

A novel digital image watermarking scheme based on visual cryptography with colored watermark and colored host image

HARINANDAN TUNGA¹ and SOUMEN MUKHERJEE²

¹Department of Computer Sc. & Engineering RCC Institute of Information Technology
Kolkata, West Bengal-700.015 (INDIA)

²Department of Computer Application RCC Institute of Information technology
Kolkata, West Bengal-700.015 (INDIA)

(Acceptance Date 6th January, 2012)

Abstract

This paper proposes a copyright protection scheme for color images and colored watermarks using visual secret sharing based on the concept of visual cryptography. Most watermarking algorithms call for a piece of information to be hidden directly in media content, in such a way that it is imperceptible to a human observer, but detectable by a computer. This paper presents an improved cryptographic watermark method based on Hwang and Naor-Shamir approaches. The technique does not require that the watermark pattern to be embedded in to the original digital image. Verification information is generated and used to validate the ownership of the image. The method is expected to be proved robust for various image processing operations such as filtering, compression, additive noise, and various geometrical attacks such as rotation, scaling, cropping, flipping, and shearing.

Keywords : Digital Watermark, Visual Cryptography Copyright Protection, Secret Sharing, Pixel Expansion, Peak Signal-to-Noise Ratio (PSNR), Mean Square of Error (MSE).

I. Introduction

In cyberspace, however, the availability of duplication methods encourages the violation of intellectual property rights of digital data, such as document, image, audio, and video⁴. Therefore, the protection of the rightful

ownership of digital data has become an important issue recently. Today, researchers have proposed many techniques to protect the intellectual property rights for digital images. Digital watermarking, a type of such technique, is a method that hides a meaningful signature, or the so-called digital watermark, in a host

image for the purpose of copyright protection, image authentication, copy protection, and captioning⁹. When the rightful ownership of the image must be identified, the hidden watermark can be extracted for ownership verification. Digital watermarking algorithms³ have been in production catering to this aspect lately. This paper proposes a novel solution for watermarking digital images. Watermarking will be conducted without directly embedding patterns into images. This leaves marked images unchanged with respect to size and other image properties. Retrieving the watermark pattern from the marked image will be reasonably fast and without the help of original host image. At first existing watermarking methods are briefly explained. Afterwards the proposed watermark method is explained and illustrated in detail. Afterwards the experimental results are detailed.

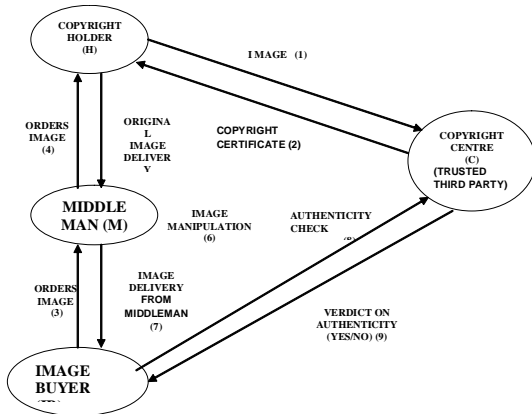


Figure 1. Digital Rights management system

We envision the watermark system operating an open environment like the Internet with different interconnected computers. Users can be located anywhere and can sell or buy images. The salient features of this system are highlighted below^{5,6}.

1. The host image is in the possession of the image owner or the copyright holder. The right for the colored watermark, which may be the proprietor's logo, is also reserved with him.
2. For legal dispute resolution or authenticity verification the Copyright Holder (H) sends copyright information (watermark) and authentic image information to the Copyright Certificate Center (C).
3. At the copyright centre (C) the following steps are followed for copyright registration.
 - a) The copyright verification information is generated with the help of
 - (i) Original host image
 - (ii) Original watermark and
 - (iii) A random array associated with the particular process of verification share generation.
 - b) The verification share, the owner's logo (watermark) and the random array used are registered to the owner of the host image and kept in the database.
 - c) The original host image is returned to the owner. Thus the host image is used for one time registration purpose only⁸.
4. The image buyer (IB) orders the image from the image owner through a middle party (M). M might be trusted or untrustworthy middleman. We assume the latter and M performs image manipulations while delivering the host image to IB from H.
5. On receiving the host image its authenticity is in question. So IB takes the suspect received image to the copyright centre C.
6. The copyright centre replies with a yes/no answer on the authenticity of the image received, by a verification process which uses verification information registered previously with H and its original image.

