Blind Invisible Watermarking Technique in DT-CWT Domain Using Visual Cryptography

Meryem Benyoussef, Samira Mabtoul,
Mohamed El Marraki, and Driss Aboutajdine

Mohammed V-Agdal University, Faculty of Science, Department of Physics
LRIT Associated Unit to the CNRST-URAC N 29
benyoussef.meryem@yahoo.fr

Abstract. A method for digital image copyright protection is presented in this paper. The proposed method is a blind invisible and robust image watermarking scheme based on Dual Tree Complex Wavelet Transform (DT-CWT) and Visual Cryptography concept (VC). This method does not require that the watermark to be embedded into the original image which leaves the marked image equal to the original one. In the concealing and extracting process, the image is transformed in the complex wavelet domain to generate a secret and a public share respectively, using LL sub-band features and a VC codebook. To extract the watermark from the attacked image, the secret and public shares are stacked together. To improve the visual quality of the extracted watermark, a post process called reduction procedure is also proposed. The experimental results show that the proposed method can withstand several image processing attacks such as cropping, filtering and compression etc...

Keywords: Robust Blind Watermarking, Visual Cryptography, Complex Wavelet Transform, Copyright Protection.

1 Introduction

Visual Cryptography (VC) was first introduced by Moni Noar and Shamir at Eurocrypt'94 [1]. VC is described as a secret sharing scheme of digital images. It involved breaking up the image into n shares using a codebook. Those shares are binary images usually presented in transparencies; so that each participant can hold a transparency (share). The act of decryption is to simply stack shares and view the secret image that appears on the stacked shares. The decoding of the secret image by the Human Visual System (HVS) is the interesting feature that has attracted the researchers in adapting this concept for several applications including watermarking. In accordance with cryptography, the security of a crypto-system does not reside in the algorithm, but resides in the secret key; that is, the security will maintain well even if the algorithm has been published.

Digital image watermarking is the technique of embedding a secret image, called also "watermark pattern", into a cover image, to protect intellectual property. The watermark pattern in the cover image can be either visible [2] or invisible [3]. However the visible watermarking techniques destroy the image quality

A. Petrosino (Ed.): ICIAP 2013, Part I, LNCS 8156, pp. 813–822, 2013.

and are easily attacked through direct image processing, which increase studies on invisible watermarking. By using this later scheme, the owner can prove his copyrights by extracting the watermark pattern from the watermarked image.

Hwang [4] is the first author who proposed a method of how to take benefit of VC to create digital image copyright protection. Since the security characteristics of VC, the watermark pattern is difficult to detect or recover from the marked image in an illegal way. Based in the Hwang idea, others related works have been proposed [5] [6] [7] [8] [9]. In the watermarking schemes using VC, the watermark pattern can be either physically embedded into the cover image or not. The first category schemes which are similar to traditional methods are called watermark embedding schemes. The second category are called watermark concealing schemes, they are particularly useful in protecting highly sensitive images, since the original image is not altered. In [9], a recent VC based watermark concealing scheme in DWT domain is proposed. To improve the security, the authors introduce three new security related performance criteria: column equity, code equity, and color equity. Column equity refers to the probability of selecting each column in the codebook of VC; code equity refers to the similarity of code-block used for coding black and white pixels of the secret image while color equity refers to the distribution of black and white pixels in each code-block.

As traditional techniques, VC based watermarking methods, described in the literature, can be grouped into two main categories. In the first one, the watermark is embedded in the spatial domain, such methods are low computational complexity but vulnerable to attacks [5] [6]. In the second one, the watermark is embedded in the transform domain, especially Discrete Wavelet Transform (DWT) [9]. In general, the DWT produces watermark images with the best visual quality due to the absence of blocking artifacts. However, it has two draw backs [12]:

- Lack of shift invariance, which means that small shifts in the input signal can cause major variations in the distribution of energy between DWT coefficients at different scales.
- Poor directional selectivity for diagonal features, because the wavelet filters are separable and real.

