Analyzing Visual Cryptography with Watermark Hiding Technique

Kamaljit I Lakhtaria, Ph.D.
Assistant Professor, CSE Department,
Sir Padampat Singhania University,
Udaipur, Rajasthan

ABSTRACT

In this paper, a watermark hiding scheme based on Visual Cryptography and Discrete Wavelet Transform is proposed. The proposed method modifies the codebook of related works, and utilizes statistical average to offer better security. The proposed method also reduces the size of the codebook and probability of false positives when compared to the existing works. Experimental results prove that the scheme is also robust to wide range of attacks

KEYWORDS

Copyright Protection, Digital Watermarking, Secret Sharing, Visual Cryptography.

1. INTRODUCTION

In recent years, digital data distribution has grown enormously, because of advances in wide spread databases and web technologies. Hence multimedia data can be easily modified, duplicated and distributed. It is often required to trace illegal distribution of multimedia data and to identify the copyrights.

Digital Image Watermarking techniques protects the given image, by hiding a watermark representing copy rights of the owner in the form of image or textual data, into the image to be copyright protected. It can be extracted later to make an assertion about the data. In practice, there is a very good chance for a watermarked image to be altered while being transmitted through the channel. These alterations can be a result of intentional attacks such as filtering, blurring, cropping etc. or unintentional distortions such as JPEG compression and channel noise addition. An effective watermarking technique should satisfy high invisibility, robustness, security, capacity & low computational complexity [1].

Traditional watermarking schemes fail in resolving the tradeoff between invisibility, capacity and robustness. This is due to the fact that these techniques physically embed the watermarks into the host images. To resolve this tradeoff, some researchers used the features of the host image and the concept of Visual Cryptography (VC) to conceal and verify the copyrights of the owner. This approach doesn't actually embed the watermark in the host image, but conceals it using random looking images called shares. Such an approach is particularly suitable in protecting sensitive images such as military, medical and satellite images, where any modifications to these images are not acceptable.

Visual Cryptography (VC) [2] is basically a secret sharing scheme extended to images. It was first presented by Naor and Shamir in mid 90's. Its ability to decode the encrypted data by Human Visual System (HVS) has attracted the research community only recently. A k-of-n threshold visual cryptography scheme splits a secret image into n random looking share images using a codebook. Any k out of n share images can be used to restore the secret image by overlaying one above the other.

Most of the digital image watermarking schemes based on visual cryptography [3-11] works as follows: Given a host image and a binary watermark, these schemes first compute a feature vector from the host image. A method of comparison and a secret key is then used to obtain a secret binary matrix from the extracted feature vector. Note that the security of the watermarking technique increases if the probability of occurrences of logical ones and zeros in this matrix are equal.

Depending on the color of each pixel in the binary watermark, and the bits in the secret binary matrix a particular code is selected from the code book of 2-of-2 visual cryptography to create a random looking binary image, called private share. This share is time-stamped and is confidentially kept secret at a Certified Authority (CA). During copyright verification, a similar process is used to extract another random looking binary image called public share from the claimed image using the same secret key. It is then combined with the private share to prove the copyrights. The combination function can be a Boolean OR operation or XOR operation.

The schemes in [3-6] use the above approach to hide watermarks in spatial domain. Though they are simple, watermarks hided in frequency domain [7-11] are more robust. It is to be noted that, even if all the properties of the watermarking are satisfied the technique becomes meaningless, if it leads to false positives. A false positive is a result of extraction of a watermark from an unauthorized image, which doesn't actually belong to the owner. Since, false positives encourage the malicious owners in claiming other unauthorized images, this problem should be avoided.

