A Multiple Watermarking Technique for Images based on Visual Cryptography

B Surekha
Associate Professor,
Department of ECE,
TRR College of Engineering,
Hyderabad, India - 502 319.

Dr GN Swamy
Professor & HOD,
Department of ECE,
Gudlavalleru Engineering College,
Gudlavalleru, India - 521 356

Dr K Srinivasa Rao
Professor of ECE & Principal,
TRR College of Engineering,
Hyderabad, India-502 319

ABSTRACT
With the explosive growth of internet technology robust methods are being developed to protect the proprietary rights of the multimedia. In this paper, an invisible watermarking technique is proposed, to embed multiple binary watermarks into digital images based on the concept of Visual Cryptography (VC). Unlike traditional watermarking schemes, the watermarks are not embedded directly into the digital image. Instead, the proposed method constructs independent Master Shares for the authors according to the original image and the corresponding watermarks. When piracy happens, the authors can show their shares to reveal the watermarks. The proposed scheme embeds the watermarks without modifying the original host image. In addition, the size of the watermarks is not restricted to being smaller than that of the original host image. Experimental results prove that, the proposed watermarking technique is resilient to several common attacks.

Categories and Subject Descriptors
K.4.4 **[Electronic Commerce]:** Intellectual Property-Security

General Terms
Design, Security.

Keywords
Copyright Protection, Cryptography, Digital Watermarking, Multiple Watermarks, Visual Cryptography.

1. INTRODUCTION
In recent years, internet revolution resulted in an explosive growth in multimedia applications. Today many photo agencies expose their collection on the web with a view of selling access to the images. They typically create web pages of thumbnails, from which it is possible to purchase high resolution images that can be used for professional publications. However this kind of ultimate flexibility to avail digital images has its negative side too. Easy access facilitates information piracy, through unauthorized replication and manipulation of digital images with the help of inexpensive tools. Cryptographic techniques can solve the problem of unauthorized access to the information. But, it can't prevent an authorized user from illegally replicating the decrypted content. Therefore robust methods must be developed to protect the proprietary rights of the data owners. Digital watermarking is a technology being developed to provide protection from illegal copying [1].

Digital Image watermarking is the process of embedding into a digital image a digital signature called watermark. Detection or extraction of this watermark at a later time enables data owners to make an assertion about the authenticity and ownership of their object. Visible watermarks may be visual patterns such as a company logo or copyright sign, which overlay about digital images. These are limited in many applications, as they distort the original image fidelity and are susceptible to attacks. However, invisible (or transparent) watermarks, when added to the image can't be perceived as such, and have wider applications than visible watermarks [2]. Watermarks can be embedded in almost every domain (Spatial, DCT, Wavelet, Fourier etc.) using different schemes. While most schemes embed only a single watermark, some extend the single watermark algorithms for multiple watermarks. There are different ways to extract the watermark from the image. Those requiring both the original image and the secret key for the watermark extraction are called private watermark schemes. Those requiring the secret keys but not the original image are called public or blind watermark schemes [5]. Those requiring the secret keys and the watermark are called semi-private or semi-blind watermark schemes [11]. In general an effective watermarking scheme should satisfy properties such as invisibility, robustness, security, capacity and low computational complexity [6].

Any watermarking system is usually divided into three distinct phases: embedding, attack and detection. In the embedding phase, a binary watermark is embedded into the host image and the result is a watermarked image. The watermarked image is usually transmitted or stored. If a person makes a modification to the marked image, it is called an attack. Detection (also called extraction) is an algorithm which is applied to the attacked image to extract the watermark from it. In robust (secure) watermarking applications, the detection algorithm should be able to reproduce the watermark, even if the modifications were strong.

There have been many watermarking schemes proposed. The disadvantage of almost all the schemes is that, they modify the host image while embedding the watermarks in the original image. Also, many spatial domain techniques seem to have the lowest bit capacity and the lowest resistance to JPEG compression. [12]

Visual Cryptography (VC) is basically a secret sharing scheme extended for images. It has the ability to restore a secret without the use of computations [13]. VC, when used in conjunction with watermarking allows multiple watermarks to be embedded in the same image without modifying the host image. In addition, the watermarks can be extracted without using the original image. Thus, they are very suitable for applications such as medical images, where modifications to the images are not allowed. The concept of VC can also be employed, so that the identification of rightful ownership can be made without the use of computers. Recently, many researchers applied the concept of VC to Copyright Protection of images [3, 4, 7, 9, 10]. Some of them [7, 9], fully employs the visual decryption ability of VC. These methods convert the gray-level host images into two-tone images, using halftone techniques before embedding a binary watermark.