II. Related Works

Naor and Shamir² give a brief concept of Visual Secret Sharing Scheme in their work. Hwang *et. al.*¹ gives an idea how digital copyright protection scheme is used for grey level images using visual cryptography. Braudaway *et. al.* use the concept of protecting publicly-available images with a visible image watermark. Hwang *et.al.*¹² in their work gives a concept how watermarking technique based on one-way hash functions can work. Eskicioglu *et. al.*⁴ done a work on digital video content protection. Swanson *et. al.*⁷ done one work on transparent robust image watermarking. Xia *et. al.*⁹ done a work on multiresolution watermark for digital images.

III A. Visual Cryptography and Digital Watermarking Technique :

The growth of networked multimedia systems has magnified the need for image copyright protection. One approach used to address this problem is to watermark the image using visual cryptography². Visual cryptography is a concept introduced by Naor and Shamir in 1994², which is a kind of cryptography that can be decoded directly by the human visual

system without any special calculation for decryption. Naor and Shamir further describe the visual cryptography scheme as a visual secret sharing problem in which the secret message can be viewed as nothing more than a collection of black and white pixels as illustrated on Table 1. Each pixel P in the shared image is divided into two sub pixels in each of these two shadows. If P is black, then the dealer randomly selects one of the first two rows in Table 1. If P is white, then the dealer randomly selects one of the last two rows in Table 1. Then, the dealer puts two sub pixel blocks from Columns 2 and 3 to the corresponding positions in shadows 1 and 2, respectively. Let's consider the result when these two shadows are stacked together. For each pixel P in the shared image, if P is black, then it generates a block with two black sub pixels when these two shadows are stacked together. If P is white, then it generates a block with one black sub pixel and one white sub pixel when these two shadows are stacked together^{10,11}.

III B. Concept of Pixel Expansion:

Hwang's method¹ is based on the simple (2, 2) visual threshold scheme presented by Naor-Shamir². According to Hwang, the

Table 1. A(2,2) – Visual threshold scheme; Note: bit “1” denotes black and bit “0” denotes white.

Pixel	Block 1	Block 2	Block 1 superimposes on Block 2
Black	(1,0)	(0,1)	(1,1)
Black	(0,1)	(1,0)	(1,1)
White	(1,0)	(1,0)	(1,0)
White	(0,1)	(0,1)	(0,1)

owner should select $h \times n$ black/white image as his/her watermark pattern W and a key S which must be kept securely. Then, verification information V is generated from the original $k \times 1$ image I and the watermark pattern W using the key S ; as follows:

1. Use the secret key S as the seed to generate $h \times n$ different random numbers over the interval $[0, k \times 1]$. (R_i represents the i th random number).
2. Assign the i -th pair ($Vi1, Vi2$) of the verification information V based on the following Table 2:

Table 2. Rules to assign values of verification information

The color of the with pixel in watermark pattern W is	The left most bit of the R_i -th pixel of image I is	Assign the i -th Pair ($Vi1, Vi2$), of Verification information V to be
Black	"1"	(0,1)
Black	"0"	(1,0)
White	"1"	(1,0)
White	"0"	(0,1)

($Vi1, Vi2$) pairs are used to construct the verification information V . This verification information is registered with the copyright centre / trusted third party. In case the owner claims the ownership of an image W' as a copy of the original image W , he/she provides the secret key S , and the watermark pattern is restored using the image W' and verification information V as follows:

1. Use S as the seed to generate $h \times n$ different random numbers over the interval $[0, k \times 1]$. (R_i represents the i -th random number).
2. Assign the color of the i -th pixel of the watermark pattern W' based on the image

F as follows:

- a. Get the left-most bit, b , of the R_i -th pixel of image F , and if b is 1 then, assign $ti = (1,0)$; otherwise assign $ti = (0,1)$.
- b. If ti is equal to i -th pair of V then assigns the color of the i -th pixel of W' to be white; otherwise, assign it to be black.
3. If W' can be recognized as identical to W visually, then it shall be adjudged that the image I' is a copy of I .