One such robust scheme, which leads to false positives, is LTL scheme [8], proposed by Lou et al., This scheme constructs a secret binary matrix by comparing the modified Discrete wavelet Transform (DWT) coefficients obtained, from two selected sub bands of same level with that of LL sub bands coefficients. The security of this scheme is analyzed by Chen et al, [9]. They proved that for almost all host images, the LL sub band coefficients of DWT are greater than or equal to coefficients in other sub bands. The result is that the most of the bits in secret binary matrix are logical ones, irrespective of the host image. Thus the scheme becomes monotonous, as verification of watermark purely depends on secret key. This way, the LTL scheme increases the probability of false alarm and leads to ambiguity in copyright verification. Hence, this scheme can't be used for copyright protection.

To overcome this drawback, park et al [10] used a different threshold for comparison. They have compared the same modified DWT coefficients of LTL's scheme with the average of the coefficients in LL sub band. Though this scheme reduces the probability of false alarm to some extent, it fails in secure verification of watermark. The security of this scheme is analyzed by Xing et al in [11] and has proved that, if someone gains a copy of private share, they can overlay it on a share consisting of all black pixels to extract a trace of the watermark without the need to extract a Public Share. The result is that the scheme becomes independent of the host image and the secret key. This problem arises due to majority of black sub pixels in their codebook. The scheme also has a drawback that it requires the original watermark, in addition to Private Share for copyright verification.

To improve the security of the above schemes, Xing proposed a new DWT based scheme that compares modified LL sub band coefficients with the same average used in Park's scheme. It results in four different decimal values (0,1,2,3), instead of binary 1's and 0's to be contained in the secret matrix for generation of shares. This doubles the size of the codebook. In addition, the selected feature may not guarantee to result equal probability of occurrences of all the four decimal values. This reduces the security of Visual Cryptography.

This paper proposes a new digital image copyright protection scheme based on Discrete Wavelet Transform and Visual Cryptography. The proposed method utilizes sample averages and central limit theorem to reduce false alarm probability. The proposed scheme modifies and reduces the codebook, to offer better security when compared to the related techniques. The scheme also aimed at achieving high robustness to several image processing attacks.

The rest of the paper is organized as follows. Section2 briefly reviews 2-of-2 Visual Cryptography. Section3 describes the proposed watermark hiding and revelation procedures. Simulation results are illustrated in Section4 and Section5 concludes the paper.

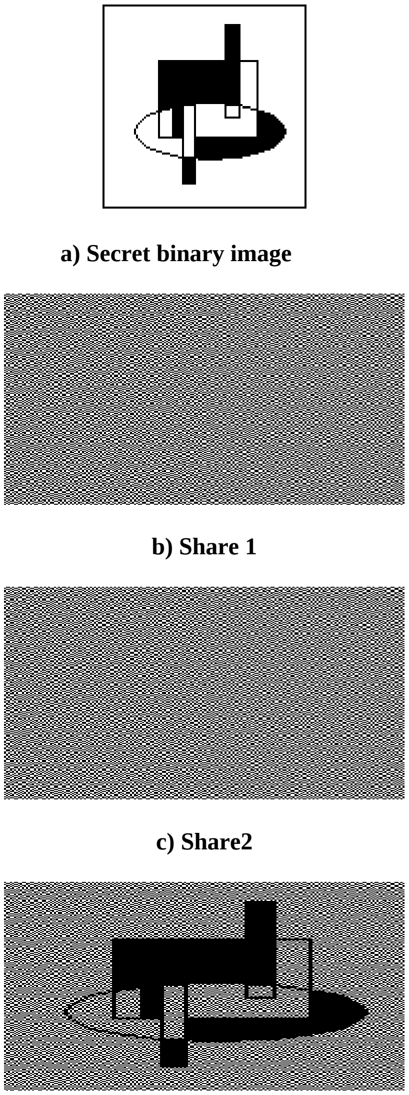
2. BASIC 2-OF-2 VISUAL CRYPTOGRAPHY

All A 2-of-2 visual cryptography splits a secret image into two random images called shares. The splitting is done in the following way. Each pixel in the secret image, a code-block of two sub-pixels is substituted in each of the shares using a codebook given in Table 1. A white pixel is shared into two identical code blocks of sub-pixels. A black pixel is shared into two complementary code blocks of sub-pixels. While creating the shares, if the given pixel p in the original image is white, then the encoder randomly chooses one of the first two columns of Table.1. If the given pixel p is black, then the encoder randomly chooses one of the last two columns of Table.1. Each code block has half white and half black sub-pixels, independent of whether the corresponding pixel in the secret image is black or white. The security of Visual Cryptography lies in random selection of these columns. To achieve high security the probability of selecting each column, for either pixel color same.

