WATERMARKING TECHNIQUES – BINARY AND TRANSPARENCY AUTHENTICATION IN VISUAL CRYPTOGRAPHY

K.S.Charumathi [1], I.B.Rajeswari[2]

[1] *ME Student, Computer Department, Pillai's Institute of Information Technology, Maharastra, India,*
ks.charumathi@yahoo.co.in
[2]*ME Student, Computer Department, Pillai's Institute of Information Technology, Maharastra, India,*
rajeswari_ib@yahoo.co.in

Abstract

With the rapid growth of internet technology, services and devices, transferring of images over internet becomes increasingly popular. This paper proposes a watermarking using binary scheme and transparency authentication scheme used in visual cryptography. Watermarking using binary scheme offers better security than Hwang's method, so that ownership information will not be detected by the attackers. In addition, transparency authentication scheme is embedded in the same image, so that secret image can be perceptible when stacking transparency. In authentication scheme, the Watermark image is half of the size of the secret image and both are encrypted at the same time. Experimental results shows that the scheme effective and practical.

Index Terms: *Cryptography, Digital watermarking transparency, authentication, multiple watermarks, Visual cryptography*

-- *** --

1. INTRODUCTION

Digital watermarking is a powerful technology to provide to protection, authentication and detect alteration. Cryptographic techniques do not solve the problem of illegal copying completely. Digital watermarking provides protection from illegal copying [1].watermarking is used to identify the owner's information by embedding information into a digital image. If the image is copied, then the owner's information is also copied. To avoid this invisible watermarks are added to the applications than visible watermarks [2]. Visual cryptography is hidden technique, and is basically a secret sharing scheme extended for the images [3]. Visual cryptography can be used to hide a two- tone (eg. Binary and half tone image) secret image into a set of binary transparency images. No extra computations and prior knowledge are required while decrypting the images. The secret image is perceptible by human visual system as long as stacking transparency. This paper proposes a watermarking using binary scheme which overcomes the drawbacks Hwang's scheme and transparency authentication scheme used in Visual cryptography. Both scheme based on simple (2, 2) Visual cryptography scheme. Many Watermarking techniques include a binary watermark after converting the gray-level host images into two-tone images [5], [6] using halftone techniques.

In Hwang's method, watermarking is based on simple (2, 2) Visual cryptography scheme. He proposed a scheme [4] which hides binary watermark directly into gray-level images. In His scheme, a secret key is used to select random pixels within the host image. From randomly selected pixels, the most significant bits selected as first share called verification share. The second share called master share that is generated by combining the first share and the binary watermark, using the principles of Visual cryptography scheme. Master scheme is kept with third trusted party. While decrypting the image, the same secret key is used to select the most significant bits(MSB) of the encrypted image and the resulted verification share and the master share are combined to get the original image. The drawback of the Hwang's Scheme is does not provide security. For example, In the host image 90% of the pixels have gray level greater than 128, then 90% of the MSB will have value as logic one. So the verification share is recognized without the knowledge of the secret key indirectly. This paper proposes a scheme to overcome the drawback.

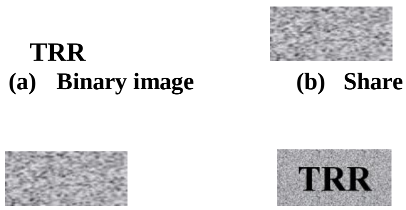
In transparency authentication scheme, a secret image S, another watermark image W is encrypted in two transparency T1 and T2. Content of S can be clearly recognized by stacking T1 and T2. One transparency is shifted to an appropriate Position and overlaps with the other, W will be visible. The rest of the paper is organized as follows section 2 briefly reviews the traditional (2, 2) Visual cryptography Scheme. Section 3 describes the two schemes. Besides some experimental results are illustrative in section 4 that concludes the paper.

2. {2, 2} VISUAL CRYPTOGRAPHY SCHEME

Noar and Shamir [3] was introduced Visual cryptography. A secret is encoded by applying a {2, 2} Visual cryptography Scheme, each and every pixel in host image is replaced with a block of (non-overlapping) 2 subpixels. When these two sub pixels are stacking, the information about the secret image is revealed. For decoding the image, each of the subpixels in stacked with its Xerox copy of other subpixels. If anyone holding one subpixels, will not help to reveal the information about the secret. The following table illustrates the {2, 2} Visual cryptography Scheme for encoding one pixel. A white pixel is divided into two subpixels which are identical. A black pixel is having two subpixels which are complementary blocks. Encoder selects first two columns randomly, if the pixel is white. If the pixel is black, the last two columns are selected from table 1.

