ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 7, September 2012

A Novel Watermarking Technique Based on Visual Cryptography

A.Umaamaheshvari, K.Thanushkodi

Abstract—**Digital Watermark processing technology has developed very rapidly during the recent years and widely applied to protect the copyright of digital image.**
In today's scenario protection of digital data is utmost necessary in every part of life. More 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 medical images based on the concept of Visual Cryptography (VC). The proposed scheme embeds the watermarks without modifying the original host image. Multiple watermarks can be embedded as shares in the same 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 output of proposed watermarking technique gives good similarity ratio, peak signal to noise ration and correlation coefficient.

***Index Terms*— Copyright, Digital medical image, digital watermarking, Multimedia, visual cryptography.**

I. INTRODUCTION

Modern telecommunication infrastructure supports the possibility of delivering quality health care without the physical presence of medical experts. Important telemedicine applications include health care in rural areas and during space travel. Biomedical signal compression has been an active research area in recent years to achieve efficient data transmission over communication channels of limited bandwidth [1]. Integrity of the transmitted biomedical signals must be assessed as well due to the literally life-and-death nature of the application.

Visible watermarks may be visual patterns such as a company logo, copyright sign, or patient information which overlay about digital images. These are limited in many applications, as they distort the original image fidelity and are susceptible to attacks. Moreover, invisible (or transparent) watermarks, when added to the image can't be retrieved as such. They have wider applications than visible watermarks [2].

Watermarks can be embedded in almost every domain (Spatial, DCT, Wavelet, Fourier etc.) using different schemes[3]. 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 [4]. Those requiring the secret keys and the watermark are called semi-private or semi-blind watermark schemes [5]. In general an effective watermarking scheme should satisfy properties such as invisibility, robustness, security, capacity and low computational complexity [6].

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 [7]. 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.

In this paper, we develop a unified approach to allow multiple levels of authentication[8]. The encryption method, while being able to maintain a high level of data security and, thus, an implied integrity, prevents general access of the signal. 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

II. PREVIOUS RESEARCH

Moni Noar and Adi Shamir[6](1995) first introduced the concept of visual cryptography based on the visual variant k out of n secret sharing problems.After that it gained momentum.

Ryo ITO, Hidenori kiwakado, and Hatsukasu tanaka[11](1999) investigate the visual cryptographic system by proposing a (k,n) visual secret sharing scheme to encode a black and white image into the same size shares as the secret image, where the reconstructed image of the proposed scheme is visible as well as that of the conventional scheme.

Manuscript received Aug 24, 2012.
A.Umaamaheshvari, Electronics and Communication Engineering, Sree sakthi Engineering College/Anna University of Technology/Reional Center. Coimbatore,India,/9486476293
K.Thanushkodi, Director/Akshaya college of engineering and Technology,Coimbatore,India,/9486476295.

Stelvio Cimato, Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci[12] (2005) they Constructed a perfect VCSs with pixel concept .In their schemes each participant is required to store a certain number of transparencies, each having the same number of pixels as the original secret image. Moreover, the schemes guarantee no loss of resolution, since the reconstructed image is exactly the same as the original secret image

Zhi Zhou,, Gonzalo R. and Giovanni Di Crescenzo[13](2006) worked on halftone visual cryptography. This scheme is based on the blue-noise dithering principles. The proposed method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information.

B.SaiChandana , S.Anuradha [14] (2010) study the impact of applying the visual cryptographic system which can be used to hide the original image information from an intruder or an unwanted user. The advantages of the proposed method are its resizing factor and its capability of perfect reconstruction of the secret image. This work is an attempt to make a secured transfer of valuable images between two trusted parties.

Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S.[8](2010) gave an extensive overview of visual cryptographic system.

Mizuho nakajima and Yasushi yamaguchi [15] presents a system which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together.