The results of basic 2-of- 2 VC are shown in Fig.1. When the two shares are overlaid one above the other, as in Fig.1.d, the black pixels in the original image remain black and the white pixels become gray. Since each pixel in the original image is replaced by two sub-pixels in each share, some contrast loss occurs in the decoded image.

Table 1. Basic 2-of-2 visual cryptography

Pixel	Black		White	
Prob.	50%	50%	50%	50%
Share1	■□	□■	■□	□■
Share2	□■	■□	■□	□■
Stack Share1 & Share2	■■	■■	■□	□■



a) Secret binary image

b) Share 1

c) Share2

d) Decoded Image

Fig. 1. Example of 2-of-2 visual cryptography

3. THE PROPOSED SCHEME

The Unlike traditional watermarking schemes, the proposed scheme uses the features of host image to hide a binary watermark image by constructing a Private Share during watermark hiding phase, and a Public Share during watermark revelation phase.

3.1. Watermark Hiding Phase

The hiding algorithm conceals the watermark using the original host image H in case of a gray-scale, or it uses the intensity component, if it is a color image. Let the relevant component of the original host image is referred to as cover image I. Decomposition of the image to obtain the required component is done in the preprocessing stage of the algorithm.

After preprocessing, the real watermark hiding procedure follows.

Inputs: Original Host image of size (m×n), Binary watermark of size (w×h)

Outputs: Private share of size (w×2h)

1. Select the number of wavelet decomposition levels j such that, $2^j \geq (m\times n)/(w\times h)$
2. A j-level discrete wavelet transform is performed on the cover image I to obtain LL^j sub band image.
3. Calculate average gray level of the LL^j sub band image. Let it be LL_{avg}.
4. A secret key *K* is used as a seed to select w×h random pixel locations with in LL^j sub band image. Let $R_i(x,y)$ be the i^{th} random location.
5. For each $R_i(x,y)$, select a 5×5 size sub image area centered at location $R_i(x,y)$, and find its average.
6. Construct a feature matrix F of size w×h, such that the entries in the matrix are the sample averages obtained in the above step.
7. Construct a secret binary matrix S, using the following comparison:

$$S(x,y)=\{0, if\ F(x,y)<LLvag$$

8. Use the codebook given in Table 2 to create a private share.

Finally, this private share is time-stamped and is confidentially kept secret at a Certified Authority (CA). During verification of copyright, the owner should provide the same secret key to the Certified Authority, to retrieve a second share called Public Share. When this share is overlaid on the Private Share, the watermark can be revealed.

3.2. Watermark Revelation Phase

The process of extracting the watermark from the Intensity component I' of the claimed image is given below.

Inputs: Cover image I' of size (m×n), Private Share of size (w×2h)

Outputs: Watermark of size (w×2h)

1. The procedure to create secret binary matrix S is same as in hiding phase.
2. Use the codebook given in Table 2 to create a public share. Note that the sub block assignment for Public Share corresponding to each secret bit is independent of watermark pixel color.
3. Finally, the watermark can be revealed by performing bitwise logical OR operation on the Public Share and the Private Share.

The proposed scheme can be extended to hide to gray-level or color watermarks. They are first transformed into bi-level halftone images and then embedded into the host images using the same procedure.

