International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

A Comprehensive Study on Securing Visual Cryptographical Image Shares Using Digital Watermarking

Neena[1], Gunjan[2]

[1]*PG Scholar, Department of computer science, PDM college of Engineering, Bahadurgarh, Haryana, India*
[2]*Assistant Professor, Department of computer science, PDM college of Engineering, Bahadurgarh, Haryana, India*

Abstract - *This paper shows the study of various digital watermarking techniques and also the merits of combining the visual cryptography with digital watermarking techniques. The Visual cryptography scheme (VCS) is an encryption method that encrypts a secret image by breaking it into shares. Unlike traditional cryptographic schemes, decryption of secret image in VCS could be done visually by just superimposing the shares without any complex algorithm. Watermarking can be described as a method of embedding information (audio, video or image) into another signal so that the information cannot be removed easily. The embedded information can either be in hidden or visible form. In case of digital images,. This technique can be used to provide more security to visual cryptographic (VC) image shares by embedding image shares into the host image.*

Key Words*: *Digital Watermarking, Visual cryptography, Cover images, Secret shares, Spatial Domain, Transform Domain.

1. INTRODUCTION

During the past decade, with the advancement in information digitalization and internet huge amount of digital data is being transmitted or stored. Information security is one of the major issues in modern computerized society as the transmitted data on networks or stored data in computers can easily be illegally manipulated if the information is not secured by modern cryptographic tools.

Visual Cryptography [1] is a cryptographic technique of encrypting a secret image into shares in a way that superimposing a sufficient number of shares reveals the secret image whereas shares are binary images usually presented in form of transparencies. Visual cryptographic technique is being used by several countries for secret transmission of images in defense, financial documents, hand written documents, text images, internet- voting etc. Fig -1 shows the flow of visual cryptography in which a secret binary image is divided into two different shares and then original image is recovered

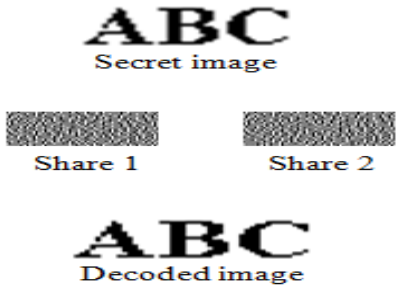


Fig -1: Visual cryptography flow

Digital image watermarking is the technique of embedding a secret image into a host image without affecting its perceptual quality so that the secret image can be revealed by some process. The digital watermarking is used for the security of the digital content and to protect the data from illegal users by providing the ownership right on the digital data. An important characteristic of digital watermarking is invisibility and robustness against various types of attacks or common image manipulation like rotation, filtering, scaling, cropping and compression. Watermarking technologies is applied in every digital media where security and owner identification is required. Some most common applications [9] are owner identification, copyright protection, broadcast monitoring, medical applications, fingerprinting and data authentication.

It could be seen that VCS alone is not secure to the cheating process where malicious adversaries can create and share fake image shares or modify the image shares. To overcome the cheating attacks, image shares can further be secured by embedding the image shares into some host images by using digital watermarking. It will not only provide authentication to image shares but also make the shares invisible into host images and thus protects shares from any illegal manipulations [6].

1.1 Visual Cryptography

Moni, Naor and Adi Shamir in 1994 [1] had been credited for the development one of the best known techniques in visual cryptographic technique. In this scheme an image is divided into *n* shares so that someone with all *n* shares could only

decrypt the image by superimposing the shares over each other. This can be achieved by printing each share on a separate transparency and then placing all of the transparencies over each other. The main characteristic of this technique is that *n*-1 shares of the image reveal no information about the original image. This can be achieved by using one of following access structure schemes [7].

1: (2, 2) – Threshold VCS: This scheme involves a secret image which is encrypted into two non-identical shares that reveal the secret image when they are superimposed. In creation of this kind of access structure no additional information is required.