This paper proposes a watermarking technique, to directly embed multiple binary watermarks into a single image. The proposed scheme embeds the secret image without modifying the original host image. Thus, at no point of time, the watermark information is passed in the transmission channel, thereby providing maximum security. In addition, the size of the watermark is not restricted to being smaller than that of the original host image.

The remaining part of the paper is organized as follows. Section 2 briefly reviews the basic (2, 2) VC scheme. Section 3 describes the proposed Single Watermark Embedding (SWE) scheme. Section 4 extends SWE for Multiple Watermark Embedding (MWE). Experimental results are illustrated in Section 5. Section 6 concludes the paper.

2. BASIC (2, 2) VISUAL CRYPTOGRAPHY

Visual Cryptography (VC) was first introduced by Noar and Shamir at Eurocrypt'94 [13]. To encode a secret using a (2, 2) VC Scheme, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two sub-pixels. Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret. Table.1 illustrates the scheme of encoding one pixel in a (2, 2) VC scheme. A white pixel is shared into two identical blocks of sub-pixels. A black pixel is shared into two complementary 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 block has half white and half black sub-pixels, independent of whether the corresponding pixel in the secret image is black or white. All the pixels in the original image are encrypted similarly using independent random selection of columns. Thus no information is gained by looking at any group of pixels on a share, either.

Table 1. A (2, 2) Visual Cryptography Scheme

Pixel	White		Black	
Prob.	50%	50%	50%	50%
Share1	(0,1)	(1,0)	(0,1)	(1,0)
Share2	(0,1)	(1,0)	(1,0)	(0,1)
Stack Share1 &2	(0,1)	(1,0)	(0,0)	(0,0)

Fig.1 shows the results of basic (2, 2) VC Scheme. When the two shares are stacked together, as in Fig.1.d, the black pixels in the original image remain black and the white pixels become gray. Although some contrast loss occurs, the decoded image can be clearly identified. Since each pixel in the original image is replaced by two sub-pixels in each share, the width of the decoded image is twice that of the original image.

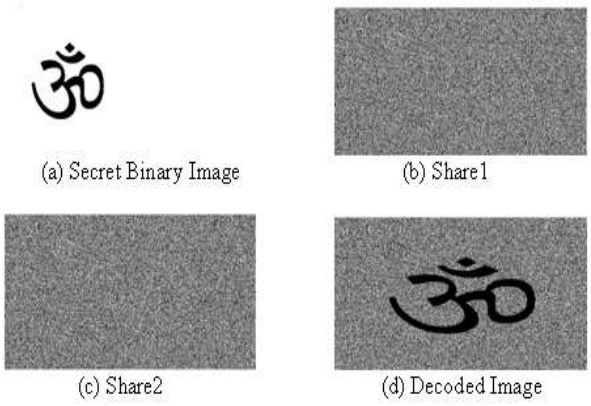

Figure 1. Example of (2, 2) Visual Cryptography Scheme

3. SINGLE WATERMARK EMBEDDING (SWE)

The proposed scheme embeds a single binary watermark in a color image, and securely extracts and authenticates it by using a secret key as demonstrated in Fig. 2. Unlike traditional watermarking schemes, the watermark is not embedded directly into the digital image. Instead, the proposed method constructs a Master Share for the author according to the original image and the watermark. When piracy happens, the author can show his share to reveal the watermark. The advantage of the proposed scheme is that at no point of time watermark information is passed in the transmission channel, thus providing maximum security.

