Design and Performance Evaluation of Hybrid Visual Cryptography and Watermarking Scheme using DWT and SVD Algorithms

Pooja Maan[1] Raman Chawla Poria[2]
[1]Research Scholar [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]NCCE, Panipat

Abstract— Visual cryptography scheme is a technique which allows visual information to be encrypted such that the decryption can be performed by the human visual system, without the aid of computers. It is based on cryptography where n images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. This scheme hides the secret image into two or more images which are called shares. The secret image can be recovered simply by stacking the shares together without any complex computation involved. The shares are very safe because separately they reveal nothing about the secret image. But there is an issue regarding their security as every intruder knows that if he/she overlap or super impose two shares than secret data may be revealed. Also, there is need to design shares with a complex method, which would enhance the security of the design method. In this research work, we proposed and experimented advanced visual cryptography. Related work in area of visual cryptography is also discussed in this work. Encryption at each level of VC is expansion less. A share generated out of VC represents the same size of secret. The key-share generated is having random nature. It has been observed that the expansion less shares consume less memory. Graying effect is reduced to zero. A method is designed which provide more security to the shares. This is done by converting the shares in to camouflages. Also more attention is paid to keep the size of reconstructed image according to the size of input secret image with proper contrast matching. All the implementation work will be done is MATLAB R2013a using generalized MATLAB toolbox and image processing toolbox.

Key words: Visual Cryptography, Shares, Camouflage, Secret Images, Secret Shares etc

I. Introduction

Cryptography is the art of achieving security by encoding messages to make them non-readable [7]. It is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. Proper care has to be taken while transferring important secret images. Visual cryptography is the techniques that deal with providing security to the multimedia data. The main concept behind this is, to encrypt a secret image into some shares. The secret can be discovered only when all the shares are combined. Thus, this scheme is very effective. It hides secrets within images. These images are encoded into multiple shares and decoded afterwards without any computation

A. Advanced Visual Cryptography

Visual cryptography is an evolving cryptographic methodology, which is proposed by Naor and Shamir [4]. The very basic idea behind visual cryptography is to share the secret among group of n participants. For sharing the secret is divided into n number of pieces called shares. These shares are circulated among the various participants. To disclose the original secret, each participant provides his own share. Complete knowledge of n-1 shares is unable to decrypt the secret.

B. Visual Cryptography Schemes

Many visual cryptographic schemes exist. The basic scheme is 2out of2 visual cryptography in which the secret is divided into exactly two parts. Second scheme is known as *2* out of n scheme. The original information to be encrypted is called as secret. Third scheme of VC is formally known as K out of n scheme in which the secret is divided into exactly n parts. To reveal the secret any K shares are sufficient.

C. Visual cryptography schemes(VCS) algorithms

VCS algorithm's effectiveness is very important factor and reliability and level of security are some more parameter which we need to consider while designing a VCS algorithm.

– Size of shares which should be same as that of original image to prevent doubt for unauthorized user [1].

D. Region based Visual Cryptography Schemes for Color Images[3]

A region based visual cryptography scheme deals with sharing of image based upon dividing the image into various regions. The main concept of visual secret sharing scheme is to encrypt a secret image into n worthless share images. It cannot disclose any information about the original image unless all the shares are obtained. The original image is obtained by superimposing all the shares directly, so that the human visual system can recognize the shared secret image without using any complex computational devices.

E. Applications of Visual Cryptography

Various applications of visual cryptography are following:

1) Banking Application

Visual cryptography is used in banks at a very large scale. In this type of applications, the 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. 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 [6].

2) Watermarking

It is the technique of embedding a secret image into a cover image without affecting its perceptual quality so that secret image can be revealed by some process. One significant advantage of watermarking is the inseparability of the watermark (secret image) from the cover image. Some of the vital characteristics of the watermark are: hard to perceive, resists ordinary distortions, carries numerous bits of information, capable of coexisting with other watermarks, and demands little computation to insert and extract Watermarks [5].

II. Problem Formulation

It can be formulated from the above literature survey that there are some commonly problem present in existing visual cryptography schemes such as the contrast of the reconstructed image is not maintained, perfect alignment is troublesome, due to pixel expansion the width of decoded message is twice the original message and additional processing is required for colored images. In contrast to existing methods, the shares i.e. share 1 & share 2 will be first converted into camouflages and then will transmitted to the receiver. This modification will give rise to the security of the shares as well for the proposed method. The problems with the existing methods are as follows:

- The contrast of the reconstructed image is not maintained.
- Due to the pixel expansion the width of the reconstructed image is twice as that of the original image. It leads to the loss of information due to change in aspect ratio.