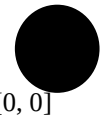
III. Basic (2, 2) Visual Cryptography

A special cryptographic technique allowing visual information was first introduced by Noar and Shamir in 1994. The image is divided into two shares. Here pixel wise masking technique is used. An image is divided into n shares. These n shares are required for decryption. When all the shares are stacked or overlaid original image is recovered.

An equal number of black pixel block and white pixel block is obtained when dividing a pixel. For example If the given pixel p is white, the encoder randomly chooses one of the 2nd two columns of black shares. Half white and half black sub pixels are present in each block whether the corresponding pixel in the secret image is black or white. The black pixels in the original image remain black whereas the white pixels become grey. The decoded image can be clearly identified even though there is some contrast loss. Each pixel in the original image is replaced by two sub pixels, the width of the decoded image is increased twice that of the original image.

TABLE I

Visual Cryptography Scheme for (2,2)

Pixel	White		Black	
Probability	50%	50%	50%	50%
Share 1	 [0,1]	 [1,0]	 [0,1]	 [1,0]
Share 2	 [0,1]	 [1,0]	 [1,0]	 [0,1]
Stack Share 1 & 2	 [0,1]	 [1,0]	 [0, 0]	 [0, 0]

IV. Watermark Embedding and Detection

A. Watermark embedding

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 Ri be the ith random number. A binary matrix A of size *wxh* is created such that the entries in the array are the most significant bits of *Ri* th pixel of the cover image I. A binary matrix C of size *wxh* is created such that the entries in the array are the most significant bits of the *Ri* th random number. Now, both the matrices A and C are bitwise Exclusive-OR ed to create a binary matrix B of size wxh. Finally a Master Share M is created by assigning a pair of bits for each element in the binary matrix B, according to the predefined encryption rules of VC scheme as shown in Table 1. 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.

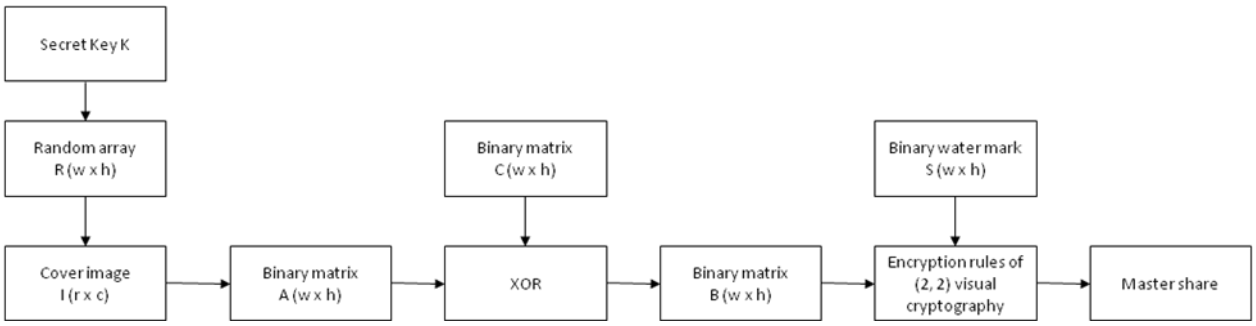


Figure2a. Watermark Embedding Process

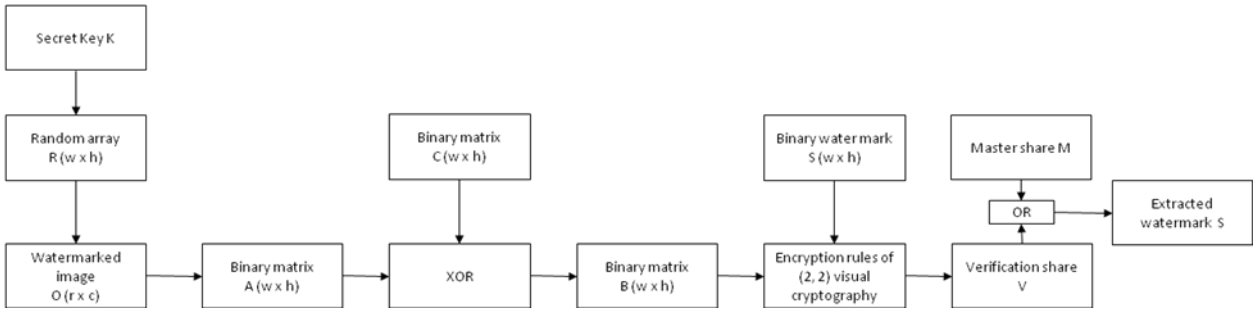


Figure2b. Watermark Extraction Process

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.