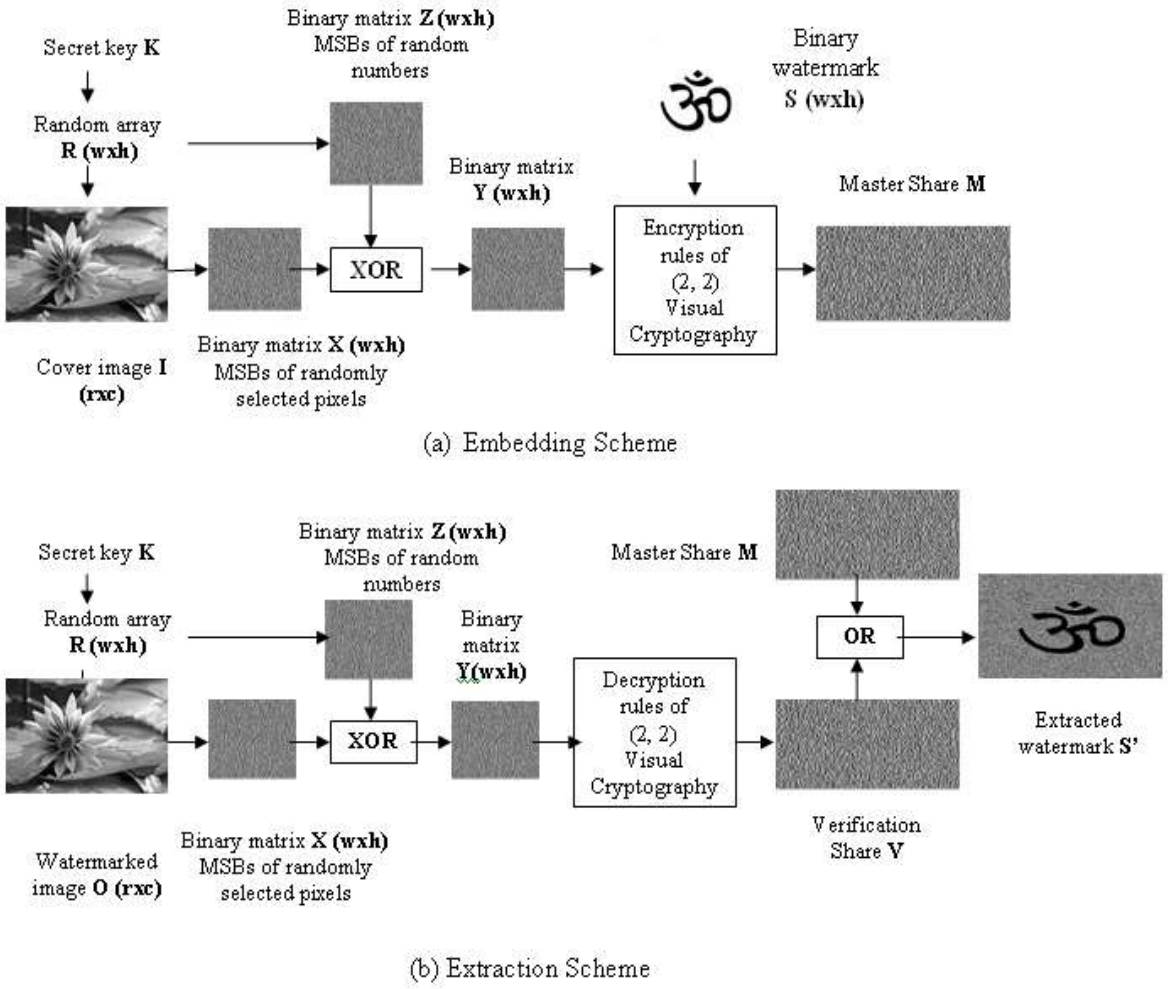

Figure 2. The Proposed Watermarking Scheme

3.1 Embedding Algorithm

The proposed embedding algorithm embeds the watermark into the intensity image of the original image in case of a gray-scale, or into the Y-component of the 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.

Supposing that the cover image *I* have size *rxc* and the binary watermark *S* is of size *wxh*. Let *K* be a random integer selected by the owner as a secret key. The output of the embedding algorithm is a Master Share *M* of size *wx2h*.

After preprocessing, the real watermark embedding procedure follows as in Fig 2.a. The secret key *K* is used as a seed to generate *wxh* random numbers over the interval [*1 to rxc*]. Let R_i be the i^{th} random number. A binary matrix *X* of size *wxh* is created such that the entries in the array are the most significant bits of R_i^{th} pixel of the cover image *I*. A binary matrix Z of size wxh is created such that the entries in the array are the most significant bits of the R_i^{th} random number. Now, both the matrices X and Z are bitwise Exclusive-Ored to create a binary matrix *Y* of size *wxh*. Finally a Master Share *M* is created by assigning a pair of bits for each element in the binary matrix *Y*, according to the predefined encryption rules of VC scheme as shown in Table 2. The Master Share, thus created has to be registered with a trusted third party for further verification. Note that, the watermark is not embedded directly into the digital image. The original image is not at all altered and so, at no point of time the watermark information is passed in the transmission channel, thereby providing maximum security.

3.2 Extraction Algorithm

The extraction algorithm extracts the watermark from the intensity image of the host image in case of a gray-scale, or from the Y-component of the color image. Let the relevant component of the host image is referred to as watermarked image *O*. Decomposition of the image to obtain the required component is done in the preprocessing stage of the algorithm. The other inputs to the algorithm are the Master Share *M* and the secret key *K*. The output of the extraction algorithm is the extracted watermark *S'*.

