

# Hybrid Algorithm Implemented on Color Image to Design Watermark Image with PSNR & MSE baesd on Cryptography

Garima Sharma

*Department of Computer Science and Engineering  
KIIT College of Engineering, Gurgaon, Haryana –122102*

Shweta Tyagi

*Department of Computer Science and Engineering  
KIIT College of Engineering, Gurgaon, Haryana –122102*

Sharvan Rewri

*Assistant Professor  
KIIT College of Engineering, Gurgaon, Haryana -122102*

**Abstract-** Visual Cryptography (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. During the past decade, with the development of information digitalization and internet, digital media increasingly predominate over traditional analog media. 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. Share generation for the visual cryptography can also be done using watermarking technique. We can use these watermarked shares for retrieving the hidden information. This effort can generate the meaningful shares rather than some shares having no information.

**Keywords –** cryptography, encryption, digital watermarking, host image, spatial domain, predictive coding, patch work, wavelet and discrete cosine transform.

## I. INTRODUCTION

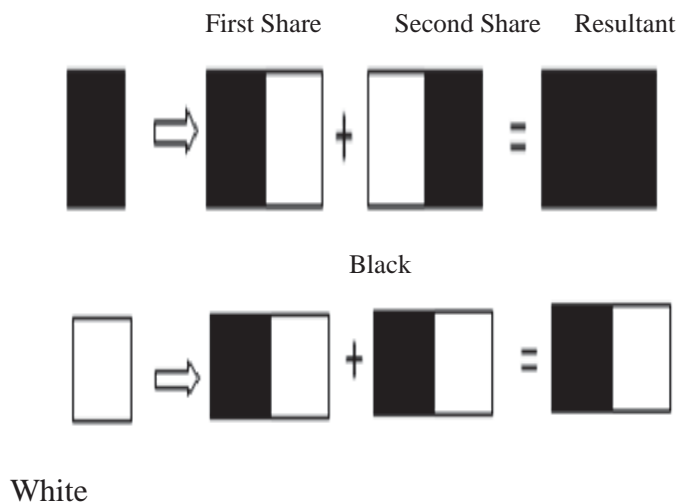
Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Such a technique thus would be lucrative for defense and security. Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret image. The act of decryption is to simply stack shares and view the secret image that appears on the stacked shares. Visual cryptographic technique is being used by several countries for secretly transfer of images in army, hand written documents, financial documents, text images, internet- voting etc. The digital watermark is then introduced to solve this problem. Covering many subjects such as signal processing, communication theory and Encryption, the research in digital watermark is to provide copyright protection to digital products, and to prevent and track illegal copying and transmission of them. Watermarking is embedding information, which is able to show the ownership or track copyright intrusion, into the digital image, video or audio. Its purpose determines that the watermark should be indivisible and robust to common processing and attack. The proposed scheme adds the advantages of both visual cryptography as well as invisible watermarking technique. Visual cryptography encryption adds the advantage and security of basic scheme. Watermarking is used for embedding shares into cover image without affecting its perceptual quality so that the secret image's share can be revealed by watermark extraction process.

## II. BACKGROUND

With the rapid advancement of network topology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identification are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with security problems of secret images, we should develop some secure appropriate algorithm by which we can secure our data on internet. . Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique  $n-1$  shares reveals no information about the original image. We can achieve this by using one of following access structure schemes

Figure 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. Let B shows black pixel and T shows Transparent (White) pixel. Each share will be taken into different transparencies. When we place both transparencies on top of each other we get following combinations, for black pixel  $BT+TB=BB$  or  $TB+BT=BB$  and for white pixel  $BT+BT=BT$  or  $TB+TB=TB$ . Similarly second approach is given where each pixel is broken into four sub pixels. We can achieve  $4C2 = 6$  different cases for this approach