Pixel	**White□**		**Black ■**	
Prob	50%	50%	50%	50%
Share 1	■□	□■	■□	□■
Share 2	■□	□■	□■	■□
Stack Share 1 & 2	■□	□■	■■	■■

Fig.1 is the example of {2, 2} Visual cryptography Scheme. Fig 1(d) is the decoded image, black pixels remain black in the next image and white pixels become gray. Since each pixel is replaced by two subpixels, the decoded image with this double that of the host image.



(a) Binary image **(b) Share 1**

(c) Share 2 **(d) Decoded Image**

3. PROPOSED SCHEME

This section describes schemes for watermarking based on binary image and transparency authentication. Scheme 1 overcomes flaws of Hwang's methods. Scheme 2 overcomes security drawbacks of {2, 2} Visual cryptography Scheme.

3.1 Scheme: Watermarking based on binary image

3.1. 1. Encoding Procedure:

This scheme assumes that the binary image watermark(S) of size wxh is to be encoded with the original image (H) of size rxc. Let K be the secret key, randomly selected by the owner. The resultant image of this encoded phase is the watermarked image (O) of size rxc(same as original image) and Master share M of size wx2h. The procedure for encoding the watermark is as follows.

1. Select secret key K randomly to generate wxh random numbers between the intervals (1 to rxc). Let Ri be the ith random numbers.

2. Create binary matrix(X), having a size wxh, such that the array entries are the MSB of Ri th pixels of the original image.

3. Create a binary matrix (Z), having a size wxh, such that the array entries are the Master share scheme of Ri th random number.

4. Create a binary matrix(Y), having a size wxh, such that the Yi = XOR (Xi,Zi).

5. Master share (M) is generated from binary matrix Y, by combining a pair of bits for each elements M the matrix Y. the master key is kept registered with trusted third party.

3.1.2: Extraction Procedure

Extraction algorithm is used to extract the watermark of the attached image. A secret key K, modified image O and the Master share M are the inputs and extract watermark S are the output of this algorithm. Since secret key is used to generate the random numbers. The procedure is same that of encoding procedure upto to step 4. After step 4, verification share is created such that, if the element is binary matrix Y is O. Then Vi = (0, 1) to be assigned or else Vi = (1, 0) is to be assigned.

By performing logical OR operation to extract the secret image. (Si= OR (Mi,Vi))

3.1. 3. Security Analysis

In the scheme, the XOR operation is performed during the encoding phase will provide security, and is better than Hwang's method. The Master share Binary of the selected pixels and the Master share Binary of the corresponding random numbers will be the entries of binary matrix. This XOR operation indicates the large resultant binary matrix, and is used in detection phase. The verification share cannot be estimated by an attacker irrespective of the contrast of the original image.

3.2. Scheme 2

3.2. 1. Transparency Authentication

In this scheme, two transparencies T1 and T2 are created from secret image S and a watermark image W. consider the size of S is 2mx2m and of W is mx2m. The size of two transparencies will be 4mx4m obviously. The encryption scheme is as follows. Note that, the white and the black pixels are represented as 1 and 0 respectively.

Step 1: Secret image S is partitioned into two parts, the upper part SP1, and the lower part SP2. Partition T1 and T2 into 2 segments such that T1 has 2 parts A and B, the upper and lower part respectively. Same way T2 has upper C and lower part D.

Step 2: To encrypt SP1, select any pixel (SP1 (i, j)) randomly. (i, j) is the co ordinates of pixel lies in the range 1≤i≤m and 1≤j≤2m. Divide the secret pixel into 2 subpixels, If SP1 (i,j)=0, it is a black pixel, one share of pixel is placed is 'A' and its complement is placed in C.

Step 3: If the pixel value of W (i,j)=1, then the pixel is divided into 2 identical pixels, one is placed in A and another is placed in D and its indicated by arrow(2).