Fig.2.b. shows the process of extracting the watermark from the watermarked image. As seen from the figure the

extraction algorithm follows the same procedure as embedding algorithm to create a binary matrix *Y* of size *wxh.* Now a Verification Share *V* of size *wx2h* is created in such a way, that if the element in the binary matrix Y_i is '0' then assign $V_i = (0, 1)$ else assign $V_i = (1, 0)$. Finally the watermark can be extracted by performing bitwise logical OR operation on the Master Share and Verification Share.

Table 2. Encryption Rules to Create Master Share

Color of i^{th} pixel in binary watermark(S_i)	i^{th} entry in binary array(Y_i)	Pair of bits to be assigned in master share
Black	1	(0, 1)
Black	0	(1, 0)
White	1	(1, 0)
White	0	(0, 1)

4. MULTIPLE WATERMARK EMBEDDING (MWE)

Multiple Watermark Embedding (MWE) extends SWE to embed multiple watermarks in the same image. Multiple watermarks are embedded in the cover image independently, as in SWE. Different secret keys are used with different watermarks to result different Master Shares. These Master Shares are then distributed to the corresponding owners. Note that the watermark is not embedded directly into the digital image. Instead, the cover images information is used to construct the Master Shares. When piracy happens, the detection of multiple watermarks is done independently, using the corresponding author's shares and their secret keys.

5. EXPERIMENTAL RESULTS

The proposed algorithm is tested on many benchmark images [14] of size 512x512. These images are shown in Fig.3. All the images shown are the luminance components obtained after preprocessing the original host images. Fig.4. shows four different sized binary logo images, used in the experiments. Fig.5. shows the results of Single Watermark Embedding (SWE). Fig.5.a. shows the Original Lotus image into which the watermark is to be embedded. Fig.5.b. shows the preprocessed Intensity component of the Lotus image of size 500x300. Fig.5.c. shows the binary watermark image of size 100x100. Fig.5.d. shows the extracted watermark resulted from stacking the Master Share and Verification Share. Fig.6. shows the results of Multiple Watermark Embedding (MWE) in the same Lotus image. Although some contrast loss occurs, the decoded image can be clearly identified. However, Threshold techniques [8] can be used to resize the decoded image to its original size. Note that the size of the watermarks can exceed the size of original host image.

In practice, there is a very good chance for a watermarked image to be altered (intentionally and unintentionally) while being transmitted through the channel. These alterations may be a result of intentional attacks such as filtering, blurring, etc. or unintentional distortions such as JPEG compression, channel noise addition etc. To test the robustness of the proposed algorithm, the watermarked images were subjected to various image manipulating operations and compression attacks. All attacks are implemented using the Matlab Image Processing Tool box. Finally, the performance of the algorithm with respect to attack resilience has been established by the results shown in Table 3. The watermarking survived all. In the table, only the binary outcomes of different attacks are reported, that is, whether the watermark extracted has survived in the sense that it is recognizable as a replica of the original watermark, or not. As long as the extracted watermark is recognizable, the purpose is served. There is always a tradeoff between the perceptual quality of the watermarked image produced by an algorithm and the quality of the extracted watermark under noise and other degradations. Hence, after establishing with different images that the visual quality of our watermarked images is acceptable, the results are presented.

Figure 3. Test images used in the experiments

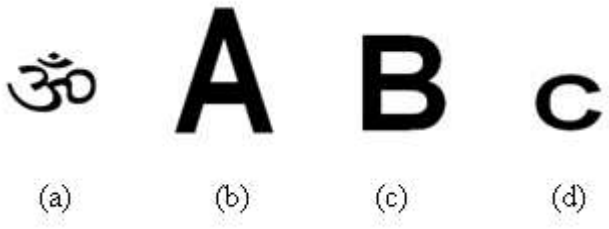

Figure 4. Multiple Watermarks used in the experiments

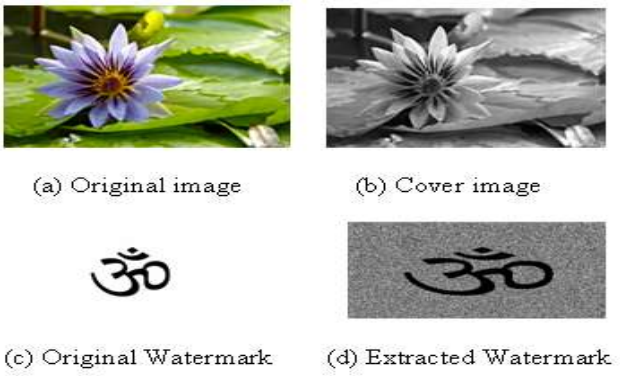

Figure 5. Results of Single Watermark Embedding (SWE)