Table 2. Codebook used in Proposed Scheme

Watermark bit	**Black**		**White**	
Secret bit	**0**	**1**	**0**	**1**
Public Share	■□	□■	■□	□■
Private share	□■	■□	■□	□■
Public Share + Private Share	■■	■■	■□	□■

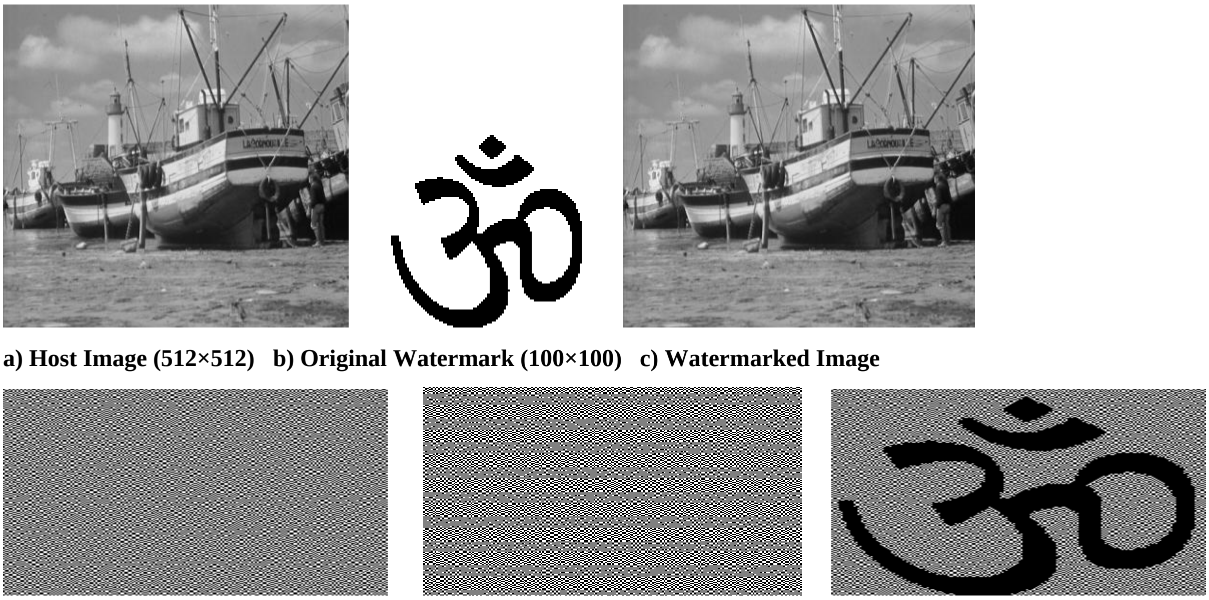
3.3. Security analysis

The security of the proposed scheme lies in the generation of secret binary matrix S, and the design of codebook used in creating Public Share and Private Share. Unlike LTL scheme, where most of the bits in secret binary matrix are logical ones, the bits in our proposed scheme are equally likely. Here, each entry in the secret binary matrix is obtained by comparing an average of 25 randomly selected coefficients in LL sub band, with that of average value of all the coefficients in the same LL sub band. According to the central limit theorem, even if the coefficients of LL sub band image are not normally distributed, the sampling distribution of averages will approximate a normal distribution, provided the sample size is sufficiently large. The result is that the probability of occurrence of logical ones and zeros in secret binary matrix is almost same. Thus, there is no way an attacker can estimate the secret binary matrix without the knowledge of secret key. In this way, the proposed scheme improves the security of LTL's scheme.

Unlike Park's scheme where the majority of sub pixels in the codebook are black, the number of black and white sub pixels in our codebook is equal. This reduces the chances of revealing the watermark if a private share is overlaid on all black or all white pixel shares. Also, the codebook size is small when compared to schemes in [8, 10, 11].

