A Visual Cryptographic Technique to Secure Image Shares

Jagdeep Verma, Dr.Vineeta Khemchandani

*(Department of Computer Science, JSSATE, Noida, UPTU, India)
** (Department of Computer Science, JSSATE, Noida, UPTU, India)

ABSTRACT

The Visual cryptography scheme (VCS) is a secure method that encrypts a secret image by breaking it into shares. A distinctive property of VCS is that one can visually decode the secret image by superimposing shares without computation. The project presents an approach for embedding visual cryptographically generated image shares in the host images to provide authentication for the VC shares and makes these secret shares invisible by embedding them into host images. The secret shares generated from VC encryption are watermarked into some host images using digital watermarking. Digital watermarking is used for providing the double security of image shares. The share is embedded into the host image in frequency domain using Discrete Cosine Transform (DCT). In frequency domain, the obtained marked image must be less distorted when compared to the original image. Thus secret shares are not available for any alteration by the adversaries who try to create fake shares. Every pixel of the binary VC share is invisibly embedded into the individual block of the host image. The process of watermark extraction necessitates only the watermarked image and it does not require the original host image. The scheme provides more secure and meaningful secret shares that are robust against a number of attacks like blurring, sharpening, motion blurring etc.

Keywords **– Secret shares, Visual cryptography, Watermarking, Host images.**

1 INTRODUCTION

Visual Cryptography (VC) [1] is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies. Each participant holds a transparency (share). Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to simply stack shares and view the Secret image that appears on the stacked shares.

Watermarking 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, endures malevolent attacks, carries numerous bits of information, capable of coexisting with other watermarks, and demands little computation to insert and extract Watermarks. Generally, robust watermarking is used to resist un-malicious or malicious attacks like scaling, cropping, lossy compression, and so forth. Watermarking techniques can be categorized into different types based on a number of ways. Watermarking can be divided into Nonblind, Semi-Blind and Blind schemes based on the requirements for watermark extraction or detection. Nonblind watermarking schemes necessitate the original image and secret keys for watermark detection. The Semi-Blind schemes require the secret key(s) and the watermark bit sequence for extraction, whereas, the Blind schemes need only the secret key(s) for extraction. Another categorization of watermarks based on the embedded data (watermark) is: visible and invisible. With visible watermarking of images, a secondary image (the watermark) is embedded in a primary image in such that it is perceptible to a human observer, whereas the embedded data is not detectable in case of invisible watermarking; nevertheless, it can be extracted by a computer program.

Here our proposed scheme will add the merits of both visual cryptography as well as Invisible and Blind watermarking techniques, where we will generate the secret shares using basic visual cryptography model and then we will watermark these shares into some host image using invisible and blind watermarking. Thus the secret shares are protected from cheating attacks. The decryption will be same as in the visual cryptographic model i.e. by stacking of the shares after the secret shares have been extracted by a simple watermark extraction technique. The proposed watermarking scheme doesn’t necessitate the original image or any of its characteristics for the extraction of watermark, and hence the proposed scheme is blind. The experimental results have been demonstrated for efficiency of the proposed Invisible and Blind Watermarking scheme for Binary images.

2 REVIEW OF RELATED TOPICS

A. (2, 2) Visual Cryptography Scheme

Visual Cryptography (VC) was first introduced by Moni Noar and Shamir at Eurocrypt'94 [1]. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. To encode a secret employing a (2, 2) VC Scheme, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two or four sub-pixels as shown in Fig.1.

Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret.

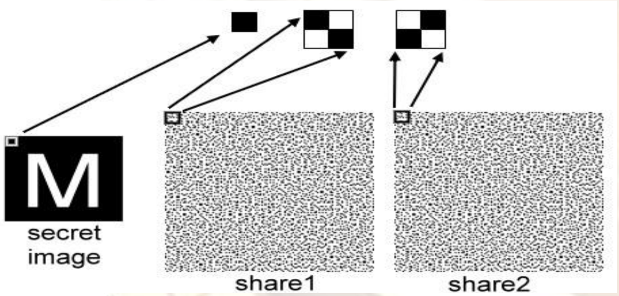
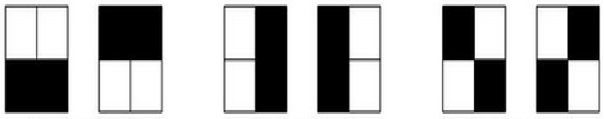


Fig. 1 (2, 2) Visual Cryptography scheme

There are several schemes of encoding the pixels of the secret image. In our scheme, each pixel in the secret image is broken into four sub pixels. A white pixel is shared into two identical blocks of four sub-pixels. A black pixel is shared into two complementary blocks of four sub-pixels. Fig. 2 illustrates this scheme of encoding one pixel into four pixels in a (2, 2) VC scheme. All the pixels in the original image are encrypted similarly using this scheme. These shares can be either Vertical or Horizontal or Diagonal Share as shown in the Fig.2.