This method has limitations in the sense that it does not give consideration to the rotation, and scaling of images. Moreover it is not flexible enough for the image owner to use anything other than grey-leveled host images and only binary watermarks are to be used for proof of authentication purposes¹³.

IV A. The Proposed Scheme

Hwang's method has the following limitations-

- It is applied over grayscale images only.
- At present most watermarking schemes perform poor against geometrical attacks, and the robustness of this algorithm is also weak against some of geometrical attacks like rotation, scaling, shearing, and flipping.
- If we have an image F with some similarities with the original image M . The watermark pattern W may be restored successfully, although the image F is not the same as the image M .

Our method is a significant improvement over Hwang's since

- Our scheme is not restricted to either binary watermark or grey-leveled host image; rather we are extending its application to true colored images and watermarks.
- Our technique is focused towards achieving a better stand of test against standard

geometrical attacks.

- The algorithms are designed keeping in mind that the trade off between robustness and transparency is never beyond the point of acceptance.

IV B. Schematic Description Of The Proposed Scheme:

I) Verification Share Registration-

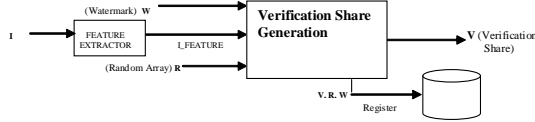


Figure 2. Verification Share Registration

- The original image (I) is first fed to a Feature Extractor, which generates a unique image feature matrix $I_FEATURE$ corresponding to I.
- $I_FEATURE$, the original watermark W, and the random array (R) unique to the process is fed as input to a Verification Share Generator.
- This Verification Share Generator produces Verification Share (V) as the output.
- V, W and R are registered with the copyright holder and kept in the database securely. The original image (I) was returned to the owner as soon as the feature matrix was generated.

II) Authenticity Checking –

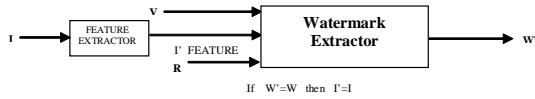


Figure 3. Authenticity Checking

- The Feature Extractor generates $I_FEATURE$ from the suspect image I' .
- V (verification share) and R (random array) are retrieved from the database.
- V, R and $I_FEATURE$ are fed to a Watermark Extractor which generates a Watermark W' corresponding to I' .
- W' and W (original) are compared now visually and also signal properties are compared. If it is found to be satisfactory such that W' can be said to be the same as W then we can infer that I' must be same as I. otherwise I' is a heavily distorted or fake version of the original image I.

III) Verification Share Generation Process

It consists of the following steps -

i) Image Feature Extraction –

- $I_{pxqx3} = (I-R)_{pxq} + (I-G)_{pxq} + (I-B)_{pxq}$
- $I_FEATURE(i,j)_{pxq} = \max(I_R(i,j), I_G(i,j), I_B(i,j))$

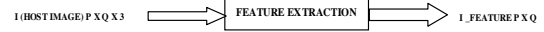
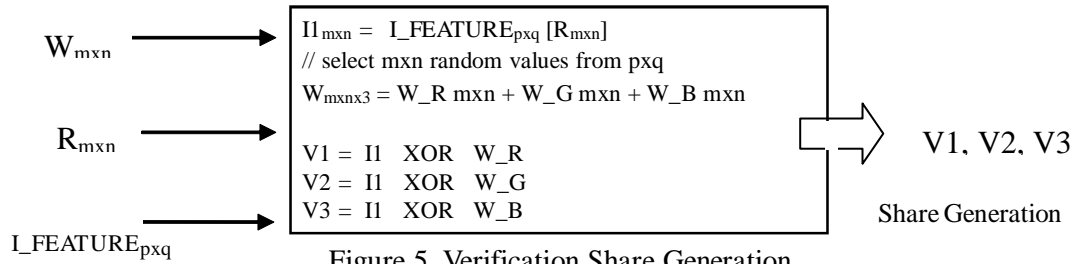