III. Proposed Methodology

All the implementation work will be done is MATLAB R2013a using generalized MATLAB toolbox and image processing toolbox. Three secret images (1.bmp, 2.bmp and 3.bmp) are hidden into two 1200 x 1200 cover images (animal.jpg). In this research work, we proposed and experimented advanced visual cryptography. Related work in area of visual cryptography is also discussed in this work. Encryption at each level of VC is expansion less. A share generated out of VC represents the same size of secret. The *key-share* generated is having random nature. It has been observed that the expansion less shares consume less memory. Graying effect is reduced to zero. A method is designed which provide more security to the shares. In this research work, the secret image to be transmitted is first converted into shares. The vulnerability of binary secret shares is overcome by hiding them invisibly into some host images. During the decryption phase, the secret shares are extracted from their cover images without needing any of the cover image characteristics because the watermark extraction technique is blind. The overlapping of these shares reveals the original secret. The decoded secret signature image quality is improved by using perfect restoration technique. The steps for implementation are as follows:

1) Reading of input secret image to be hided.
2) Conversion of input image to binary.
3) Calculation of size of secret image.
4) Creation of filling vertical matrices.
5) Creation of filling horizontal matrices.
6) Creation of filling diagonal matrices.
7) Creation of random column matrix (having 1s and 2s only) according to the number of elements of secret image.
8) Declaration of index (to be updated further) for above random matrix.
9) Creation of random column matrix (having 1s only) according to the number of elements of secret image.
10) Declaration of index (to be updated further) for above random matrix.
11) Creation of shares A and B randomly in any of the format i.e. Vertical, Horizontal and diagonal for each white and black pixels of secret image.
12) Display of both shares A and B.
13) Creation of camouflages (i.e. Hiding of both shares into an image) for both shares using SVD_DWT watermarking algorithm.
    - Inputting of cover image for camouflages.
    - Conversion of cover image into binary format.
    - Display of cover image.
    - Calculation of size of cover image.
    - Comparison of size of cover image with that of superimposed image.
    - Conversion of watermark or share image into binary one.
    - Calculation of size of watermark image matrix.
    - Calculation of total number of elements in watermark.
    - Decomposition of cover image into approximation coefficients and detailed coefficients using wavelet transform Singular value decomposition of approx. Coefficients.
    - Calculation of size of approx. Coefficients matrix.
    - Creation of dummy matrix (i.e. All elements are zero) according to the size of approx. Coefficients declaration of outer and inner loop according to rows and columns of watermark matrix.
    - Putting up of encrypted watermark elements into dummy matrix.
    - Mixing of watermark with decomposed singular value of approx. Coefficients of cover image
    - Again singular value decomposition of mixed elements and generation of new decomposed values
    - Mixing of new decomposed values with old decomposed values
    - Mixing of newly mixed values with detail coefficients of cover image using inverse wavelet transform.
    - Display of cover image with hide watermark.

IV. Extraction of Watermark

- Decomposition of newly attacked image with help discrete wavelet transform

- and getting of approximation coefficients and detail coefficients
- Singular value decomposition of approx. Coefficients.
- Mixing of diagonal matrix s2 with nonnegative diagonal elements and unitary matrices u2 and v2 obtained previously.
- Extraction of watermark from mixed matrix.
    1) Selection of a central area in cover image according to the size of superimposed image.
    2) Creation of camouflages by mixing of both shares individually to selected portion of cover image.
    3) Display of both embedded images for share 1 and share 2.
    4) Extraction of both shares one by one from camouflages.
    5) Superposition or overlapping of both shares by pixel wise multiplication.
    6) Display of extracted secret image.

