ISSN:0975-9646
Malvika Gupta et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4339-4343

A Visual Cryptographic Scheme To Secure Image Shares Using Digital Watermarking

Malvika Gupta, Deepti Chauhan

Department of Computer Science, YIET, Yamuna Nagar, Kurukshetra University

Abstract-Visual Cryptographic Scheme is a special technique used to send the data securely over the network. It is a technique which allows visual information (pictures etc.) to be encrypted in such a way that the decryption can be performed by the human, without using any decryption algorithm or without doing any computation.

In this paper we have introduced the new technique known as the "Digital Watermarking" technique in order to secure or ensure the owner authentication. Digital Watermarking is almost same as that of the Steganography but as steganography more focused about hiding the information over a cover object so that it cannot be perceived by the user but in watermarking the hidden information is usually related to the cover image.

In this we have introduced the new technique, digital watermarking as the simple visual cryptography is not so secure for sharing of data and it also does not ensure the owner authentication. This cryptographic technique involves dividing the secret image into n shares and a certain number of shares (m) are sent over the network.

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 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.

Earlier it was implemented in spatial domain but it was not successful as the marked image was very much distorted and not able to bear the attacks.

In this paper we have discussed about the watermarking, how it can be done and upto which level it can bear the attacks.

OVERVIEW

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.

The technique was proposed by Naor and Shamir in 1994 [1]. It is used for the secure

encryption of the visual information like written notes, videos etc. in a secure way so that decryption becomes a mechanical operation that does not require computer it means that decryption can be done using the human visual system i.e. human eye.

Visual Cryptography (VC) [2] is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. It is a visual secret sharing scheme, where an image was broken into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. It is shown in Fig 1(a) & Fig 1(b)

Fig 1(a): Two shares of a Secret image

Fig 1(b): Embedded image Occurs.

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.

A watermark technique has few characteristics like 'robust' with respect to transformations if the embedded information may be detected reliably from the marked image, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping and additive noise.

Share generation in visual cryptography can also be done using the watermarking technique. We can use these watermarked shares to retrieve the hidden information.

Watermarking techniques can be categorized into different types based on a number of ways. Watermarking can be divided into Non-blind, Semi-Blind and Blind schemes based on the requirements for watermark extraction or detection. Non-blind 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.

Digital watermark is a visible or perfectly invisible, identification code that is permanently embedded in the data and remains present within the data after any decryption process. It means 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.

In our proposed scheme, will include both visual cryptography as well as invisible and blind watermarking techniques where we will generate the secret shares using visual cryptography model and then we will watermark these shares into some hosts using invisible and blind watermarking. Thus the secret shares can be protected from the cheating. For decryption we are using the simple visual cryptography scheme.

DESCRIPTION OF RELATED TOPICS

A.Access Structure Scheme:

1: **(2, 2) – Threshold VCS**: This takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

2: **(2, n) – Threshold VCS**: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

3: **(n, n) – Threshold VCS**: This scheme encrypts the secret image into n shares such that only when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.

4: **(k, n) – Threshold VCS**: This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the threshold, and n, the number of participants.

Fig. 2 & Fig. 3 shows two of the several approaches for (2, 2) – Threshold VCS. In this particular figure first approach shows that each pixel is broken into two sub pixels.

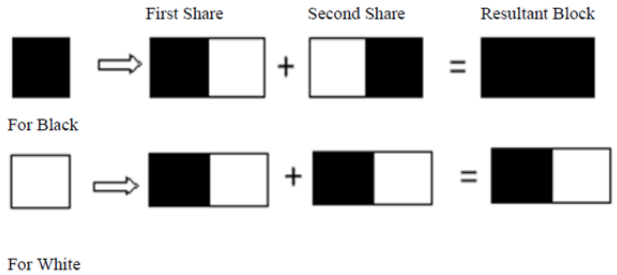

Fig 2: Pixel is broken in two sub-pixels.

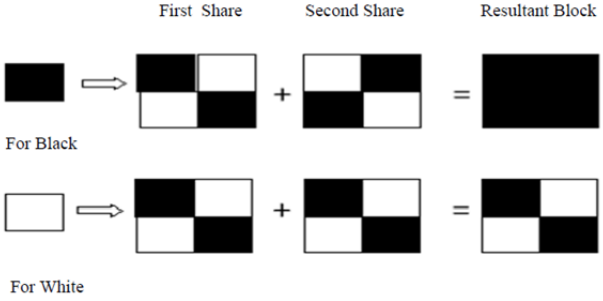

Fig 3: Pixel is broken into four sub-pixels.

The above two figures shows the shares and these shares can be represented horizontally or vertically or diagonally as shown in the Fig 4 given below.