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



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

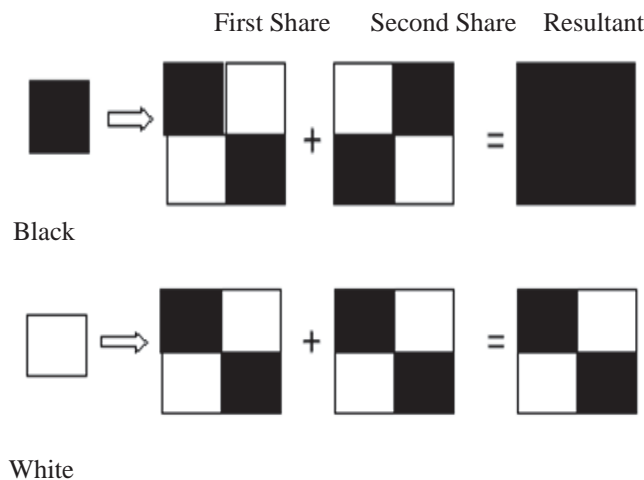


Fig. 1 Pixel is broken into four sub pixel

### III. DESCRIPTION OF SYSTEM DESIGN AND METHODOLOGY

Information hiding can be mainly divided into three processes - cryptography, stenography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Watermarking is closely related to stenography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication.

#### *Principle of Watermarking:*

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it [1-2]. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. Figure 2 shows the basic block diagram of watermarking process.

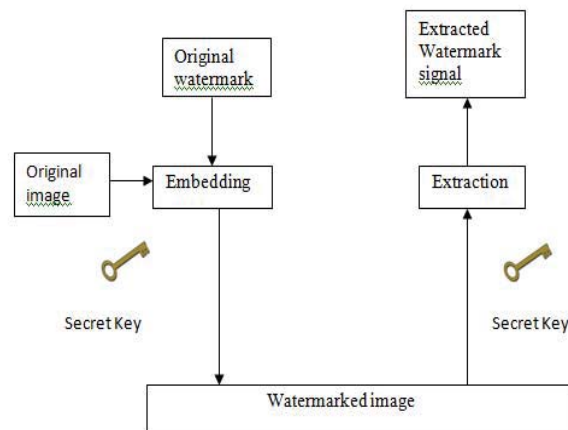


Fig. 2 Watermarking block diagram

#### *Classification of Watermarking:*

It can be classified in visible and invisible watermarking.

- Visible: The watermark is visible which can be a text or a logo used to identify the owner.

Any text or logo to verify or hide content

$$F_w = (1-\alpha) F + \alpha W$$

$F_w$  = Watermarked Image

$\alpha$  = constant;  $0 \leq \alpha \leq 1$ , IF  $\alpha=0$  No watermark, if  $\alpha=1$  watermark present

$F$  = original image

$W$  = watermark

- Invisible: The watermark is embedded into the image in such a way that it cannot be perceived by human eye. It is used to protect the image authentication and prevent it from being copied. Invisible watermark can be further divided into three types. Robust Watermarks, Fragile Watermarks, Public and Private Watermark

#### A. *Techniques of Watermarking*

Digital watermarking is addressed mostly in spatial or frequency domain. Based on application's requirement different watermarking techniques can be selected. Most of the present work in the area of digital watermarking is inspired by the manipulating the frequency domain of the multimedia objects. In frequency domain, researchers have selected different transformation methods for embedding and extracting watermark objects. These includes Discrete Cosine Trans-form (DCT), Discrete Fourier Transform (DFT) and Wavelets.

- 1) *Frequency Domain techniques:* Frequency domain watermarking technique is also called transform domain. Values of certain frequencies are altered from their original. Typically, these frequency alterations are done in the lower frequency levels, since alterations at the higher frequencies are lost during compression. Watermarking in the frequency domain involves embedding in the image's transform coefficients.
- 2) *Discrete Cosine Transform (DCT) Technique:* Discrete cosine transform (DCT): It is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to set of n coefficients [3-5]. A linear combination of n known basis vectors weighted with the n coefficients will result in the original vector. The known basis vectors of transforms from this class are "sinusoidal", which means that they can be represented by sinus shaped waves or, in other words, they are strongly localized in the frequency spectrum. Therefore one speaks about transformation to the frequency domain. The most popular member of this class is the Discrete Fourier Transformation (DFT).The difference between DCT and DFT is that DFT applies to complex numbers, while DCT uses just real numbers. For real input data with even symmetry DCT and DFT are equivalent.