2: (2, n) – Threshold VCS: In this scheme the secret image is encrypted into n shares in such a way that when any two (or more) of the shares are superimposed the secret image is revealed. Here n stands for the number of participants.

3: (n, n) – Threshold VCS: In this scheme the secret image is encrypted into n shares in such a way that when all the n shares are superimposed the secret image is revealed. Here n stands for 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 superimposed, the secret image will be revealed. Here k, stands for the threshold and n, stands for the number of participants.

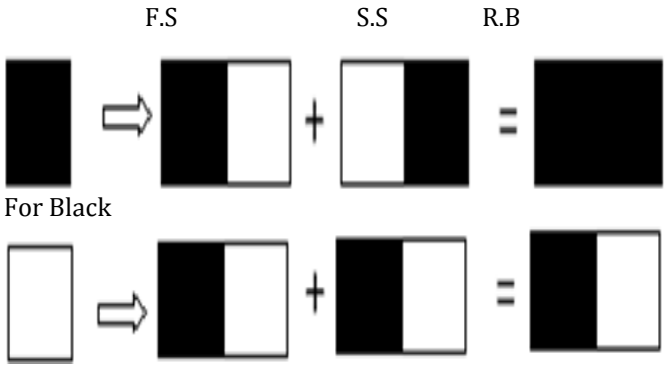
Fig -2 shows two of the several approaches for (2, 2) – Threshold VCS. In this figure first approach shows that each pixel is broken into two sub pixels. Let B shows black pixel and W shows white pixel. Each share will be taken into different transparencies. Following combinations are generated when both transparencies are placed over each other. For black pixel BW+WB=BB or WB+BW=BB and for white pixel BW+BW=BW or WB+WB=WB. In Similar way a second approach is also given where each pixel is divided into four sub pixels. We can achieve 4c2 = 6 unique cases for this approach.

1: Each Pixel is broken into two sub pixels as follows.

F.S: First Share.

S.S: Second Share.

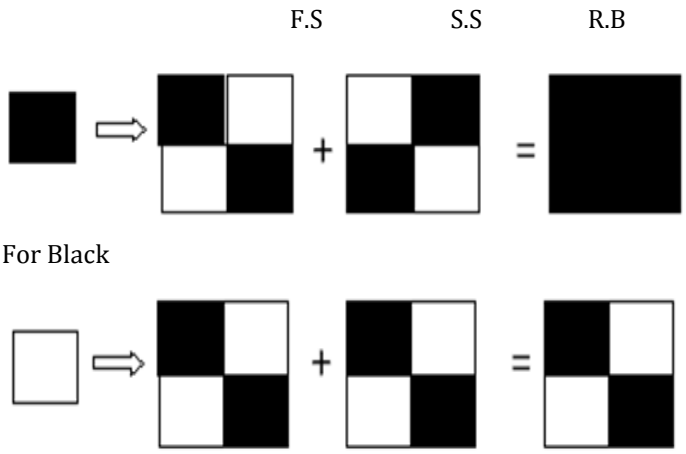
R.B: Resultant Block.



For Black

For White

2: Each Pixel is broken into four sub pixels as follows.



For Black

For White

Fig -2: (2, 2) – Threshold VCS

1.2 Digital Watermarking

The process of embedding a digital signal (image, audio or video) with information which cannot be removed easily is called digital watermarking. This information is not usually visible and only dedicated receiver can see and extract that information. Basic working of digital image watermarking can be divided in three stages [8].

1.2.1 Embedding Stage

This is the first stage of watermarking in which the watermarked image is generated when the secret information is embedded into the host image by using an embedding algorithm and a secret key. The generated watermarked image is then eventually shared on the network.

1.2.2 Distortion/Attack Stage

In this stage, when the watermarked image containing secret information is transmitted over the network, some noise is added or some attacks may be performed on the watermarked image.

1.2.3. Detection/Retrieval Stage

In the last stage, some detection algorithm and a secret key is used to retrieve the secret information by the dedicated detector from the watermarked image. Some noise is also detected in the secret information. Fig -3 shows the basic block diagram of watermarking process.