To overcome these problems, Kingsbury introduced the design and implementation of 2-D multi-scale transform, called Complex Dual Tree Wavelet Transform (DT-CWT), that represent edges more efficiently than does the DWT [10] [11], this will be discussed in the next section.

According to the research that we did, we didn't found any work combining VC and DT-CWT. So To benefit from the advantages of DT-CWT transform over DWT transform; we present in this work, a blind, invisible and robust VC-based watermark concealing scheme in DT-CWT domain.

The rest of this paper is organized as follows: the concept of visual secret sharing scheme and DT-CWT are explained briefly in section 2. Section 3 describes the watermark concealing/extracting phases and the reducing procedure. The experimental results and some comparisons are shown in section 4. Finally, section 5 concludes this paper.

2 Techniques Used

2.1 Dual Tree Complex Wavelet Transform (DT-CWT)

Kingsbury [10] [11] introduced a new kind of wavelet transform, called the Dual-Tree Complex Wavelet Transform that exhibits approximate shift in variant property and improved angular resolution. The DT-CWT is an over complete transform with limited redundancy (2^m: 1 for m dimensional signals). This transform has both the advantages of being approximately shift invariant and having additional directionalities ($\pm 15, \pm 45, \pm 75$) compared to three directionalities (H,V,D) for traditional DWT (Fig 1). There are many successful applications

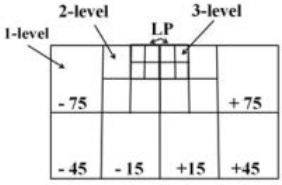


Fig. 1. 3-level DT-CWT decomposition of an image. LP corresponds to low-pass CWT coefficients

on DT-CWT watermarking, for example P. Loo and N. Kingsbury [12] suggested adding the watermark, which is a pseudo-random sequence generated from the valid wavelet coefficients (i.e. coefficients which come from the CWT of an image), to the host image CWT coefficients. Detection involves retrieving the original watermark by correlation between the original watermark CWT coefficients and the CWT of the received image. Y. Hu and al. [13] proposed a new technique of visible watermarking based on the principle of image fusion, and to better protect the host features and increase the robustness of the watermark, the dual-tree complex wavelet transform DT-CWT is used, in [14], the DT-CWT-based watermarking algorithm, robust for affine transformation and time-varying according to the degree of distortion is given.

2.2 Visual Cryptography (VC)

VC, introduced by Naor and Shamir during Eurocrypt in 1994 [1], is a Visual Secret Sharing Scheme (VSS) which uses the Human Visual System to decrypt a secret image without expensive and complicated decoding process. The original problem of VC is the special case of a 2 out of 2 visual secret sharing problem which is the most frequently used. In this scheme the secret image is divided into two shares that consist of random dots. For each pixel P of the secret image, two blocks of 1×2 pixels are generated in the corresponding location for each share. Therefore, the generated shares have a size of $1s \times 2s$ if the original image

is of size $1s \times 1s$. If P is white, then the encoder chooses randomly a block of the first two columns in Table 1. If P is black, then the encoder chooses randomly a block of the last two columns in Table 1. Note that if P is white the two blocks generated are identical, but if P is black the two blocks are complementary.

In the decryption process, the two shares are stacked together. Then for a black pixel P, the result is a block with two black subpixels. But for a white pixel, the result is a block with one black subpixel and one white subpixel. By the human vision system, the block with black and white subpixels will be recognized as a white pixel and the block with two black subpixels will be recognized as a black pixel. Therefore, the secret information can be easily detected when these shares are stacked together.

Table 1. Codebook of the basic (2,2) visual cryptography

Pixel	□		■	
Probability	1/2	1/2	1/2	1/2
Share 1				
Share 2				
Share 1 ⊕ Share 2				

3 Proposed Watermarking Scheme

The proposed watermarking method consists of three components: watermark concealing, watermark extraction and watermark reduction. In the concealing process, we firstly apply the DT-CWT transform to create a binary matrix B based on LL sub-band features. The binary matrix B is used to generate the secret share from the watermark pattern based on a (2,2) VSS scheme (Table 2). This same process is repeated in the extraction process to generate the public share. This later is superimposed on the secret share to recover the ownership label. Finally, we apply a reduction process to improve the image quality of the recovered watermark (Fig 2).