B.Watermark Extraction

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 Yi is '0' then assign Vi = (0, 1) else assign Vi = (1, 0). Finally the watermark can be extracted by performing bitwise logical OR operation on the Master Share and Verification share.

C. Construction Algorithm

Input. A gray-level host image **H** of size $M1\times M2$ pixels, a secret image **S** of size $N1\times N2$ pixels,
a window of size $W\times W$ pixels, a private key *PK*, and a codebook *C*.
Output. An ownership share **O** of size $2N\times 2N2$ pixels.
1.Select a list of pixel positions,
$P=\{p1, p2, \ldots, pN1\times N2\}$, with the private key *PK*.
2. Perform the SVD on the window centered at each pixel position in *P* and a sequence of SVs,
$\lambda=\{\lambda^1_1, \lambda^2_{1,\ldots,} \lambda^{N1\times N2}_{1}\}$, consisting of the largest SV of each window, is acquired.
3. Calculate the threshold *Tc*
4. Construct a master share **M** by utilizing the sequence and the threshold *T* according to the code *C*.
5. Create the ownership share **O** by mapping the master share **M** and the secret image **S** to the codebook *C*.

After the ownership share construction, the window size *W*W* pixels, the private key *PK*, and the codebook *C* must be kept secretly by the copyright owner. In addition, the resultant ownership share **O** should be registered to a CA for further authentication.

D. Ownership Identification

Assume that a dispute over the rightful ownership of the host image **H**' has arisen. To determine the rightful ownership of the suspected image, the copyright owner should provide the same window size, private key, and codebook used in the ownership share construction phase, so that the hidden secret image can be revealed after performing the ownership identification procedure. The procedure comprises two stages. The first stage is utilizing the host image **H'** to generate a master share **M'**. The process of master share generation is the same as that used in the ownership share construction phase. The second stage is retrieving the secret image **S'** y using the master share **M**'

and the ownership share **O** according to the VC technique. Since the secret image revelation is based on the VC technique, we can simply print the two shares, **M'** and **O**, onto transparencies and then stack them together to reveal the secret image without the aid of computers. Moreover, with the aid of computers, we can perform the reduction process on the retrieved secret image **S'** to acquire a reduced secret image **S'**, which is of the same size as the original one. The ownership identification procedure is described by the following algorithm.

E. Identification Algorithm

I*nput*. A suspected host image **H'** of size $M1\times M2$ pixels, an ownership share **O** of size $2N1\times 2N2$ pixels, a window of size $W\times W$ pixels, a private key *PK*, and a codebook *C*.

Output. A retrieved secret image **S'** of size $2N1\times 2N2$ pixels and a reduced secret image **S**'of size $N1\times N2$ pixels.

1. Select a list of pixel positions, $P'=\{p'1, p'2, \ldots, pN1\times N2\}$, by using a PRNG seeded with the private key *PK*.
2. Perform the SVD on the window centered at each pixel position in *P*' and a sequence of SVs, $\lambda'=\lambda'1, \lambda'2, \ldots, \lambda'N1\times N2$, consisting of the largest SV of each window, is acquired.
3. Calculate the threshold *T*.
4. Generate a master share **M'** by utilizing the sequence λ' and the threshold *T'* according to the codebook *C*.
5. Retrieve the secret image **S**' by stacking the master share **M'** and the ownership share **O**.
6. Divide the retrieved secret image **S'** into non overlapping 2×2 blocks, $sk'(1\le k\le N1\times N2$.
7. Perform the reduction process to obtain a reduced secret image **S**'.