V. Experimental Results

In this research work, the secret image to be transmitted is first converted into shares. The vulnerability of binary secret shares is overcome by hiding them invisibly into some host images. During the decryption phase, the secret shares are extracted from their cover images without needing any of the cover image characteristics because the watermark extraction technique is blind. The overlapping of these shares reveals the original secret. The decoded secret signature image quality is improved by using perfect restoration technique. Three secret images (1.bmp, 2.bmp and 3.bmp) are hidden into two 1200 x 1200 cover images (animal.jpg). Snapshot of secret image 1.bmp is shown in figure 1. Snapshot of share 1 and share 2 is shown in figure 2 and 3. Cover image is shown in figure 4. As seen in figure 5 and figure 6, the camouflage images obtained using the proposed algorithm are bit noisy and of improved resolution as compared to existing algorithm. Figure 7 and 8 shows the snapshot of extracted shares from the camouflages. Figure 9 shows the snapshot of overlaid shares. This overlaid share is clearly indicating the original secret image content but the advancement of proposed method improves the overlaid image. The improved overlaid image is shown in figure 10. Therefore, the recovery process is lossless and the used cover images are meaningful. Results shows that the camouflage obtained using the enhanced algorithm where noise is considerably reduced while achieving lossless recovery of the secret message. Also, output parameters have been calculated. These parameters are MSE, PSNR and normalized correlation value. The value of these parameters for proposed method is given in table 1.

