Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018)
IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1

Visual Cryptography based Grayscale Image Watermarking in DWT domain

Pranesh Kulkarni
Department of Computer Science and Engineering
KLS's VDR Institute of Technology
Haliyal, India

Girish Kulkarni
Department of Master of Computer Applications
BLDEA's V.P. P.G. Halakatti College of Engg. and Tech.
Vijayapur, India

***Abstract*—Watermarking is a technique to protect the copyrights of digital media like image, audio, video, etc. Visual Cryptography (VC) is a scheme for hiding information in still images. The Visual Cryptography Scheme splits the secret image into unintelligible images, these images are called shares. The shares are distributed to 'n' participants. Any 'k' shares out of 'n' reveal the secret image and less than 'k' shares recover no information about secret. Amalgamating Visual cryptography with watermarking yields the best solution for resolving image ownership disputes and detection of infringements of copyrights. In this paper, (2,2) VC scheme is employed, one of the shares is embedded in the low frequency domain of DWT and the other share is registered with the Trusted Authority(TA). The secret image is obtained by performing XOR operation on the two shares. The experimental results revealed that the proposed scheme can not only prove the ownership of image but also withstand various image processing attacks.**

***Index Terms*—Visual Cryptography, Discrete Wavelet Transform (DWT), Digital Watermarking, Copyright Protection.**

I. INTRODUCTION

With the dawn of Internet and Computer Networks enormous amount of digital data is generated and disseminated in everyday life. The tremendous growth of data is posing new challenges in securing and managing copyrights of the digital material [1] one of the facets of this digital data is ease of duplication. Hence copyright protection if digital data is the need of the hour in the current digital society.

Problems related to copyright protection can be solved by adopting watermarking techniques. The watermarking technique must meet the following properties:

- Robustness: The resiliency of watermark from attack.
- Imperceptibility: The watermarked image and original image must be indistinguishable to Human Visual System (HVS).
- Security: The authorized owner must be able to elicit the watermark.
- Blindness: The original image is not required for extraction of watermark.
- Unambiguity: The extracted watermark must conclude the ownership of the image.

Hitherto, myriad of watermarking techniques have been proposed in last few years. These watermarking techniques are broadly categorized into spatial domain and frequency domain or transform domain techniques.

The earlier literature elucidated that compared to spatial domain techniques; frequency domain techniques are more robust. Cox [4] put forward the watermarking ides which provides robustness against attacks but it requires original image for extraction. Zhang Nana [2] proposed watermarking in spatial domain using Singular Value Decomposition (SVD) and scrambling technology. It meets blindness and robustness property but the embedding capacity is small. The technique proposed by Jobin et.al[3] for color image watermarking in spatial domain using two masks meets imperceptibility property. [5] Focuses on watermarking scheme for multiple cover images and multiple owners. It uses Visual Cryptography scheme. [6] provides VC based watermarking in which shares are generated using the codebook.[7] proposed the basic idea of Visual Cryptography based on Visual Secret Sharing Scheme (VSS).

In this paper, copyright protection proposed is based on VC and Discrete wavelet transform. First, the feature extraction from cover image is carried out using wavelet decomposition. The watermark image is split into two shares using (2,2) VC scheme. One of the shares is registered with arbitrator (TA) and other is embedded in the host image. Finally the extraction process recovers original watermark by performing XOR operation between the shares.

The rest of the paper is organizes as follows: section 2 discusses the VC scheme, wavelets and proposed algorithms for embedding and extraction. Section 3 gives look on experimental observations and conclusion is presented in section 4.

II. PROPOSED SCHEME

A) Visual Cryptography

The core concept of Visual cryptography was proposed by Naoir and Shamir [7]. Generally (k,n) VC scheme takes binary image as input and produces 'n' shares as output, satisfying two conditions: first, 'k' out of 'n' shares reveal the secret and

second, any 'k-1' shares cannot uncover any secret information. The operation of VC scheme can be XOR or OR [7]. In this paper, XOR based operation is used, as it provides better visual quality of recovered image than OR.

In this paper (2,2) VC scheme is adapted, where each pixel is associated with two pixels i.e. pixel expansion is 2. This results in enlarging of the input image and introduces distortion. In order to reduce the distortion pixel expansion of larger size can be used replacing each pixel by 4 (2x2) sub pixels as shown in fig. 1.