3.1 Concealing Process

The steps of watermark concealing are given below:

Inputs: Host Image I ($m \times n$), Watermark Image ($r \times c$), Secret Key S, Number of decomposition level k
Outputs: Secret Share ($r \times 2c$)
Step 1: Select the number of wavelet decomposition level k.
Step 2: A k-level DT-CWT transform is performed on the image I.

Table 2. Codebook used to generate public and secret shares

Pixel	□		■	
Matrix B	0	1	0	1
Public Share	◧	◨	◧	◨
Secret Share	◧	◨	◨	◧
Public Share ⊕ Secret Share	◧	◨	■	■

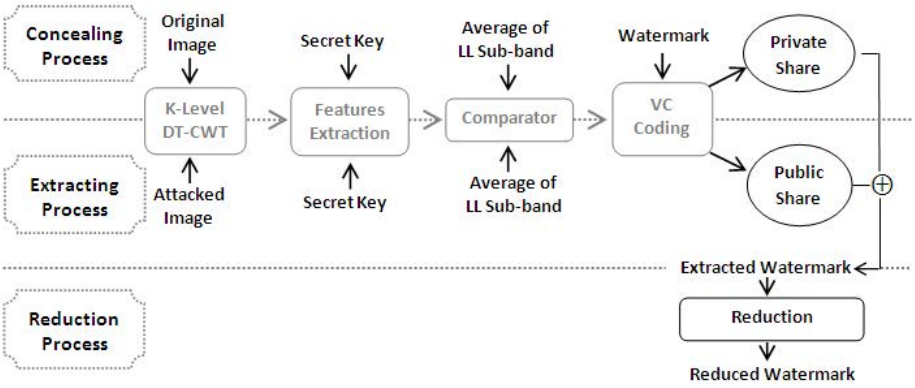


Fig. 2. Proposed watermarking sheme

Step 3: Calculate average gray level LL_{avg} of the LL^k sub-band image.
Step 4: Use S as a seed to select $r \times c$ random pixel locations within LL^k. Let $R_i(x, y)$ be the i^{th} random location. Note that, these positions should not be the last 3 boundary pixels.
Step 5: For each $R_i(x, y)$, select a 7×7 size sub-image area centered at location $R_i(x, y)$, and find its average.
Step 6: Construct a feature image F of size $r \times c$, such that the entries in the matrix are the sample averages obtained in the above step.
Step 7: Construct a binary matrix B:

$$B(x, y) = \begin{cases} 1, & \text{if } F(x, y) \geq LL_{avg} \\ 0, & \text{if } F(x, y) < LL_{avg} \end{cases} \quad (1)$$

Step 8: Use the bits in matrix B to select columns in Table 2 for generating the secret share. Note that, the secret share size is $(r \times 2c)$, due to the codebook used.

3.2 Extracting Process

The steps of watermark extraction are given below:

Inputs: Attacked image I' ($m \times n$), Secret Share ($r \times 2c$), Secret Key S, Number of decomposition level k
Outputs: Watermark ($r \times 2c$)
Step 1: A k-level DT-CWT transform is performed on the image I'.
Step 2-6: Same as steps 3-7 of the concealing process.
Step 7: Use the bits in matrix B to select columns in Table 2 for generating a public share. Note that, the code-block assignment for public share corresponding to each secret bit is independent of the pixel pair colors in the watermark image.
Step 8: Perform logical OR operation on the public share and the secret share to extract the watermark.

3.3 Reduction Process

To generate the secret and public shares, the author of the basic system [9] proposed a PWVC (Pair Wise Visual Cryptoraphy). This technique aims at resolving pixels expansion by coding a pair of pixels instead of coding a single pixel each time. However it cannot allow a reduction process, without using the original watermark, to improve the image quality. Due to the proposed codebook that we used to generate the two shares in our method, the extracted watermark has a size of ($r \times 2c$) compared to the original one. To retrieve the original size and to mitigate the noise effect caused by the watermark extraction, we use a post-process called "reduction process" that can reduce the redundancy data caused by VSS scheme in a blind way. Indeed, this process can perform a function of data reduction (Table 3); that is, a block data with two pixels located in each group will be transferred into a corresponding pixel. As shown in Table 3, if the block is composed of one black and white pixel or two white pixels then the corresponding pixel is white, but if the block is composed of two black pixels then the corresponding pixel is black.