Step 4: If S (i+m,j)=0 and it is a black pixel, one subpixel is placed in D and its complement part is placed in B. This is shown by arrow (3)

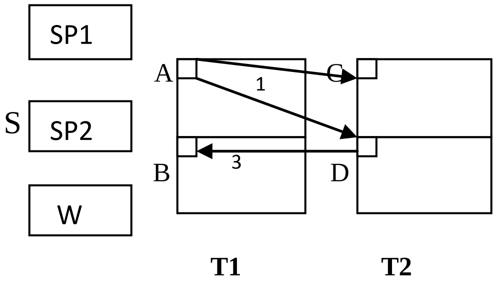
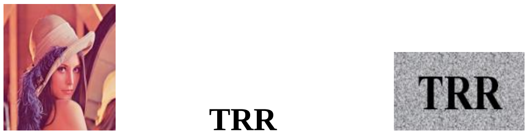


Fig: Secret Image and watermark encryption of scheme 2

4. EXPERIMENTAL RESULTS: SCHEME 1

The proposed scheme is tested on a host image of size 512 x 512 gray-level bitmap Lena image [8] is shown in Fig 2(a). In Fig 2(b), the embedded binary watermark of size 125 x 125 pixels, and Fig 2(c) Extracted watermark is shown.

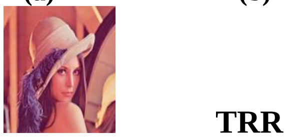


(a)Host image (b)Watermark (c)Extracted watermark

Scheme 2

Fig. (a) and (b) of size 256X256 and 128x256 are S and W respectively. When stacking T1 and T2 content of S can be seen, while alligning upper part of T1 and lower of T2, content of watermark image is clearly distinguishable. This is shown in Fig (e) and (f).

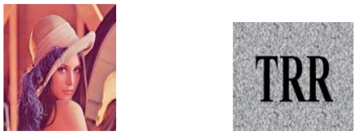
(a) **(b)**



Experimental results of scheme 2.(a) Secret image S (256x256), (b) watermark W (128x256), (c) tranparency T1

(c) **(d)**

(e) **(f)**



(d) tranparency T2, (e) T1 stacking T2(512x512), (f) T1 stacking shifted T2(768x512).

5. CONCLUSION

In this Paper, Hwang's work is extended on watermarking and new scheme is proposed that provides better security and a scheme for transparency authentication is proposed. In scheme 1, multiple watermarks can be included and can be of any size in a single host image. The proposed scheme is not tolerable to some attacks like rotations, cropping, scaling, contrast adjustments and translation. In scheme 2, both secret and watermark images are encrypted at the same time. So, they are authenticating to each other. Apart from this, while decrypting the image no computation is needed and size of the watermark image is half the size of the secret image. Further work would improve on these schemes.

REFERENCES

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

[2] G. W. Braudaway, K. A. Magerlein, and F. Mintzer, "Protecting Publicly-available Images with a Visible Image Watermark", In proceedings of SPIE, Vol. 2659, pp.126-133, 1996.

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

[4] R. Hwang, "A digital Image Copyright Protection Scheme based on Visual Cryptography", Tamkang Journal of Science and Engineering, Vol.3, No.2, pp. 97-106, 2002.

[5] Y-C Hou, P-M Chen, "An Asymmetric Watermarking Scheme based on Visual Cryptography", In Proceedings of ICSP, Vol. 2, pp.992-995, 2000.

[6] M. S. Fu and O. C. Au, "Joint Visual Cryptography and Watermarking", In proceedings of IEEE International Conference on Multimedia and Expo, pp.975-978, 2004.

[7] C. M. Hu, W. G. Tzeng, "Cheating Prevention in Visual Cryptography", IEEE Trans. On Image Processing, vol.16 (1), pp. 36-45, 2007.

[8] www.ece.rice.edu/~walkin/images

[9] S. Punitha, S. Thompson, and N. Siva Rama Lingam "Binary Watermarking Techniques based on Visual Cryptography", IEEE pp. 978-1-4244-7770-8, 2010

[10] Hao Luo, Jeng-Shyang Pan, Zhe-Ming Lu, Bin-Yih Liao "Watermarking-Based Transparency Authentication in Visual Cryptography", IEEE pp. 0-7695-2976-3/07, 2007.

BIOGRAPHIES

K.S.Charumathi has experience in teaching for seven years and pursuing ME (Comp) in Mumbai University. Area of interest is Network Security.

I.B.Rajeswari has experience in teaching for five years and pursuing ME (Comp) in Mumbai University. Area of interest is Network Security.