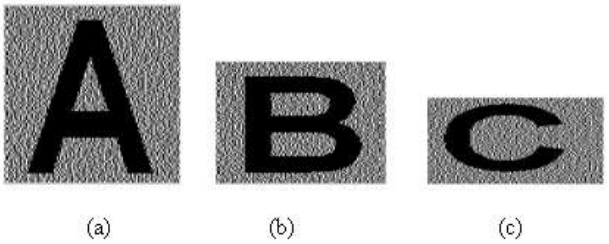

Figure 6. Results of Multiple Watermark Embedding

Table 3: Test Results for Robustness against Several Attacks

Attack performed for testing	Lena	Pepper	F-16	Mandrill
JPEG Compression 0 quality	Survived	Survived	Survived	Survived
Blurring	Survived	Survived	Survived	Survived
Sharpening	Survived	Survived	Survived	Survived
Salt & pepper noise	Survived	Survived	Survived	Survived
Median filtering	Survived	Survived	Survived	Survived

6. CONCLUSIONS

This paper proposed an invisible watermarking technique to embed multiple binary watermarks into digital images, based on the concept of Visual Cryptography. Unlike traditional watermarking schemes, the watermark is not embedded directly into the digital image. Instead, the proposed method constructs multiple Master Shares for the authors according to the original image and the corresponding watermarks. When piracy happens, the authors can show their Shares to reveal the watermarks. The proposed scheme embeds multiple watermarks without modifying the host image. Thus, at no point of time, the watermark information is passed in the transmission channel, thereby providing maximum security. In addition, the size of the watermarks is not restricted to being smaller than that of the host image. Experimental results prove that, the proposed watermarking technique is resilient to several common attacks such as blurring, sharpening, JPEG compression and noise adding. However, the proposed scheme is not resistant to some attacks like rotations, cropping, scaling, contrast adjustments and translations. Further work would improve on these lines.

7. ACKNOWLEDGMENTS

The authors acknowledge the management of TRR institutions, Hyderabad, for their constant encouragement in completing this work.

8. REFERENCES

[1] Anderson R. J., Ed.1996., Information Hiding, in The 1st International Workshop, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1174, 1-7.

[2] Braudaway G. W., K. A. Magerlein, and F. Mintzer.1996, Protecting Publicly-available Images with a Visible Image Watermark, in the Proceedings of SPIE, 2659, 126–133.

[3] Chang, C.C., Chaung ,J. C.2002., An Image Intellectual Property Protection Scheme for Gray-level Images using Visual Secret Sharing Strategy, Pattern Recognition Letters, 23, 931−941.

[4] Chang, C. C., Hsiao, J. Y., and Yeh, J. C.2002., A Color Image Copyright Protection Scheme based on Visual Cryptography and Discrete Cosine Transform, The Imaging Science Journal, 50, 133−140.

[5] Cox, I. J.,M. L. Miller, and J. A. Bloom. 2002, Digital Watermarking, New York: Morgan Kaufmann Publishers Inc., San Fransisco, CA.

[6] Cox, I. J., Kilian, J., Leighton, T., and Shamoon, T..1997, Secure Spread Spectrum Watermarking for Multimedia, In IEEE Transactions on Image Processing, 6(12), pp. 1673−1687.

[7] Fu M. S., 0. C. Au. 2004, Joint Visual Cryptography and Watermarking, In Proceedings of IEEE International Conference on Multimedia and Expo, 975-978.

[8] Hawkes W., A. Yasinsac, C. Clin. 2000, An Application of Visual Cryptography to Financial Documents, Technical report TR001001, Florida State University .

[9] Hou Y-C, P-M Chen.2002, An Asymmetric Watermarking Scheme based on Visual Cryptography, In Proceedings of ICSP, 2, 992 -995.

[10] Hwang R.2002, A Digital Image Copyright Protection Scheme based on Visual Cryptography, Tamkang Journal of science and Engineering,.3(2), 97-106.

[11] Kutter M. and F. A. P. Petitcolas. 1999, A fair benchmark for image watermarking systems, In Proceedings of Security and Watermarking of Multimedia Contents, 226–239.

[12] Langelaar G.C., J. van der Lubbe and J. Biemond. 1996, Copy protection for multimedia data based on labelling techniques`, 17th Symposium on Information Theory, Benelux.

[13] Noar M and A. Shamir. 1995, Visual Cryptography, Advances in Cryptography Eurocrypt'94, Lecture Notes in Computer Science, Springer-Verlag,Berlin, 950, 1-12.