Horizontal Shares Vertical Shares Diagonal Shares

Fig. 2 Pixel encoding in (2, 2) Visual Cryptography scheme

B. Digital Watermarking

Our work has been motivated by a copious number of earlier works available in the literature that utilize digital image watermarking for protecting copyrights of digital images. Debasish Jena1Sanjay Kumar [2] has proposed Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm is given, which is a modified version of existing Data hiding in halftone image by conjugate error diffusion (DHCED) algorithm [3]. S.Riaz et al. [4] proposed invisible watermarking schemes in spatial and frequency domains. Two schemes were proposed for embedding data in the image. In FFT (Fast Fourier Transform) based approach the data that was to be embedded has been pre- processed before embedding. Mrs.D.Mathivadhani, Dr.C.Meena [5] proposed Digital watermarking and information hiding technique using Wavelets, SLSB and Visual cryptography method. B.padhmavati et al. [6] proposed A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography using Image Processing. In this paper the shares have been generated first by Visual Cryptography. VC (2, 2) scheme was used for generating shares. After that both shares were embedded into the cover images with the help of blind watermarking. In this research, we propose an innovative Invisible and Blind watermarking scheme, applied to VC shares to secure them against Cheating attacks by the adversaries

3 PHASES OF PROPOSED SCHEME

We are proposing a new scheme for visual cryptography which will use watermarking technique to embed the generated shares into any cover image. Proposed scheme consists of three phases which are described in the following subsections.

Phase I - Visual Cryptographic Encryption*:* In this very first phase we will do visual cryptography encryption. It consists of generation of shares using any basic visual cryptography model. In our proposed scheme, a (2, 2) VC share creation is performed. Each pixel in the secret image is broken into four sub pixels. A white pixel is shared into two identical blocks of four sub pixels. A black pixel is shared into two complementary blocks of four sub pixels. All the pixels in the secret image are encrypted similarly using this scheme. The shares can be either Vertical, Horizontal or Diagonal shares. Any single share is a random choice of two black and two white sub pixels, which looks medium grey. When two shares are stacked together, the result is either medium grey (which represents white) or completely black (which represents black).

The visual secret sharing scheme assumes that the message consists of a collection of black and white pixels and each pixel is handled separately. Each original pixel appears in n modified versions (called shares), one for each transparency. Each share is a collection of m black and white sub pixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions. The resulting structure can be described by an n × m Boolean matrix S = $[sij]$ where $sij = 1$ iff the jth sub pixel in the ith transparency is black. When transparencies $i1, i2, \dots \dots ir$ in S. The grey level of this combined share is proportional to the Hamming weight H (V) of the "or" ed m-vector V. This grey level is interpreted by the visual system of the users as black if $H(V) \geq d$ and as white if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$. Fig.3 shows the working of visual cryptography scheme.

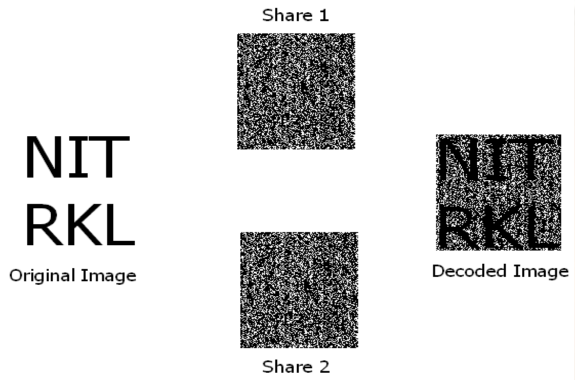


Fig. 3 working of visual cryptography

Phase II - Hiding the Shares using Digital watermarking: This phase embeds image shares into some cover images using digital watermarking. Result of this phase will be different meaningful shares consist some cover image.

Discrete cosine transformation (DCT) is used for convert the image into frequency domain. DCT can be interpreted as decomposition into a set of frequency coefficients having the same bandwidth on a logarithmic scale. The obtained coefficients are real number values. The main advantage of DCT which makes it attractive for watermarking is its energy compaction property. This property divides the image into distinct frequency bands which makes it easy to embed the watermark in the desired area of the image. The algorithm for embedding the watermark is following.