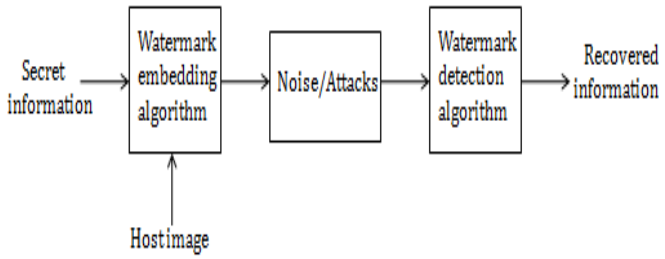


Fig- 3: Watermarking block diagram [12]

1.3 Categorization of Different Watermarking Techniques.

Digital watermarking techniques which are categorized into various types, based on different criteria are shown in Table -1 below: [9].

Table -1: Types of watermarking techniques based on different Criteria's [9]

S.no	Criteria	Classification
1.	Watermark Type	1. Noise: pseudo noise, Gaussian random and chaotic sequences 2. Image: logos, Stamps Images etc.
2.	Robustness	1. Fragile: Easily Manipulated. 2. Semi-Fragile: immune to some type of attacks 3. Robust: not affected from any attack
3.	Domain	1. Spatial: LSB, Spread Spectrum. 2. Frequency: DCT, DFT, DWT, SVD.
4.	Perceptivity	1. Visible: Channel logo 2. Invisible: Steganography
5.	Host Data	1. Audio Watermarking 2. Image Watermarking 3. Text Watermarking 4. Video Watermarking
6.	Data Extraction	1. Non- Blind 2. Semi-Blind 3. Blind

1.4 Techniques of Watermarking

Digital watermarking is majorly categorized in spatial or frequency domain [10, 11]. Based on application's requirement different watermarking techniques can be selected.

1.4.1 Spatial domain techniques

Spatial domain watermarking involves the selecting of the pixels within an image to be modified based on their location and it is very prone to cropping, geometric and mosaic attack. The spatial domain watermarking is easier and faster than transform domain techniques but it is less robust against attacks. The advantage of spatial domain technique is that it can be easily applied to any image and the most important method of spatial domain is LSB [5] is described below.

1.4.1.1 Least Significant Bit (LSB)

LSB coding is one of the earliest methods of watermarking. It can be applied to all forms of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. These bits are then embedded in a sequence which acts as the key. This sequence should be known in order to retrieve the watermark. [12].
Image:

10010101 00111011 11001101 01010101….

Watermark:

1 0 1 0…..

Watermarked Image:

1001010**1** 0011101**0** 1100110**1** 0101010**0**…..

1.4.2 Transform domain techniques

Transform domain watermarking techniques are also called frequency domain watermarking. In this technique values of the certain frequencies are modified from their original values. Generally the frequency modifications are done in the lower frequency levels, since modification at the higher level frequencies are lost during compression. Watermarking in the frequency domain involves immersing in the image's transform coefficients. Most commonly used transform domain watermarking techniques are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT).

1.4.2.1 Discrete Cosine Transform

DCT is used in signal processing to transform the signal from the spatial domain to the frequency domain. It is more robust as compared to the spatial domain watermarking techniques as it is more robust against various signal processing attacks because of the selection of perceptually

significant frequency domain coefficients. The main steps used in DCT are [10]:

1) Divide the image into non-overlapping blocks of size 8x8.

2) Forward DCT is then applied to each of these blocks.

3) Some block selection criteria are applied (ex- HVS).

4) The coefficient selection criteria is applied (ex- highest).

5) Embed the watermark by modifying the selected Co-efficient.

6) Apply inverse DCT transform on each block.

An image is split into different frequency bands to embed the watermark information, Fig -4 shows the various DCT regions where FL denotes the lowest frequency component of the block, while FH denotes the higher frequency component of the block and FM denotes the middle frequency component of the block. The FM band is chosen as the embedding region.