Figure 4. Image Feature Extraction

- The host image (in RGB format) $I_{p \times q \times 3}$ is decomposed into its R, G and B planes to yield $I_R_{p \times q}$, $I_G_{p \times q}$, $I_B_{p \times q}$ matrices.
- Each (i,j) th pixel value of the three color planes are compared.
- The maximum of these value is selected to be the (i,j) th value of the feature matrix ($I_FEATURE$) $p \times q$
- Thus the feature matrix has its dimensions as $p \times q$, downsized from the $p \times q \times 3$ dimension of the original true colored host image to yield optimum space complexity.

ii) Verification Share Generation-



- The colored watermark (RGB) $W_{p \times q \times 3}$ is decomposed into its R,G and B planes to yield W_R , W_G , W_B matrices.
- $m \times n$ random numbers are stored into the matrix R . $R_{m \times n}$ is used to map $m \times n$ random values from $p \times q$ values of the feature matrix $I_FEATURE_{p \times q}$ to generate the matrix $I1$.
- Three verification shares $V1$, $V2$ and $V3$ are generated by respectively XOR-ing $I1$ with W_R , W_G and W_B respectively.

- $V1$, $V2$, $V3$ are registered under the verification shares along with W and R .

IV) Watermark Reconstruction Process-

It consists of the following steps –

i) Image Feature Extraction –

Same as followed earlier only in this case the input to the process is the suspect image I' . The resultant feature matrix is $I'_FEATURE$.



Figure 6. Watermark Reconstruction Process

ii) Watermark Reconstruction -

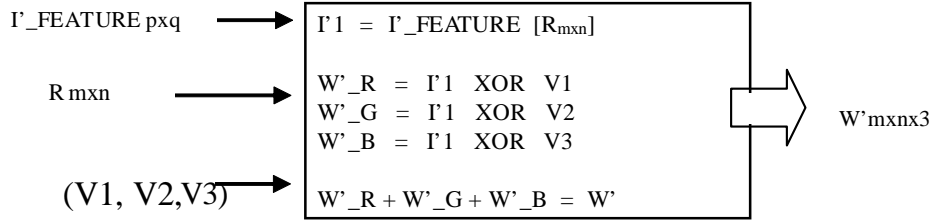


Figure 7. Watermark Reconstruction

- The input to the watermark extractor are $I'_FEATURE$ and R (random array) and $V1$, $V2$, $V3$ which are retrieved from the database.
- $R_{m \times n}$ is used to map $m \times n$ random values from $p \times q$ values of the feature matrix $I'_FEATURE_{p \times q}$ to generate

- the matrix $I'1$ like in the previous case.
- The matrices W'_R , W'_G and W'_B are generated by XOR -ing $I'1$ WITH $V1$, $V2$ and $v3$ respectively.
- W'_R , W'_G and W'_B are combined to produce the watermark pattern W' .

V) Decision Making -

Now W' and W are compared visually and also comparative signal properties are studied to take decisions whether they are identical or not. In the event of them being identical, we can infer that I' is same as I . This is because- $V = (I \text{ XOR } W)$ and $W' = (V \text{ XOR } I')$ are equivalent. Iff $I = I'$ and $W = W'$. ($W' = W \Rightarrow I' = I$).

V. Experimental Results

In order to measure quantitatively the distortion of two watermarks under comparison, Peak Signal-to-Noise Ratio (PSNR) and Mean Square of Error (MSE) are used. These two measurements are usually defined for grey level images so their values are high in our case because we are using RGB images converted into grey level. Deducting a threshold value from these values would've yielded expected normal values.