Step 1: Set minimum coefficient difference.
Step 2: Set the size of the block in cover image to be used for each bit in watermark.
Step 3: Read in cover object.
Step 4: Determine size of cover image.
Step 5: Determine maximum message size based on cover object and block size.
Step 6: Read in the message image.
Step 7: Reshape the message to a vector.
Step 8: Check that the message is not too large for cover.
Step 9: Pad the message out to the maximum message size with ones.
Step 10: Process the image in blocks.
Step 11: Transform block using DCT.
Step 12: If message bit is black then value of frequency coefficient (5, 2) > (4, 3).
Step 13: End if
Step 14: If message bit is white then value of frequency coefficient (5, 2) < (4, 3).
Step 15: End if
Step 16: Adjust the two values such that their difference >=k.
Step 17: Transform block back into spatial domain.
Step 18: Move on to next block, at the end of row move to next row.
Step 19: Exit

Phase III - Visual Cryptographic Decryption: In this phase the binary watermarked shares extracted from the host images. The proposed watermarking scheme doesn't necessitate the original image or any of its characteristics for the extraction of watermark, and hence the proposed scheme is blind. Then we apply the visual cryptographic decryption. As we know that visual Cryptographic decryption does not need any type of decryption algorithm or computation. It uses human visual system for decryption which is the core advantage for which visual cryptography was developed. Now we can decrypt the original secret image by overlapping or stacking the shares. Fig 4 is the structure of proposed scheme. The algorithm for watermark extraction is following.

Step 1: Set the size of the block in cover to be used for each bit in watermark.
Step 2: Read in the watermarked object.
Step 3: Determine size of watermarked image.
Step 4: Determine max message size based on cover object and block size.
Step 5: Process the image in blocks.
Step 6: Transform block using DCT.
Step 7: If dct_block (5, 2) > dct_block (4, 3) then message bit is 0, otherwise message bit is 1.
Step 8: End if
Step 9: Move on to next block, at the end of row move to next row.
Step 10: Reshape the embedded message.
Step 11: Exit

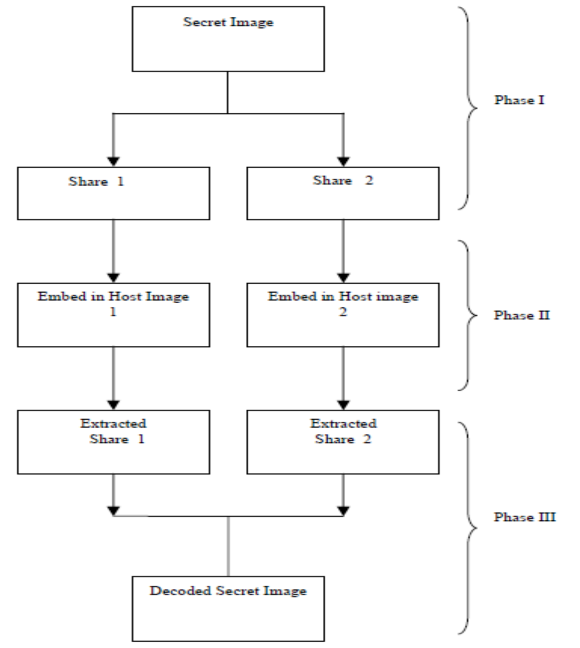


Fig. 4 Structure of proposed scheme

4 SIMULATION RESULTS

For simulation we have used MATLAB 7.0 tool and tested with images of different sizes. The proposed scheme achieves effective embedment of the binary share images into the host images. Also, the proposed scheme depicts efficient extraction of the embedded watermarks from the watermarked images. The watermarked images possess good Peak Signal to Noise Ratio (PSNR) and good visual quality. Fig. 5 depicts the results obtained on experimentation of the entire proposed Visual Cryptography scheme. The results include original secret image, encoded secret shares, host image, watermarked images and the decoded secret image.