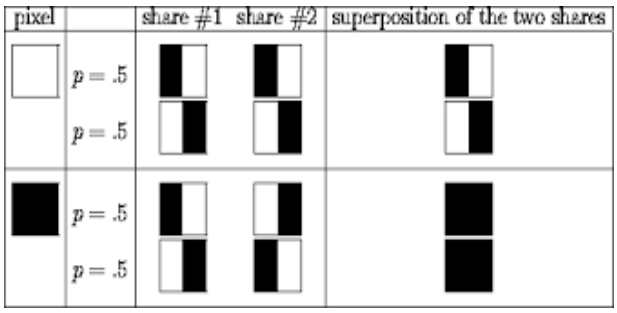


Fig. 1. (2,2) VC Scheme with pixel expansion 4

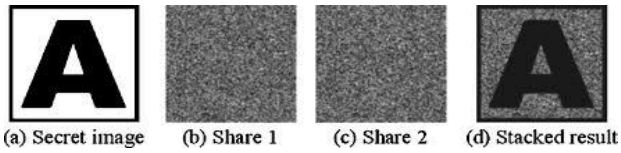


Fig. 2. Shares generation and reconstruction using (2,2) VC scheme

B) Discrete Wavelet Transform

Wavelet theory was originally presented by J.Morlet, A.Grossman and Y.Meyer. Later Mallet and Daubechies provided the bonding between wavelet and signal processing. Wavelet transform overcome the limitation of Fourier transform of having both frequency and temporal information simultaneously.

Discrete wavelet transform is based on sub band coding, which provides multiresolution analysis of digital signal. DWT can be achieved using digital filter banks. The signal is passed through different cut-off frequencies at various scales.

If x[n] is original signal, it is passed through half band high pass filter g[n] and low pass filter h[n]. This results in 1-level decomposition, which is given by eqn 1 and eqn 2:

$$y_{low}[k]=\sum_n x[n] * h[2k-n] \quad (1)$$

$$y_{high}[k]=\sum_n x[n] * g[2k-n] \quad (2)$$

where $y_{low}[k]$ and $y_{high}[k]$ are the outputs of low and high pass filters respectively. The same process can be repeated to get the next level of decomposition.

The reconstruction can be obtained using Inverse Discrete wavelet transform (IDWT), which is given by eqn 3:

$$x[n]=\sum_k (y_{high}[k]*g[-n+2k]+y_{low}[k]*h[-n+2k]) \quad (3)$$

The DWT and IDWT of an image 'I' is obtained by applying wavelets separately to rows and columns of image. The DWT of an image results in 4 sub bands LL, HL, LH and HH as shown in fig. 3. LL is low frequency band and LH, HL and HH are high frequency bands as shown in fig. 4

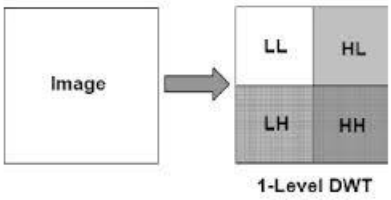


Fig. 3. 1- Level Discrete Wavelet Transform

Fig. 4. 1- Level Discrete Wavelet Transform of Lena image.

In this paper LL band is used to embed one of the shares of watermark, which results provides robustness against attacks.

C) Algorithm for Watermark Embedding

Input: cover image (I), watermark image (W)
Output: watermarked image (WI)

Step1: Read a grayscale image as cover image (I).

Step 2: Decompose 'I' into different frequency sub bands Using 1-level DWT.

Step 3: Read a binary image as secret image or watermark Image (W) to be embedded in 'I'.

Step 4: Apply (2, 2) VC Scheme to generate shares S1 and S2 of 'W'.

Step 5: Embed 'S1' in LL sub band of 'I' using the eqn. 4

$$LL`(i,j)=LL(i,j)+\alpha*S1 \quad (4)$$

Where α is embedding intensity factor $0< \alpha<1$.

Step 6: Register share S2 with Trusted Authority (TA).

Step7: Perform Inverse DWT and the resulting image is Watermarked image (WI).

Step 7: Compare I and WI images using the parameters, Peak Signal to Noise Ratio (PSNR) and Normalized Cross Co-relation (NC). If the values are above the threshold then watermarking technique has satisfied imperceptibility property.

D) Algorithm for Watermark Extraction

Input: Attacked Image (WI`), share S2.
Output: watermark image (W`).

Step1: Read the attacked image (WI`)

Step 2: Apply 1-level DWT to obtain different frequency sub bands.

Step 3: Extract share S1 from LL sub band using the Eqn. 5

$$S1= (LL`-LL)/ \alpha \quad (5)$$

Step4: Obtain the share S2 from Trusted Authority.

Step 5: Watermark can be recovered from the S1 and S2 by performing XOR operation as given below.

$$W=S1 \oplus S2 \quad (6)$$

Step 6: Compare W and W` using PSNR and NC parameters.

III. Experimental results

This section discusses about results of the experiments. The experiments are carried out using 3 grayscale images (Lena, Barbara and cameraman) of size 256x256. The binary image (key) of size 128x128 is used as watermark image. The watermark embedding is carried out in LL sub band of cover images. The performance of the proposed scheme is evaluated using the parameters PSNR and NC.