Table 3. The lookup table of reduction process

Block of the extracted watermark		
Block of the reduced watermark		

4 Experimental Results

In this section, we present some experimental results concerning the proposed method. To evaluate the effectiveness of the proposed approach, four standard grayscale images are used: F-16, Elain, Boat and Mandrill of size 512×512 pixels. The watermark is a binary image with the size of 100×100 pixels (Fig. 3).

(a) F-16 (b) Elain (c) Boat (d) Mandrill (e) Watermark

Fig. 3. Test images and watermark pattern used

The first type of simulation is done to show the advantage of our method compared the watermarking scheme of [9]. To test the robustness of the algorithm to attacks, our test images are subjected to several common attacks. They are compression, median filer, blurring, salt and pepper noise, histogram equalisation, cropping, resizing, rotation and translation. Table 4 shows the attacked images and the extracted watermark from each one using our method and [9] method.

The second type of simulation is done to show the robustness of the proposed algorithm with any cover image, we give in Tables 5-9 the PSNR (2) values of the attacked images and NC (3) values of the extracted watermark from each one. It can be seen from the high values of NC that our algorithm can successfully resist many common attacks.

$$PSNR = 10 \times log \frac{255^2}{MSE} \tag{2}$$

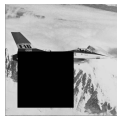
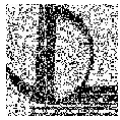
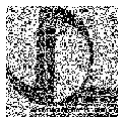
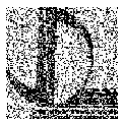
$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(c_{i,j} - c_{i,j}^{'} \right)^2$$

where $c_{i,j}$ and $c_{i,j}^{'}$ denote pixel intensity of the original and attacked images.

$$NC = \frac{\sum_{i=1}^{r} \sum_{j=1}^{c} \overline{\left(w_{i,j} \bigoplus w_{i,j}^{\prime} \right)}}{r \times c} \times 100\% \tag{3}$$

where $w_{i,j}$ and $w_{i,j}^{'}$ denote pixel intensity of the original and extracted watermarks.

Table 4. Experimental results outlining the superiority of the proposed algorithm

Attacked Images	[9]'s Results	Our Results	Attacked Images	[9]'s Results	Our Results
Cropping 25%			Cropping 50%		
					
Rotation 3			Rotation 10		
					
Scale 50%			Translate 20 lines		
					
Compression 10%			Compression 40%		
					
Salt & Pepper Noise 25%			Blurring		
					
Histogram Equalization			Median Filter (3x3)		
					

5 Conclusion

The proposed method describes a robust and blind digital image watermarking in frequency domain, which is computationally efficient. This method applies the Dual Tree Complex Wavelet Transform and uses Visual Secret Sharing Scheme to generate a secret share and hide it into the LL sub-band. Thus the proposed

Table 5. PSNR and NC values after adding Salt & Pepper noise

Images	Salt and Pepper Noise					
	Noise density					
	0.05		0.15		0.25	
	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)
F-16	34.87	99.28	25.45	98.24	21.02	97.41
Elain	38.77	98.54	29.39	97.32	24.99	96.15
Boat	37.55	98.60	28.17	97.19	23.77	95.67
Mandrill	36.23	97.68	26.87	95.90	22.44	93.21

Table 6. PSNR and NC values after image JPEG compression

Images	JPEG Compression					
	Quality factor					
	70%		40%		10%	
	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)
F-16	46.86	99.93	44.36	99.78	38.01	99.36
Elain	44.07	99.90	40.71	99.79	34.80	99.00
Boat	43.47	99.87	41.40	99.66	36.81	98.76
Mandrill	38.76	99.80	35.76	99.56	31.79	98.52