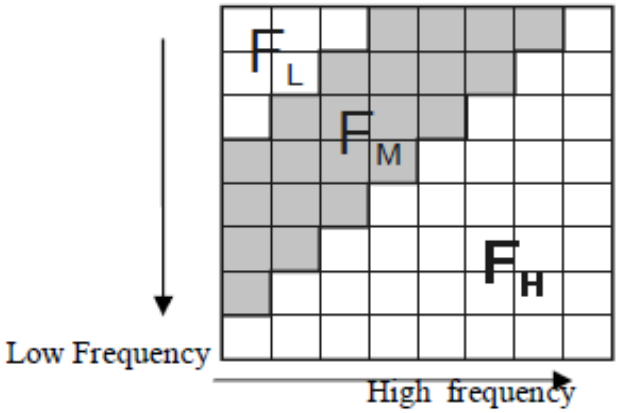


Fig- 4: Discrete Cosine Transform Region [12].

1.4.2.2 Discrete Fourier Transform

DFT divides an image into sine and cosine forms. The DFT based watermark embedding techniques are divided in two types: the direct embedding and the template based embedding. In the direct embedding technique the watermark is inserted by modifying the DFT magnitude and phase coefficients. There is a concept of templates in the template based embedding technique. To estimate the transformation factor a structure is embedded in the DFT domain known as template. This template is searched to resynchronize the image when the image undergoes a transformation, and then the embedded spread spectrum watermark is extracted by using a detector [11]. It offers robustness against geometric attacks like rotation, scaling, cropping, translation etc. Some major characteristics [14] of DFT are:

1) DFT of an original image is represented in the complex form *ie* the image is represented in magnitude and phase.

2) DFT shows invariance to translation attacks. Spatial shifts in the image affects only the phase representation of the image but not the magnitude representation. The magnitude of the Fourier transform is not affected by the circular shifts in the spatial domain.

3) DFT is resistant to cropping because the effect of cropping results into the blurring of spectrum. If the watermarks are embedded in the magnitude, these are normalized coordinates, there is no synchronization is needed.

4) The powerful components of the DFT are the main components which contain the low frequencies.

5) Image scaling results in amplification of retrieved signal and can be detected by correlation coefficient. Image translation has no result on extracted signal.

6) Image rotation results in cyclic shifts of retrieved signal and can be detected by exhaustive search.

7) Scaling in the spatial domain causes inverse scaling in the frequency domain. Spatial domain rotation causes the same rotation in the frequency domain.

1.4.2.3 Discrete Wavelet Transform

DWT watermarking schemes are conceptually same as DCT based schemes but the transformation process of an image into its transform domain is different and therefore the resulting coefficients are also different. Wavelet transforms use different kind of filters to transform the image into multi resolution representation. There are many filters used in DWT, but the most common filters used in watermarking are Daubechies Bi-Orthogonal Filters, Haar Wavelet Filter and Daubechies Orthogonal Filters. Each of these filters decomposes the image into many frequencies. The Single level decomposition of an image gives four frequency sub bands. These four representations are called the LL, LH, HL, HH sub bands as shown in Fig -5.

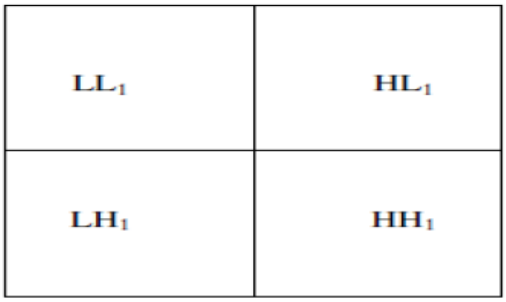


Fig -5: Single level decomposition using DWT [14]

3 REVIEW

The comprehensive study of literature shows that the use of watermarking provides more security to image shares containing secret information because some image can be shown in place of shares with only black and white pixels in the basic visual cryptography scheme. Watermarking in the spatial domain involves selecting the pixels to be modified based on their location within the image. In comparison to

frequency domain techniques the spatial domain techniques are very susceptible to cropping and geometric attacks. Any translation, rotation, scaling, compression change to the image can damage the watermark. Various attempts are made to increase the security, visual quality of the secret image shares using different watermarking techniques. Some of them are as follows.