The coefficients can be split using the zigzag ordering into low frequency coefficients, mid frequency coefficients and high frequency coefficients as shown in Fig.3

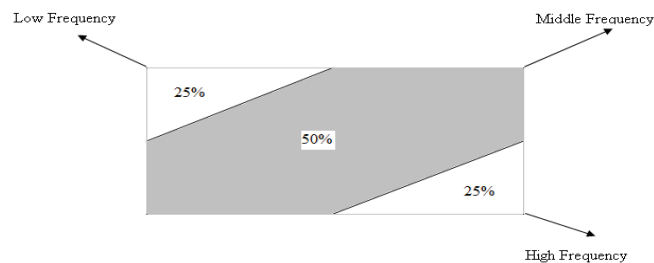


Fig. 3 DCT Decomposition

Figure 4 shows the structure of the proposed scheme. The proposed scheme generates the VC shares using basic visual cryptography model and then embed them into a cover image using invisible blind watermarking technique, so that the secret shares[6-7] will be more secure, meaningful and shares are protected from the malicious adversaries who may alter the bit sequences to create the fake shares. During the decryption phase, secret shares are extracted from the respective cover images without using any cover image characteristics to provide mutual authentication

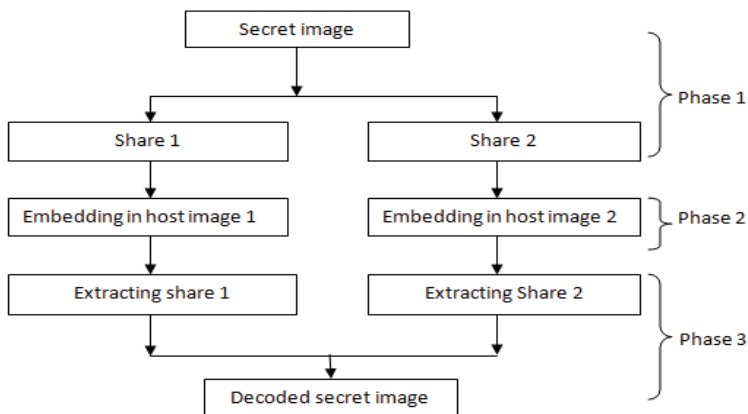


Fig. 4 Structure of the Proposed Scheme

Any single share is a random choice of two black and two white sub pixels, which looks medium grey. Fig.5 shows share creation using VC (2, 2) Encryption. When two shares are stacked together, the result is either medium grey (which represents white) or completely black (which represents black).