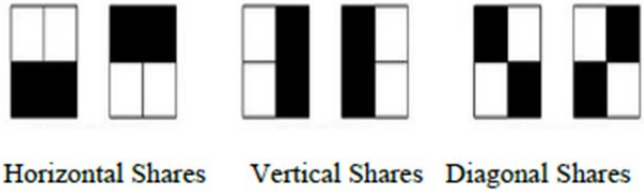

Fig 4

B.Digital Watermarking:

Our work has been motivated by a number of earlier works available in the literature that utilize digital image watermarking for protecting copyrights of digital images.

S.Riaz et al. [3] 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. B. Padhmavati et al. [4] 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.

In 2008, Yogesh Bani et al. [5] proposed a novel approach for visual cryptography using a watermarking technique. Data hiding by conjugate error diffusion algorithm was used for generating the shares. The cover image x has been error diffused, which has been used as a first share. For generating the second share the image was watermarked into the cover image. Secret and cover images have been revealed after overlapping shares.

PHASES OF PROPOSED SCHEME

Phase I-Visual Cryptographic Encryption

In proposed scheme, a VC (2, 2) 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. Fig.3.2 illustrates this scheme of encoding one pixel into four sub pixels in a (2, 2) VC scheme. 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 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) ≥ d and as white if H(V) < d – αm for some fixed threshold 1 ≤ d ≤ m and relative difference α > 0. Fig 5 shows the working of visual cryptography.

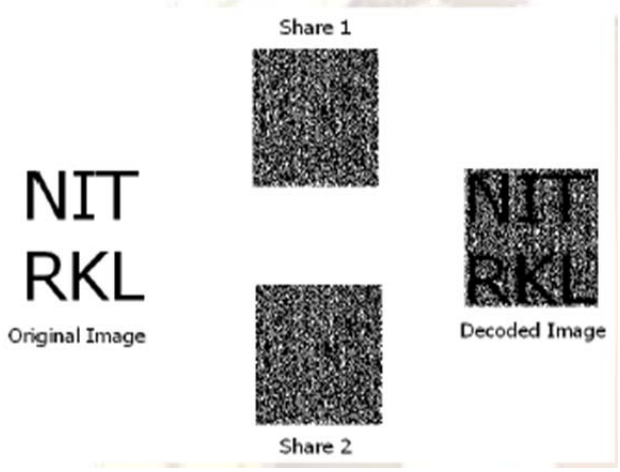

Fig 5: Working of Visual Cryptography

Phase II-Embed shares using digital watermarking

This phase embeds image shares into some cover images using digital watermarking. It will provide double security over other cryptographic security schemes. To embed the watermark in the image we are using the Discrete Cosine Transformation (DCT), which is used to convert the image into frequency domain. It can be done under the following steps:

1. It can be interpreted as decomposition into a set of frequency coefficients having the same bandwidth on a logarithmic scale.
2. The obtained coefficients are real number values.
3. The coefficients can be split using the zigzag ordering into low frequency coefficients, mid-frequency coefficients, and high frequency coefficients as shown in the Fig 6.

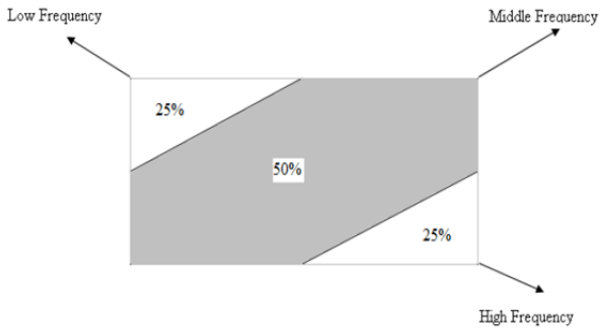

Fig 6: Frequency Coefficients Division

4. In the proposed method 50% of the total coefficients lying in the middle frequency region are used for embedding.

The main advantage of DCT in the proposed scheme 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.

Following steps have been followed to embed VC shares into the cover image.

1. The image is segmented into non-overlapping blocks of 8x8 pixels.
2. Forward DCT is applied to each of the block.
3. Region selection criteria are then applied.
4. This is followed by applying coefficient selection criteria.
5. Embed watermark by modifying the selected coefficients.
6. Inverse DCT is applied to obtain the final watermarked image.