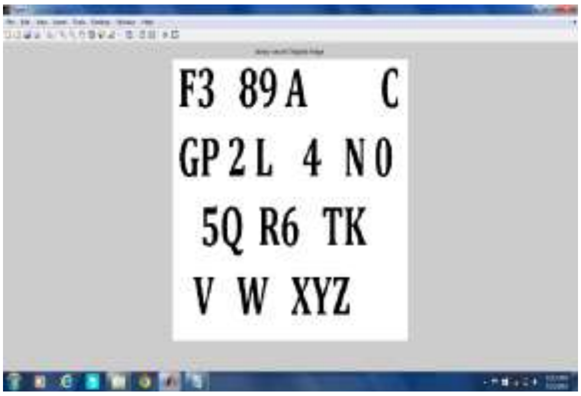

Fig. 1: Snapshot of secret image

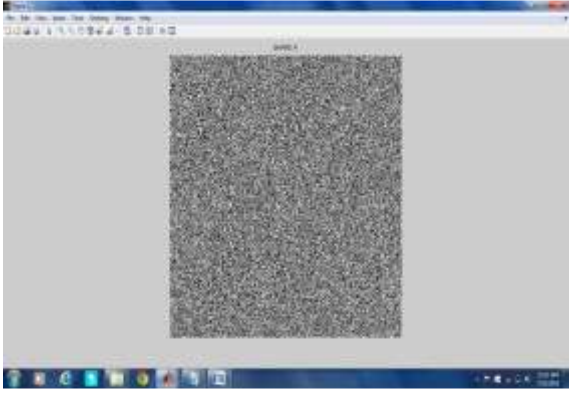

Fig. 2: Share 1

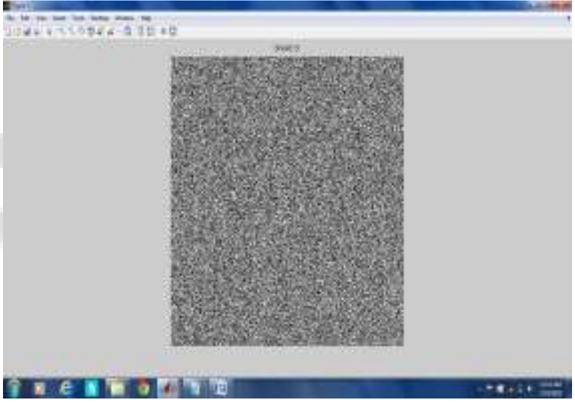

Fig. 3: Share 2

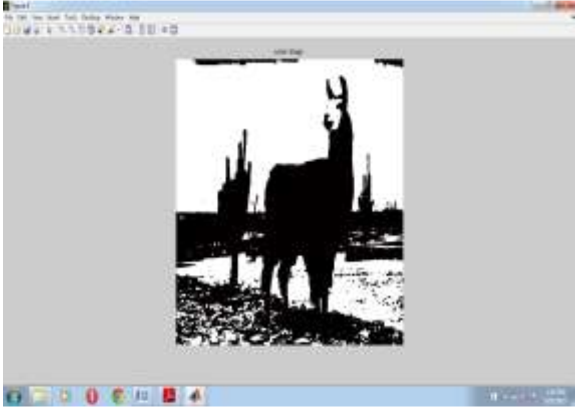

Fig. 4: Cover image

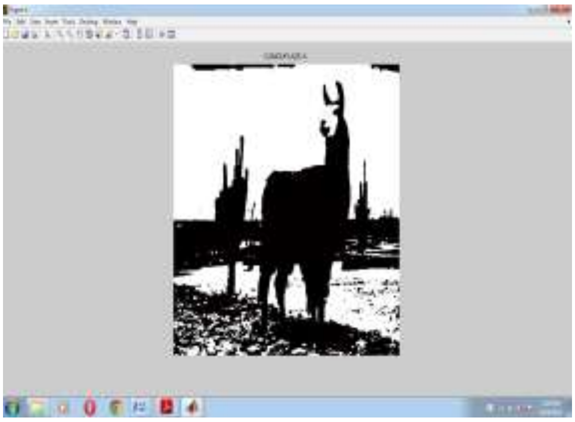

Fig. 5: Camouflage A

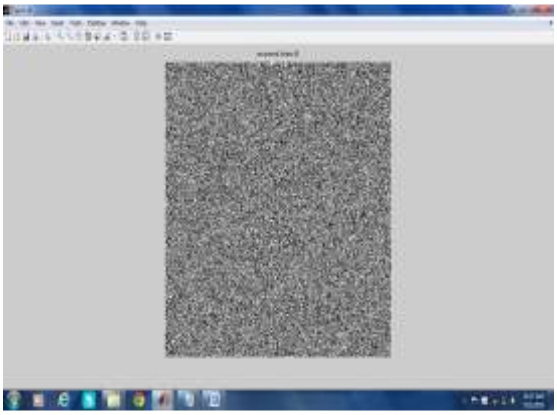

Fig. 8: Extracted share B

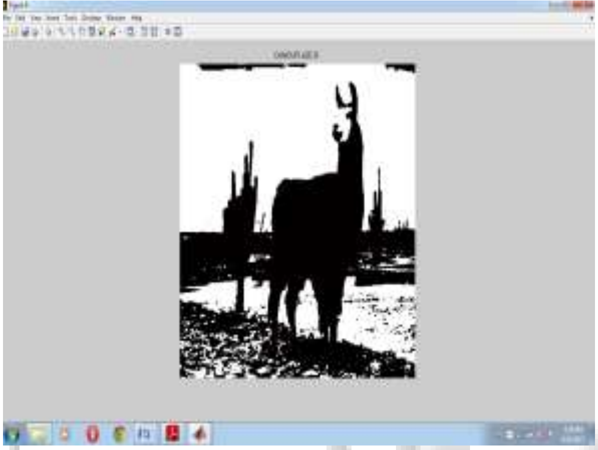

Fig. 6: Camouflage B

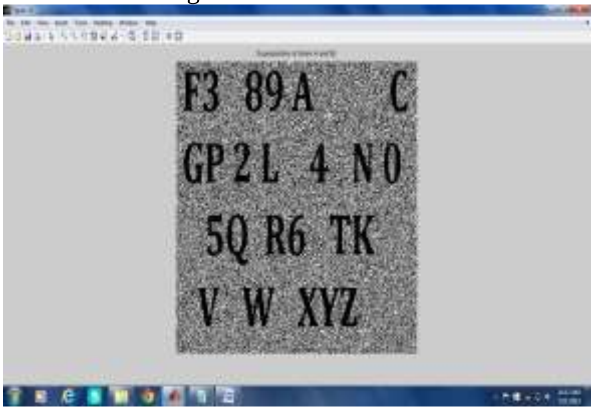

Fig. 9: Overlaid share

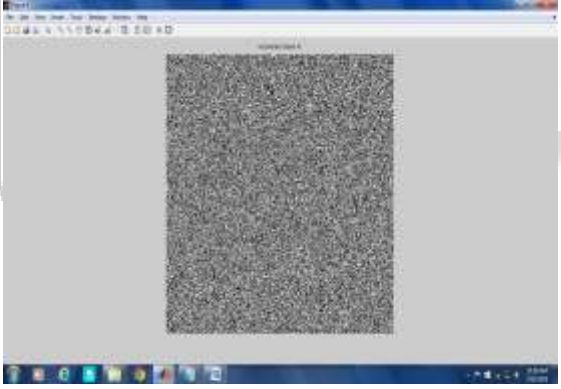

Fig. 7: Extracted share A

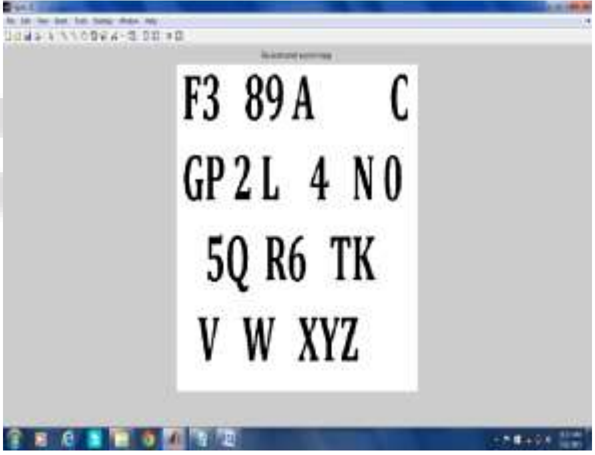

Fig. 10: Improved overlaid share

Secret image filename and size	Cover image filename and size	Camouflage A		Camouflage B		Secret image		
		MSE	PSNR	MSE	PSNR	MSE	PSNR	NC
1.bmp (512 x 512)	Animal.jpg (1200 x 1200)	1.1341e+03	17.5842	1.1341e+03	17.5842	0	Infinity	1
2.bmp (550 x 550)	Animal.jpg (1200 x 1200)	194.8816	25.2331	194.8816	25.2331	0	Infinity	1
3.bmp (530 x 530)	Animal.jpg (1200 x 1200)	607.5403	20.2951	607.5403	20.2951	0	Infinity	1

Table 1 comparison of different parameters for different secret images

VI. Conclusion and Future Scope

Visual Cryptography has proven to be a simple, robust and non-intrusive watermarking technique. In this research work, we proposed and experimented advanced visual cryptography. Related work in area of visual cryptography is also discussed in this work. Encryption at each level of VC is expansion less. A share generated out of VC represents the same size of secret. The *key-share* generated is having random nature. It has been observed that the expansion less shares consume less memory. Graying effect is reduced to zero. In earlier work of visual cryptography it has been observed that expansion of secret taking place after encryption. Thus reflects some graying effect. This results in a considerable improvement in the signal to noise ratio of the camouflage images by producing images with similar quality to the originals. An improvement in signal to noise ratio up to 25.2331 dB were obtained for the initial camouflage images used for hiding the secret image. This developed method does not require any additional