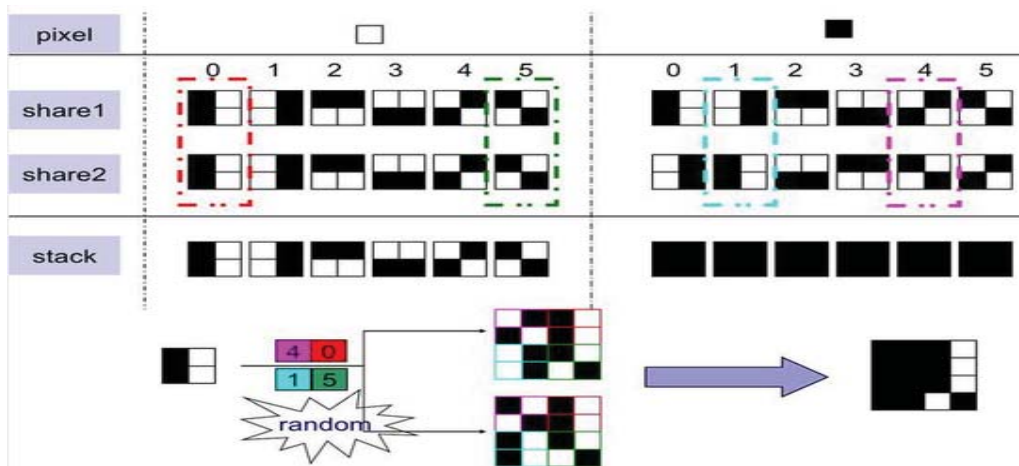


Fig. 5 Share creation using VC (2, 2) encryption Scheme

#### IV. RESULT

*RESULT I: Peak Signal to Noise Ratio*

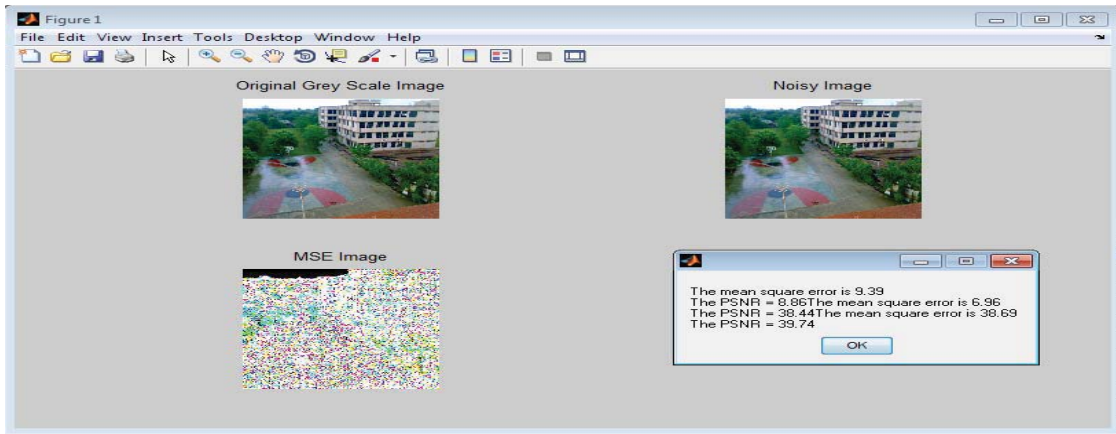


Fig. 6 show PSNR and RMSE of different images

TABLE I

PSNR & MSE of Different Image

| Sr. No. | Types of Images           | PSNR  | MSE   |
|---------|---------------------------|-------|-------|
| 1       | Original Gray scale image | 8.86  | 9.39  |
| 2       | Noisy Image               | 38.44 | 6.96  |
| 3       | Mean Square Error image   | 39.74 | 38.69 |

*RESULT II: Sharpe Images*

In result II we calculated the sharp images elapsed time from given watermark images. As shown in figure 7 which are watermark images and then determine extracted secret message then shared and finally revealed message.



(a)



(b)



(c)



(d)



Fig. 7 show watermark images (a, b) and then determine extracted secret message(c, d) then shared and finally revealed message (e, f)

- Elapsed time of first image is=1.3260
- Elapsed time of first image is=0.9828



Fig.8 Elapsed time of Fig.7 images

In the same way we calculate result for blurred image and extracted secret image, shared image and finally revealed image of both image and their processing time.

- Elapsed time of first image is=1.2324
- Elapsed time of first image is=0.9828

*RESULT IV: Blurred Images*



Fig.9 original image of size 40\*15



Fig.10 extract1 message of Fig.9



Fig.11 extract2 message of Fig.9



Fig.12 share1 message of Fig.9



Fig.13 share1 message of Fig.9



Fig.14 output message of Fig.9

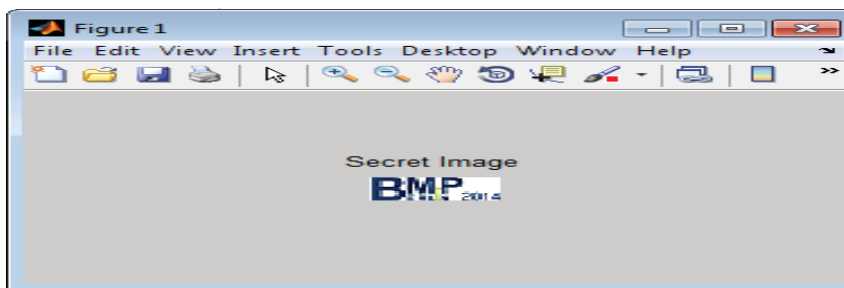


Fig.15 secret message

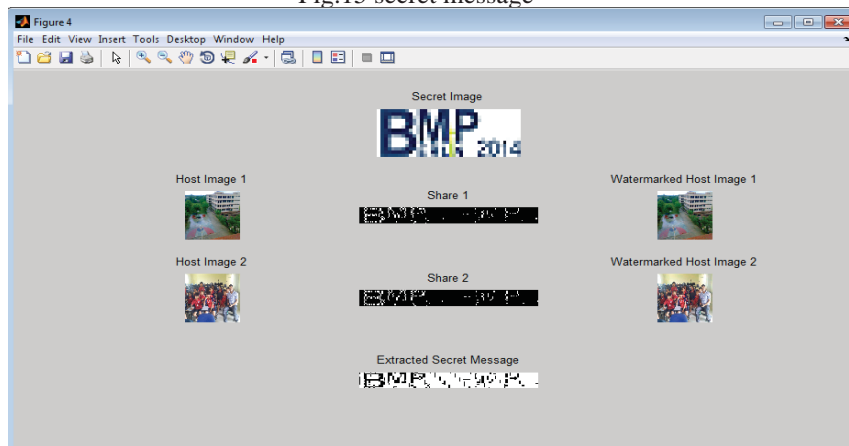


Fig.16 show Snapshot of all images obtained by cryptography ie host image1, 2 and watermark image1, 2, secret message, share1, share2, extracted secret message

```

Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

White Pixel Processing...
Black Pixel Processing...
Share Generation Completed.

elapsed_time =
    1.4664

elapsed_time =
    1.1388

fx >> |
    
```