4. SIMULATION RESULTS

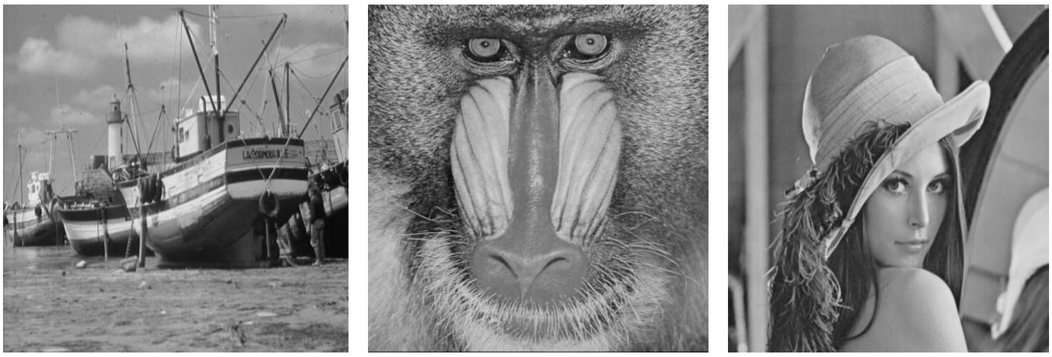
Author The performance of the proposed scheme is evaluated by conducting experiments on different benchmark images. Fig.2.a. shows the Original Boat image, from which the watermark is hidden. Fig.2.b. shows the binary watermark of size 100×100. Fig.2.c shows the watermarked image. Since the host image is not altered during watermark hiding phase the host image remains same. Fig.2.d. shows the Private Share generated during watermark hiding process. Fig.2.e. shows the Public Share generated during watermark revelation phase. Fig.2.f. shows the revealed watermark after overlaying the Public Share and the Private Share. Although some contrast loss occurs, the extracted watermark can be clearly identified.



a) Host Image (512×512) b) Original Watermark (100×100) c) Watermarked Image

d) Private Share (100×200) e) Public Share (100×200) f) Extracted Watermark (100×200)

Fig. 2. Results of proposed watermarking Scheme



c) Boat (512×512) d) Mandrill (512×512) e) Lena (512×512)

Fig. 3. Test images

The performance of the algorithm with respect to attack resilience has been established by the results shown inTable.3. All the test images are of size 512×512 and are shown in Fig.3. A set of image processing attacks were implemented using the MATLAB Image Processing Tool box.

Peak Signal to Noise Ratio (PNSR) and Normalized Correlation (NC) are used to evaluate performance of this watermarking scheme. PSNR is used to evaluate the similarity of original and attacked grey-level images. It is defined in terms of Mean Square Error (MSE) as follows:

$$PSNR = 10 \times \log \frac{255^2}{MSE} \quad \textbf{(1)}$$

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (h_{i,j} - h'_{i,j})^2 \quad \textbf{(2)}$$

Where hi,j denotes pixel color of original host image and h’i,j denotes a pixel color of attacked watermarked image, and r × c denotes the image size.

Normalized Correlation (NC) is used to measure the similarity between the original and extracted watermark. It is defined as follows:

$$NC = \frac{\sum_{i=1}^{w} \sum_{j=1}^{h} \overline{(s_{i,j} \oplus s'_{i,j})}}{w \times 2h} \times 100\% \quad \textbf{(3)}$$

Where si,j denotes pixel color of extracted watermark image from the original host when it is not altered and s’i,j denotes a pixel color of extracted watermark image when it is altered.

Experimental results illustrates that the proposed algorithm has very good robustness to JPEG compression, sharpening, median filtering, wiener filtering, scaling, blanking rows and columns, noise adding, blurring, intensity adjustments, and jitter. The scheme results in satisfactory robustness to cropping and rotations. It is noticed that the scheme results in less NC values for translation attack.

5. CONCLUSIONS

In this paper, a novel digital image copyright protection based on Visual Cryptography and Discrete Wavelet Transform is proposed. The proposed method modifies the codebook of related works, and uses statistical averages to offer better security. It also reduces the probability of false positives and size of the codebook when compared to the related works. Experimental results prove that the scheme is also robust to wide range of attacks. The proposed algorithm can resist to translations to some extent.