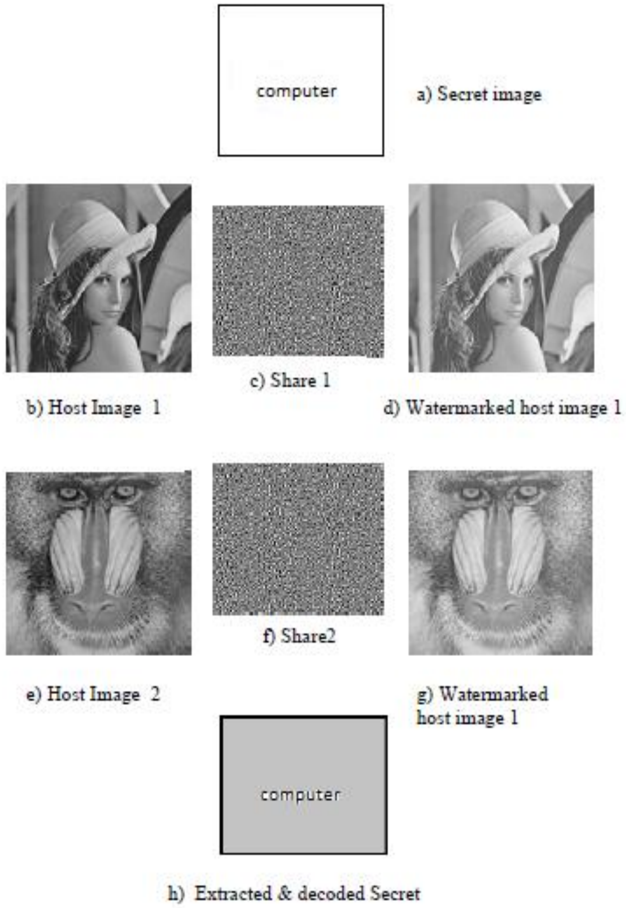

computer
a) Secret image
b) Host Image 1
c) Share 1
d) Watermarked host image 1
e) Host Image 2
f) Share2
g) Watermarked host image 1
computer
h) Extracted & decoded Secret

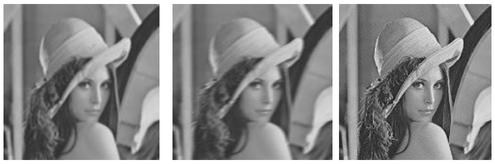
Fig. 5 Experimentation Results

4.1 Robustness to attacks: To evaluate the robustness of the proposed method, several attacks have been applied to the watermarked image. Fig.6 & Fig 7 shows watermarked image under different attacks and extracted watermarks under different attacks respectively.

Blurring: Blurring is use in pre-processing steps, such as removal of small details from an image. Noise reduction can be accomplished by blurring with a linear filter and also by nonlinear filtering.

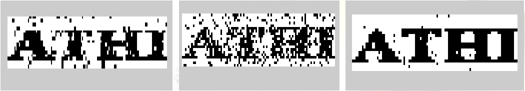
Motion blurring: The blurring of an image caused by the distance an object moves relative to the amount of camera motion. For computer graphics, this effect needs to be added artificially, either by 3D motion blur that is calculated during rendering or with a 2D motion blur that is applied as a post process on the already rendered images.

Sharpening: The principal objective of sharpening is to highlight fine details in an image or to enhance detail that have been blurred, either in error or as a natural effect of a particular method of image acquisition.



(a) (b) (c)

Fig. 6 Watermarked Image under different attacks.
(a) Blur (b) Motion blurr (c) Sharpening



(a) (b) (c)

Fig. 7 Extracted watermarks under different attacks.
(a) Blur (PSNR = 9.59db) (b) Motion blurr (PSNR = 6.78db) (c) Sharpening (PSNR=16.99 db)

5 CONCLUSION

Visual cryptography is the current area of research where lot of scope exists. Currently this particular cryptographic technique is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. There are various innovative ideas and extensions exist for the basic visual cryptographic model introduced till now. One such enhancement we are trying to do. In the existing VC schemes no security is provided to the secret shares and adversaries can alter its bit sequences to create fake shares. And in our proposed scheme, the vulnerability of these 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 image quality is improved. Yet many possible enhancements and extensions can be made to improve further.

REFERENCES

[1] M.Naor and A.Shamir, 1995. Visual cryptography. Advances in Cryptology EUROCRYPT ’94. Lecture Notes in Computer Science, (950):1–12.

[2] D.Jena and S.Jena, 2009. A Novel Visual Cryptography Scheme. In Proceedings of International Conference on Advanced Computer Control, (ICACC’2009), pp.207-211.

[3] Y.Bani, Dr.B.Majhi and R.S.Mangrulkar, 2008. A Novel Approach for Visual Cryptography Using a Watermarking Technique. In Proceedings of 2nd National Conference, IndiaCom 2008. Computing for national development, February 08-09, New Delhi.

[4] S.Riaz, M.Javed and M.Anjum, 2008. Invisible Watermarking Schemes in Spatial and Frequency Domains. In Proceedings of fourth International Conference on Emerging Technologies (ICET’ 2008), pp. 211-216.

[5] Mrs.D.Mathivadhani, Dr.C.Meena, 2010. Digital Watermarking and Information Hiding using Wavelets, SLSB and Visual Cryptography method. In Proceedings of International Conference on Computational Intelligence and Computing Research (ICCIC’2010), pp. 1-4.

[6] B.padhmavati, P.Nirmal Kumar, M.A.Dorai Rangaswamy, 2010. A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography Using Image Processing. Proceedings of Int. Conf. on Advances in Computer Science 2010, DOI: 02, ACS.2010.01.264, ACEEE.