Fig. 17 white and black pixel processing time of image is listed below  
White and Black pixel processing time:



- White pixel processing Time:1.4664
- Black Pixel processing time:1.1388

## V. CONCLUSION

The proposed scheme used visual cryptography for share generation and each share is embedded in a cover image using digital watermarking. Visual cryptography encryption adds the advantage and security of basic scheme. Watermarking provided double security to shares by hiding them in some cover images. Watermarked images are robust against a number of attacks like blurring, sharpening, cropping etc.

## REFERENCES

- [1] B.padmavati, P.Nirmal Kumar, M.A.Dorai Rangaswamy, 2010. A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography Using Image Processing. In *Proceedings of International Conference on Advances in Computer Science 2010* DOI: 02, ACS.2010.01.264, ACEEE.
- [2] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of out of visual secret sharing schemes," *Designs, Codes, Cryptography*, vol. 11, no. 2, pp. 179-196, May 1997.
- [3] H. Hajiabolhassan and A. Cheraghi, "Bounds for visual cryptography schemes," *Discrete Appl. Math.*, vol. 158, no. 6, pp. 659-665, Mar. 2010.
- [4] 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.
- [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 (ICCI'2010)*, pp. 1-4.
- [6] S. J. Shyu, "Image encryption by random grids," *Pattern Recognit.*, vol. 40, no. 3, pp. 1014-1031, Mar. 2007.
- [7] M.Naor and A.Shamir, 1995. Visual cryptography. *Advances in Cryptology EUROCRYPT '94*. Lecture Notes in Computer Science, (950):1-12.
- [8] P.S.Revenkar, Anisa Anjum, W.Z.Gandhare, 2010. Survey of Visual Cryptographic Schemes. *International Journal of Security and Its Applications*, Vol. 4, No. 2, April, 2010.
- [9] S.Punitha, S.Thompson, N.Lingam, 2010. Binary Watermarking Technique based on Visual Cryptography. In *Proceedings of International Conference on Communication Control and Computing Technologies ( ICCCT'2010)*, pp. 232-235.
- [10] 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.
- [11] Y.Bani, Dr.B.Majhi and R.S.Mangrulkar, 2008. A Novel Approach for Visual Cryptography Using a Watermarking Technique. In *Proceedings of 2<sup>nd</sup> National Conference, IndiaCom 2008*.
- [12] F. Liu, C. K. Wu, and X. J. Lin, "A new definition of the contrast of visual cryptography scheme," *Inf. Process. Lett.*, vol. 110, no. 7, pp. 241-246, Mar. 2010.
- [13] R. Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 659-662, Aug. 2009.
- [14] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," *Designs, Codes, Cryptography*, vol. 25, no. 1, pp. 15-61, 2002.
- [15] Y.Bani, Dr.B.Majhi and R.S.Mangrulkar, 2008. A Novel Approach for Visual Cryptography Using a Watermarking Technique. In *Proceedings of 2<sup>nd</sup> National Conference, IndiaCom 2008*.
- [16] G. B. Horng, T. G. Chen, and D. S. Tsai, "Cheating in visual cryptography," *Designs, Codes, Cryptography*, vol. 38, no. 2, pp. 219-236, Feb. 2006.
- [17] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. Fundam. Electron., Commun., Comput. Sci.*, vol. 82, pp. 2172-2177, Oct. 1999.
- [18] 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.
- [19] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. Fundam. Electron., Commun., Comput. Sci.*, vol. 82, pp. 2172-2177, Oct. 1999.
- [20] F. Liu, C. K. Wu, and X. J. Lin, "Colour visual cryptography schemes," *IET Inf. Security*, vol. 2, no. 4, pp. 151-165, Dec. 2008.
- [21] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Comput.*, vol. 129, no. 2, pp. 86-106, Sep. 1996.