Peak Signal to Noise Ratio (PSNR) is expressed in dB and is given by,

$$PSNR = 10log_{10}\frac{255^2}{MSE} \quad (7)$$

Where MSE is Mean Square Error, given by,

$$MSE = (1/(N*N))\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left(I_{ij} - I'_{ij}\right)^2 \quad (8)$$

Where I and I` are images to be compared and N is size of images.

Normalized cross Correlation (NC) is given by,

$$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I[i,j]I'[i,j])}{\sum_{i=1}^{M}\sum_{j=1}^{N}(I[i,j])^2} \quad (9)$$

Where M and N are sizes of image and I and I` are images to be compared for existence of similarity.

NC value ranges between 0 and 1.

In the proposed scheme, first feature extraction of cover image is performed using DWT and the watermark image is split into two shares. One of the shares is embedded in cover image and other is with the TA. After embedding process cover image and watermarked images are compared using PSNR and NC values. The following table briefs about embedding process with PSNR and NC values.

TABLE I. ANALYSIS OF EMBEDDING ALGORITHM.

Cover image	Watermark image	Watermarked image	PSNR (dB)	NC
			35.53	0.9994
			36.81	0.9996
			38.57	0.9999

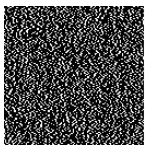
From the values of PSNR and NC it can be concluded that if PSNR and NC values are above 35 dB and 0.95 then cover image and watermarked images are indistinguishable to HVS, hence satisfying imperceptibility property.

The extraction process recovers watermark from the attacked image and is compared against the embedded watermark using

PSNR and NC. The following table gives the results of extraction algorithm.

For extraction, the cover image is not needed to retrieve the watermark, thereby satisfying blindness property.

TABLE II. ANALYSIS OF EXTRACTION ALGORITHM.

Attacked image	Share S2	Extracted watermark	PSNR (dB)	NC
			10.78	0.6817
			10.50	0.6677
			10.50	0.6716

IV. CONCLUSION AND FUTURE SCOPE

In this paper, VC based grayscale image watermarking scheme is proposed. The scheme satisfies the robustness, imperceptibility, blindness and security properties. The proposed work can be extended by using error correcting codes and filtering techniques.

REFERENCES

[1] Stelvio Cimato, James Ching-Nung Yang, and Chih-Cheng Wu "Visual Cryptography Based Watermarking: Definition and Meaning" IWDW 2012, LNCS 7809, pp. 435–448, 2013.Springer-Verlag Berlin Heidelberg 2013

[2] Zhang Nanac "Watermarking algorithm of spatial domain image based on SVD" ICALIP 2016 IEEE.

[3] Jobin Abraham, Paul varghese "An imperceptible spatial domain color image watermarking scheme" Journal of king saud university- computer and information science 2017 - Elsevier

[4] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing 6 (12) (1997) 1673–1687.

[5] F. Liu C.-K. Wu, "Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners" ET Inf. Secur., 2011, Vol. 5, Iss. 2, pp. 121– 128.

[6] Der-Chyuan Lou, Hao-Kuan Tso, Jiang-Lung Liu, " A copyright protection scheme for digital images usingvisual cryptography technique" Computer Standards & Interfaces 29 (2007) 125 – 131 Elsevier.

[7] M. Naor and A. Shamir,"Visual cryptography, "Advances in Cryptography: EUROCRYPT'94, LNCS" , vol. 950, pp. 1–12, 1995

[8] Yanyan Han, Haocong Dong, Wencai He. "A verifiable visual cryptography scheme based on XOR algorithm." 14th IEEE International Conference. Nov, 2012.

[9] Yanyan Han, Wencai He,Yixiao Shang, "DWT-domain Dual Watermarking Algorithm of Color Image based on Visual Cryptography" 978-0-7695-5120-3/13 $26.00 © 2013 IEEE.

[10] Tuyls, P., Hollmann, H.D.L., van Lint, J.H., Tolhuizen, L.: 'Xor-based visual cryptography schemes', Des. Codes Cryptogr., 2005, 37, pp. 169–186.

[11] Adel Hammad Abusitta, A Visual Cryptography Based Digital Image Copyright Protection, *Journal of Information Security*, 2012, 3, 96-104 Doi:10.4236/jis.2012.32012 Published Online April 2012 (http://www.SciRP.org/journal/jis).

[12] Ching-Sheng Hsu and Shu-Fen Tu, Digital Watermarking Scheme with Visual Cryptography, Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol I IMCS 2008, 19-21 March, 2008, Hong Kong