In 2008, S.Riaz et al. [4] proposed two invisible watermarking schemes in spatial and frequency domains. In FFT (Fast Fourier Transform) based approach the data that was to be embedded has been pre- processed before embedding. For that purpose an encryption key has been used to encode the text data. The pre-processing of both the schemes was similar but the insertion and extraction algorithms were different in two domains. The techniques used in spatial domain were not robust against many attacks but it gives useless information to the attacker unless he has the decoding key. It has been observed that the scheme in frequency domain was robust against a number of attacks. It has been observed that the spatial domain is less robust and therefore vulnerable to number of attacks. The FFT can be further enhanced to prevent the rotation attack on the image.

In 2008, Bani et al. [3] proposed an approach of securing the image shares by a watermarking technique called Data hiding by conjugate error diffusion (DHCED) algorithm [15] proposed by Ming Sun et al. In this scheme, first the secret image is converted into halftone images using density of the net dots to simulate the original grey level or colour level in the target binary representations. After this step shares of black and white pixels were generated. Various other techniques of halftoning such as error diffusion, thresholding and ordered dithering were also suggested. For watermarking DHCED algorithm is used in which shares generated from first step were embedded in some cover images. Secret and cover images were revealed just after overlapping the shares but the visual quality of the revealed image is not good as compared to original image.

In 2009, Debasish Jena and Sanjay Jena [2] proposed Data hiding technique using conjugate ordered dithering algorithm (DHCOD), which was a modified version of existing DHCED algorithm [15]. The two major modifications done in DHCED algorithm were the noise inclusion step in the secret image and the use of ordered dithering technique with respect to error diffusion technique in the halftoning technique. This scheme also has drawbacks as the visual quality of the revealed image is not good and low in contrast. In first and second steps of this scheme, some noise was added to the secret image and the image converted into a binary image. In the third and fourth steps, two image shares are generated. Share 1 is the generated dithered halftone image of some cover image and Share 2 is generated by XORing the Share 1 and binary secret image generated after second step. The secret image was revealed with the simple AND operation on share 1 and share 2. Fig.6 shows the working model of DHCOD algorithm.