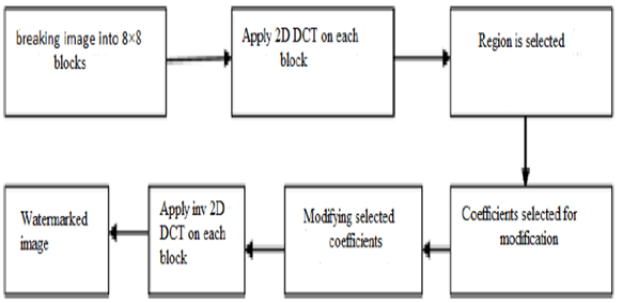

Fig 7: Block Diagram of Watermarking Steps using DCT.

Phase III-Visual Cryptography Decryption

In this phase the binary watermarked shares extracted from the host images. The watermarking scheme we have introduced does not require the original image and hence it is the blind scheme. As we know that in this proposed scheme there is no requirement of the decryption algorithm or the computation it can be easily done through the human visual system and this is also the advantage of this proposed technique.

Now decrypt the original secret image by overlapping or stacking the secret image. To extract the original image the following steps are required to be followed as discussed below:

1. It is the reverse process of embedding.
2. The watermarked gray scale image is segmented into non overlapping block of 8×8.
3. Each block of watermarked image is transformed into frequency domain using DCT.
4. After applying DCT on each block mid frequency coefficients need to be identified.
5. For each block, if the value of frequency coefficient (5, 2) > (4, 3) then message bit is 0 otherwise message bit is 1.
6. Now reshape the embedded message.

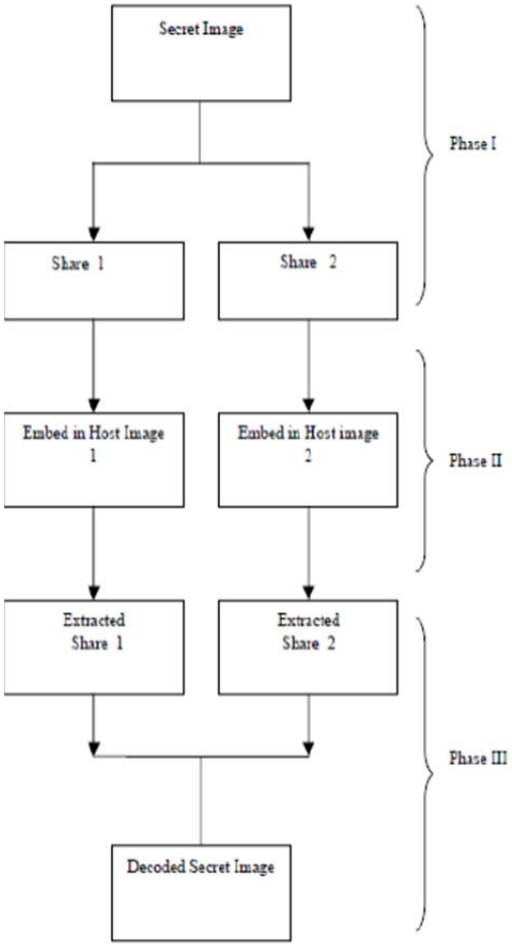

Fig 8: Structure of Proposed Scheme.

EXPERIMENTAL RESULTS

Proposed scheme have been developed in MATLAB 7.0 tool. The scheme takes as input a secret image and two cover images. It first generates the two shares of the secret image using visual cryptography encryption. After encryption, both shares are watermarked in two cover images using digital watermarking. Then using watermark extraction algorithm both shares are extracted from the watermarked images and then stacked together to revealed the original secret image.

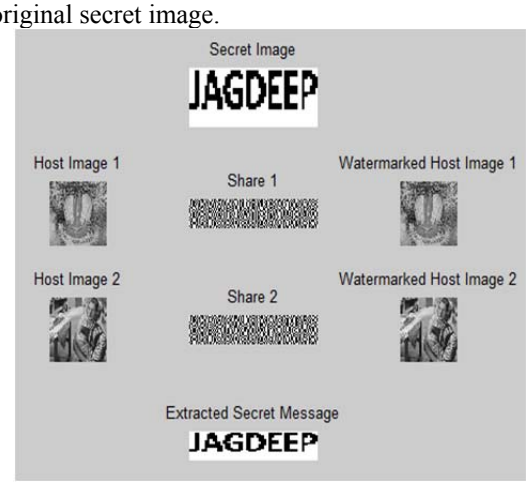

Fig 9: Experimental Result.

ROBUSTNESS AGAINST ATTACKS

Blurring

Blurring is used 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.

On experimental basis the blur attack is shown in the given Fig 10.

Fig 10: Blur Attack

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.

On experimental basis the motion blurred attack is shown in the given Fig 11.

Fig 11: Motion Blur Attack

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.

On experimental basis the blur attack is shown in the given Fig 12.

Fig 12: Sharpening Attack

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. 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] 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.

[4] 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.

[5] 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.