineetaKhemchandani, "A Visual Cryptographic Technique to Secure Image Shares," *IJERA*, vol. 2, Issue 1, pp.1121-1125, Jan-Feb. 2012.

[6] M. Agnihotra Sharma and M. ChinnaRao, "Visual Cryptography Authentication for Data Matrix Codes," *International Journal of Computer Science and Telecommunications*, vol 2, Issue 8, pp. 58-62 Nov. 2011.

[7] Shyamalendukandar, Arnabmaiti, "k-n secret sharing visual cryptography scheme for color image using random number," *International Journal of Engineering Science and Technology (IJEST)*, vol.3, no.3, pp. 1851-1857, Mar. 2011.

[8] Jayanta Kumar Pal, J. K. Mandal and KousikDasgupta, "A (2, n) visual cryptographic technique for banking applications," *International Journal of Network Security & Its Applications (IJNSA)*, vol.2, no.4, pp. 118-127 Oct. 2010.