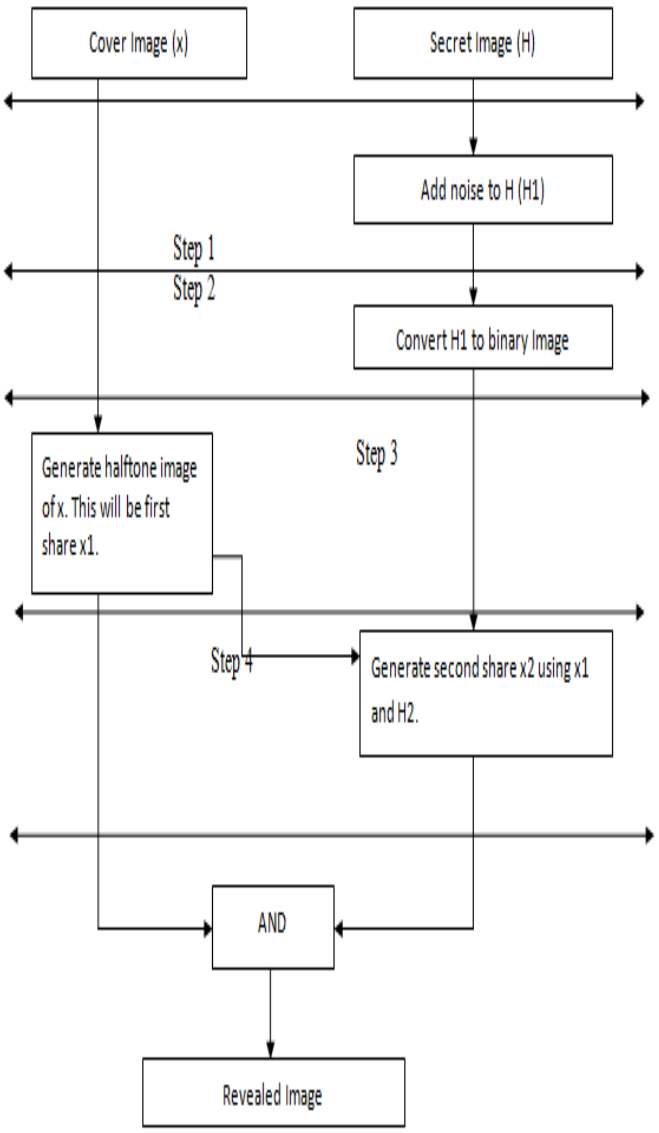


Fig -6: Working model of DHCOD algorithm [2]

In 2010, B.padhmavati et al. [6] proposed a scheme to protect secure image shares by using invisible and blind watermarking algorithm. In this paper the shares was generated using VC (2, 2) scheme then both the shares were embedded into the cover images with the help of an invisible and blind watermarking. The non-overlapping blocks of size 2x2 were extracted from the host image. A pixel of binary watermark image was embedded into a single block. The watermark embedding process involved using of mean calculation, embedding strength (γ) and the signum function. Each non-overlapping block was then converted into a vector, and the mean value of the vector was computed. Afterwards, the mean value was divided by the embedding strength (γ) and used in the embedding. As the watermark was a binary image, the embedding of watermark involved two cases: embedding pixel value '1' and embedding pixel

value '0'. Two distinct mathematical operations were performed for embedding pixel value '0' and '1'. To reveal the secret share, 2x2 non overlapping blocks were extracted from the watermarked image and the number of blocks extracted depends on the size of the watermark image. The blocks thus extracted were stored in a vector. After that all the extracted blocks were converted into a vector and the mean value of the vector was calculated. Subsequently the mean values of all the blocks were divided by the embedding strength. The resultant value was utilized in the extraction of watermark. Finally, a matrix with size of watermark image was initialized and the extracted pixel values were placed in it in order to obtain the watermark image. After that, both shares were overlapped and revealed the secret image. Fig -7 shows the working model of the scheme.

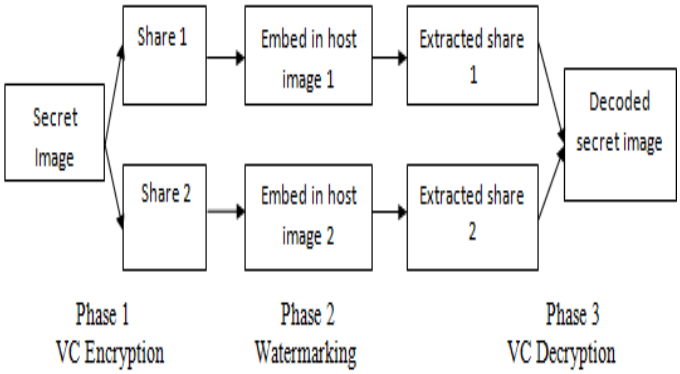


Fig -7: Working model of the scheme [6]

In 2010, Mathivadhani and Dr.C.Meena [5] proposed a digital watermarking and information hiding scheme using Wavelets, SLSB and the Visual cryptography method. The main objective of this paper was to hide an iris message and a secret message into a cover image. The objective was achieved in three phases. In the phase1, visual cryptography is applied on the secret message to obtain two shares S1 and S2. In the phase2, iris analysis has been performed to extract important features to obtain a condensed version, ICI, of the original image. In the last phase, shares S1, S2 and ICI are embedded into the lower frequency sub bands of the cover image obtained after DWT using SLSB (Selected Least Significant Bit) technique. The replacement algorithm used SLSB can be replaced by a more sophisticated algorithm. The process behind SLSB is shown in Fig- 8.