cryptographic computations and achieves a lossless recovery of the secret image. In addition, the camouflage images obtained using the modified algorithm look less susceptible of containing a secret message than the ones obtained using the original method. Though VC is widely used in case of image watermarking, video watermarking imposes more challenges. Video files have a larger size compared to simple images; this provides an excellent opportunity to add more secret information. In future, by utilizing the power of visual secret sharing methods for videos in transform domain, VC may offer a very attractive and robust solution for different sectors like defense or military video based communication services, music industries to establish their rightful copyright ownerships, digital video forensic applications etc.

REFERENCES

[1] R.Youmaran, A. Adler, A. Miri "An improved visual cryptography Scheme for Secret Hiding" 23rd Biennial Symposium on Communications 2006. PP. 340-343.

[2] B Surekha, Dr GN Swamy, Dr K Srinivasa Rao, A Ravi Kumar "A Watermarking Technique based on Visual Cryptography" Journal of Information Assurance and Security 4 (2009) 470-473.

[3] D. R. Denslin Brabin, Divya Venkatesan, Divyalakshmi Singaravelan, LekhaSri Rajendran "Region Based Visual Cryptography Scheme for Color Images" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2013. Pp. 1473-1477.

[4] T. Anuradha, K. Usha Rani "Comparative Analysis on Visual Cryptographic Schemes" International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 9, September 2014. pp.134 – 140.

[5] Mr. Abhay Sharma, Mrs. Rekha Chaturvedi, Mr. Naveen Hemrajani, Mr. Dinesh Goyal, "New Improved and Robust Watermarking Technique based on 3rd LSB substitution method", International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012 , ISSN 2250-3153.

[6] Omprasad Deshmukh, Shefali Sonavane "Multi-Share Crypt-Stego Authentication System". IJCSMC, Vol. 2, Issue. 2, February 2013, Pp. 80 – 90.

[7] P. Arunagiri, B.Rajeswary, S.Arunmozhi and K.Priethamje vithya "A Steno Hiding Using Camouflage Based Visual Cryptography Scheme" International Journal of Power Control Signal and Computation (IJPCSC) Vol. 2 No. 1.PP. 1-5.