Table 7. PSNR and NC values after cropping

Images	Cropping					
	15%		35%		50%	
	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)
F-16	26.37	94.85	16.61	81.89	12.29	75.83
Elain	31.24	96.16	21.60	85.93	16.70	73.40
Boat	38.87	99.12	19.19	83.83	15.24	74.48
Mandrill	30.75	95.58	17.56	69.49	13.25	54.89

Table 8. PSNR and NC values after rotation

Images	Rotation					
	3		5		10	
	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)
F-16	22.53	88.21	20.16	82.37	16.80	71.37
Elain	23.56	85.52	21.43	78.19	18.79	66.02
Boat	23.67	87.50	21.55	83.83	18.88	77.20
Mandrill	21.90	86.60	20.39	80.78	17.96	70.33

work is the first one that combine VC concept and DT-CWT. The simulation results of this combination, have confirmed that that the proposed method has high fidelity and it is robust against common image processing attacks such as cropping, lossy compression, filtering, etc.

Table 9. PSNR and NC values after Median filter, scale and translation

Images	Median Filter (3x3)		Scale 50%		Translate 20 lines	
	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)
F-16	46.92	99.60	40.23	99.94	15.30	75.08
Elain	35.93	99.68	35.04	99.96	17.34	66.03
Boat	41.70	99.47	39.72	99.87	17.18	72.57
Mandrill	33.15	99.12	32.38	99.84	16.17	69.19

References

1. Naor, M., Shamir, A.: Visual Cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
2. Liu, J.C., Chen, S.Y.: Fast two-layer image watermarking without referring to the original image and watermark. Image and Vision Computing 19, 1083–1097 (2001)
3. Chu, S.C., Roddick, J.F., Lu, Z.M., Pan, J.S.: A digital image watermarking method based on labeled bisecting clustering algorithm. IEICE Trans. E87-A(1), 282–285 (2004)
4. Hwang, R.J.: A Digital Copyright Protection Scheme Based on Visual Cryptography. Tamkang Journal of Science and Engineering 3(3), 97–106 (2001)
5. Abusitta, A.H.: A Visual Cryptography Based Digital Image Copyright Protection. Journal of Information Security 3, 96–104 (2012)
6. Wang, C.C., Tai, S.C., Yu, C.S.: Repeating Image Watermarking Technique by the Visual Cryptography. IEICE Trans. E83-A(8), 1589–1598 (2000)
7. Sleit, A., Abusitta, A.: A Visual Cryptography BasedWatermark Technology for Individual and Group Images. Systemics, Cybernetics and Informatics 5(2), 24–32 (2006)
8. Surekha, B., Swamy, G.N.: Multiple Watermarking Scheme for Image Authentication and Copyright Protection using Wavelet based Texture Properties and Visual Cryptography. International Journal of Computer Applications 23(3), 29–36 (2011)
9. Surekha, B., Swamy, G.N.: Sensitive Digital Image Watermarking for Copyright Prottection. International Journal of Network Security 15(1), 95–103 (2013)
10. Kingsbury, N.G.: Complex wavelets for shift invariant analysis and filtering of signals. Journal of Applied and Computational Harmonic 10(3), 234–253 (2001)
11. Selesnick, I.W., Baraniuk, R.G., Kingsbury, N.G.: The Dual-Tree Complex Wavelet Transform. IEEE Signal Processing Magazine 22(6), 123–151 (2005)
12. Loo, P., Kingsbury, N.G.: Watermarking using complex wavelets with resistance to geometric distortion. In: EUSIPCO, pp. 5–8 (2001)
13. Hu, Y., Huang, J., Kwong, S., Chan, Y.K.: Image Fusion Based Visible Watermarking Using Dual-Tree Complex Wavelet Transform. In: Kalker, T., Cox, I., Ro, Y.M. (eds.) IWDW 2003. LNCS, vol. 2939, pp. 86–100. Springer, Heidelberg (2004)
14. Joong-Jae, L., Kim, W., Na-Young, L., Kim, G.: A New Incremental Watermarking Based on Dual-Tree Complex Wavelet Transform. JSC 33(1-2), 133–140 (2005)