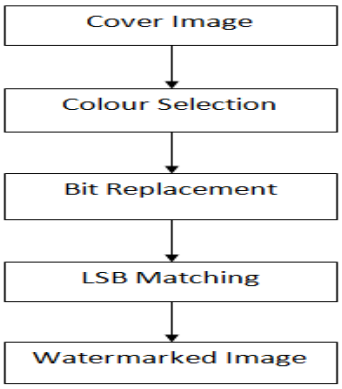


Fig -8: SLSB Algorithm [5]

In 2012, A. Kaushik [16] proposed a watermarking scheme for images based on DFT and the image segmentation techniques. In this scheme, the cover image was first divided into the blocks of 256*256 and transformed them with DFT. After that Arnold scrambling scheme modifies the watermark and generate two pseudo-random sequences and lastly DFT is used to generate the image with watermark. The watermark detection was also achieved with image segmentation process, DFT transform process and the relativity process.

In 2014, P. Parashar et al. [12] and V. Gupta et al. [14] presented a detailed analysis of various digital image watermarking techniques in spatial and transform domains and their applications in the real world. It also discusses the advantages and disadvantages of these techniques over each other. It also analyses the limitations and strengths of different watermarking methods based on their performances so that they can be used in different scenarios as per requirements.

3. CONCLUSIONS

Visual cryptography is the current area of research where the scope is unlimited. Currently watermarking and visual cryptographic technique is being used by several countries for secretly transmission of hand written documents, financial documents, text images and also for internet voting etc. There are various innovative ideas and extensions exist for the basic visual cryptographic model to enhance the security and authentication. It can be observed from literature review that a scheme could be developed that add the advantages of both visual cryptography as well as watermarking technique. Visual cryptography encryption adds the advantage and security of the basic scheme but watermarking adds the required protection to the image shares by embedding shares into a cover image without affecting its perceptual quality and later the secret image's share can be revealed by watermark extraction process. Watermarked images are robust against a number of attacks like blurring, sharpening, motion blurring, etc. The watermarking scheme provides more meaningful shares of secret image. Since it would provide high security of secret

image so it could be useful in transmission of financial documents. More applications can also be developed which require a high level security.

In particular it has also been observed that the watermarking scheme in frequency domain is more robust [2, 3, 4, 5, 11] against a number of attacks. The quality of the cover image remains good after watermarking of the secret image therefore it can be concluded that the frequency domain is better where there is no compromise can be done on security.

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.

[7] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Visual Cryptography for General Access Structures, Information and Computation, Vol. 129, No. 2, (1996), pp. 86-106.

[8] L. Robert and T. Shanmugapriya," A Study on Digital Watermarking Techniques", International Journal of Recent Trends in Engineering, vol. 1, no. 2, (2009).

[9] L.K Saini, V. Shrivastava," A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and Technology – Vol2 Issue 3, (2014).

[10] V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

[11] N. Chandrakar and J. Baggaa, "Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130.

[12] P. Parashar, R.K Singh, "A Survey: Digital Image Watermarking Techniques", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 7, No. 6 (2014), pp. 111-124

[13] N.S. Narwade, N.P. Deshmane, Pankaj Elchatwar, Pooja,L. Pande, "Robust Watermarking for Geometric attack using DFT", International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue2, (2013).

[14] V.Gupta, A.Barve, "A Review on Image Watermarking and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, (2014).

[15] Ming Sun Fu and Oscar C. Au "Data hiding in halftone images by conjugate error diffusion" D- 7803-7761-3/03 © 2003 IEEE.

[16] Awanish Kr Kaushik, "A Novel Approach for Digital Watermarking of an Image Using DFT", International Journal of Electronics and Computer Science Engineering, Volume 4, Issue 1, (2012), pp. 35-41.