Table 3. Original Image and Authentic Watermark



ORIGINAL IMAGE	AUTHENTIC WATERMARK
	

Table 4. Signal Distortions













Distorted Image	Distortion Parameters	Reconstructed Watermark (W')	PSNR, MSE values of W & W'
	SATURATION= 39, TEMPERATURE= -58		MSE= 7.3544e+003 PSNR= 9.4653
	RADIUS = 2.3 STRENGTH= 153% SHARPNESS = 34		MSE= 1.6928e+003 PSNR= 15.8447
	EXPOSURE = -28, CONTRAST = 57, HIGHLIGHTS= 41, SHADOWS = 6, BRIGHTNESS = -10		MSE= 7.3275e+003 PSNR= 9.4812

Table 5. Geometric Distortion

	CROPPED 383 X 383 SQUARE		MSE= 9.6018e+003 PSNR= 8.3073
	STRAIGHTENED BY 11.65 DEGREES		MSE= 9.2140e+003 PSNR= 8.4863
	FLIPPED HORIZONTALLY		MSE= 1.1531e+004 PSNR= 7.5120

VI. Conclusion

The proliferation of digitized image is creating a pressing need for copyright enforcement schemes that protect copyright ownership. The watermarking scheme is an excellent method to protect copyright ownership. This paper presented a digital image copyright protection method which does not require that the watermark pattern to be embedded in to the original image which leaves the original host image untouched in further process of reconstructing the watermark. The watermark pattern cannot be retrieved from the marked image unless the key is given. Also the key cannot be retrieved even if all the algorithm components are known. We summarize the characteristics of the proposed method as follows:

- The watermark pattern can be any significant true colored (RGB) image that can be used to typify the owner and the host image can also be any true colored image (dimensions bigger than the watermark)
- The watermark pattern does not have to be embedded into the original image directly. All the pixels of the marked image (indirectly) are the same as those of the original image.
- The watermark pattern can be retrieved without any information about the original image.
- It is hard to detect the pixel concerning the watermark pattern without the secret key (the random array) that is kept secretly by the owner/trusted third party
- The watermark pattern cannot be retrieved from the marked image unless the retriever has the secret key and the verification information simultaneously.
- The notary can adjudge the ownership of the image off-line.

References

1. R.J. Hwang, *Tamkang Journal of Science*

and Engineering, Vol. 3, No. 3, pp. 97-106 (2000).

2. N. Naor and A. Shamir, *Advances in Cryptology: Eurocrypt'94*, Springer-Verlag, Berlin, pp.1-12 (1995).
3. R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, *Proceedings of the IEEE*, Vol. 87, No. 7, Jul., pp. 1108–1126 (1999).
4. E.T. Lin, A.M. Eskicioglu, R.L. Lagendijk, and E. J. Delp, *Proceedings of the IEEE*, Vol. 93, No. 1, January, pp. 171–183 (2005).
5. I. Cox, J. Kilian, T. Leighton and T. Shamon, *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 1673–1687 (1997).
6. C. I. Podilchuk and E. J. Delp, *IEEE Signal Processing Magazine*, Vol. 18, No. 4, Jul., pp. 33–46 (2001).
7. M. Swanson, B. Zhu and A. H. Tewfik, *The Proceedings of IEEE International Conference on Image Processing*, Vol. 3, pp. 211-214 (1996).
8. G. Voyatzis and I. Pitas, *The Proceedings of IEEE International Conference on Image Processing*, Vol. 2, pp. 237-240 (1996).
9. Xia X. G., Boncelet C. G. and Arce G. R., *The Proceedings of IEEE International Conference on Image Processing*, Vol. 1, pp. 548-551 (1997).
10. W. Bender, D. Gruhl, N. Morimoto and, *IBM System Journal*, Vol. 35, No. 3, pp. 313-336 (1996).
11. K. Matsui, J. Ohnishi, and Y. Nakamura, *IEICE Transactions*, Vol. J79-D-II, No. 6, pp. 1017-1024 (1996).
12. Hwang M.S., Chang C.C. and Hwang K.F., *IEEE Transactions on Consumer Electronics*, Vol. 45, No. 2, pp. 286-294 (1999).
13. A. Sleit, and A. Abusitta, *Cybernetics and Informatics*, Vol. 1, pp. 227-238 (2006).