Table 3. Test results for robustness against several attacks

Attacks	Boat		Mandrill		Lena	
	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)
Median Filter 3*3	36.42	99.72	31.69	99.50	40.71	99.82
Wiener Filter 5*5	34.84	99.75	30.77	99.59	39.95	99.84
Sharpening	29.61	99.36	28.29	98.88	32.54	99.50
Scale_0.5	33.60	99.23	30.99	98.74	36.81	99.51
Remove_columns_32	36.12	97.92	36.11	97.13	36.19	98.52
Remove_rows_32	36.13	97.81	36.11	97.30	36.18	98.47
Jitter	41.74	99.48	41.26	98.41	41.4	98.43
Salt & Pepper Noise	44.08	99.32	44.10	99.32	38.05	98.66
Blurring	30.52	97.58	29.12	97.26	32.64	98.35
Histogram Equalization	26.97	93.37	27.57	99.29	41.94	98.25
JPEG_80	39.44	99.95	35.78	99.99	42.81	99.97
JPEG_50	36.77	99.87	32.69	99.87	40.21	99.79
JPEG_10	32.93	99.27	30.42	99.15	35.36	98.78
JPEG_1	30.09	95.23	29.33	96.49	30.81	98.22
Crop_10 lines around	35.10	92.86	35.07	91.47	35.10	94.74
25% Cropping	30.19	83.23	30.19	81.00	30.25	90.67
50% Cropping	27.13	73.15	27.14	77.32	27.20	81.00
Rotation 3^o	29.59	92.10	28.69	92.29	30.68	93.56
Rotation-3^o	29.47	92.47	28.62	92.41	30.76	93.62
n 15^o	27.89	85.32	27.63	80.63	27.94	81.29
Rotation-15^o	27.90	85.15	27.50	82.29	27.71	82.28
Translate_20 lines	28.13	85.17	27.74	83.22	27.93	82.66

6. REFERENCES

[1] R. J. Anderson, Ed., Information Hiding, First International Workshop, LNCS, Springer-Verlag **(1996)** vol. 1174, pp. 1-7.

[2] M. Naor and A. Shamir., Visual cryptography,in The Workshop on the Theory and Application of Cryptographic Techniques**(1995),** vol. 950, pp 1-12

[3] R. Hwang, A Digital Image Copyright Protection Scheme based on Visual Cryptography, Tamkang Journal of science and Engineering, .3, 2**(2002)**.

[4] C. C. Chang, J. C. Chuang. An image intellectual property protection scheme for gray level images using visual secret sharing strategy, Pattern Recognition Letters, 23,.8 **(2002).**

[5] M. Hassan A, M. Khalili A, Self Watermarking based on Visual Cryptography, in The World Academy of Science, Engineering and Technology, 8, **(2005)**

[6] B. Surekha , G. N Swamy , K. Srinivasa Rao , A Ravi Kumar , A Watermarking Technique based on Visual Cryptography, Journal of Information Assurance and Security, 4,6 **(2009).**

[7] S.L. Hsieh, B.Y Huang, A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformation, in International Computer Symposium, **(2004),** pp. 661-666,.

[8] D.C Lou, H.K Too, J.L. Iiu, A copyright protection scheme for digital images using visual cryptography technique, Computer Standards & Interfaces, 29, 1 **(2007)**

[9] T. H. Chen, C. C Chang, C. S. Wu, D.C Lou, On the security of a copyright protection scheme based on visual cryptography, Computer Standards & Interfaces, 31,1 **(2009).**

[10] G. D. Park, E. I. Yoon, K. Y. Yoo, A new copyright protection scheme with visual cryptography, in The Second International Conference on Future Generation Communication and Networking Symposia**(2008),** pp. 60-63.

[11] Y. Xing, J. H He, A new robust copyright protection scheme for digital images based on visual cryptography, in The International Conference on Wavelet Analysis and Pattern Recognition **(2010)**, Qingdao, pp. 6-11

[12] W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptography to Financial Documents, Technical report TR001001, Florida State University, **(2000)**