V .RESULT

This paper proposes a watermarking technique, to directly embed binary watermarks into a 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.

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

The watermarking survived all. 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.

Table.1 shows the PSNR (Peak Signal to Noise Ratio) between the original and the watermarked image expressed in dB and indicating the energy of inserted watermark. The PSNR depends on the mean squared error (MSE) which is calculated according to Eq. (1) where *p* and q are the original and watermarked images, and *M* and *N* are image dimensions. The Structural similarity Ratio gives the idea about how both the images are looking. It is given in equation (2).The Correlation coefficient is used to identify the degree of relationship between the original and recovered image using formula no (4).

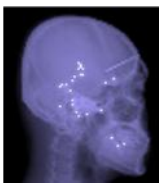
$$MSE = 1/N\sum\sum P(i,j) \quad (1)$$

$$PSNR = 10\log_{10} 255^2/MSE \quad (2)$$

$$SR = (2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)/(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2) \quad (3)$$

$$CR=\rho_{xy}=\frac{E(XY)-\mu_x\mu_y}{\sigma_x\sigma_y} \quad (4)$$

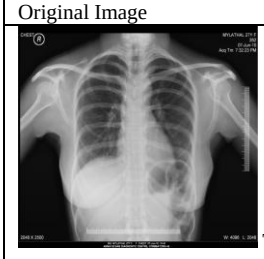
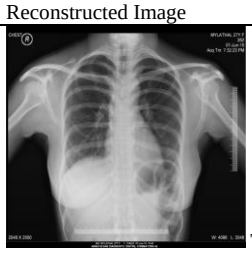
a)Original Image **b)Cover Image**



c)Original Watermark **d)Extracted Watermark**

TABLE I PSNR OF PROPOSED  METHOD

Metric Used	PSNR	SR
Method(9)	57.2177	0.85
Proposed Method	59.8622	0.72

Original Image	Reconstructed Image
 Test Image set 2:	 Test image set 3:

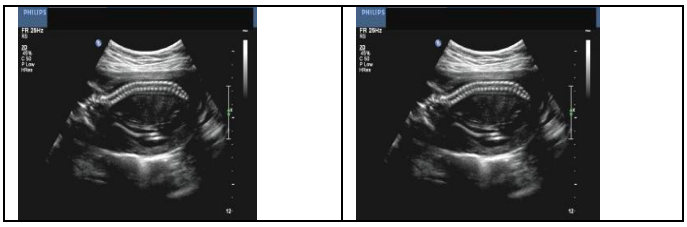


TABLE II CR OF PROPOSED METHOD

Metric Used	Reference[10]	Proposed method
Correlation coefficient test image 2	0.99	0.999
Correlation coefficient test image 3	0.98	0.99

VI. CONCLUSION

This paper proposes the extended visual cryptography scheme for medical images. It shows the method to improve the quality of the image by enhancing the contrast. The trade-off between the image quality and security are assessed by observing the actual results of the method. In our future work we are optimizing the quality of the image by introducing a new concept and calculating the parameters for all types of attacks. The occurrence of violations is stochastic in images constraint fulfillment rate function is to be introduced for optimization.

ACKNOWLEDGMENT

The author express her special thanks to SOWMI clinic for their assistance in providing the images.

REFERENCES

[1] Swanson.M , Kobayashi.M and Tewfik.A, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, vol. 86, pp. 1064–1987, June 1998

[2] Braudaway G. W., Magerlein. K .A and Mintzer.F, Protecting Publicly-available Images with a Visible Image Watermark, in the Proceedings of SPIE, 2659, 126–13F.., 1996.

[3] Zhou yaxun,Ye Qin-wei & Xu Tiefeng, "A New Scheme of image Watermarking based on wavelet and cosine transform,' Actapress .

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

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

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

[7] M. Wu and B. Liu, "Watermarking for Image Authentication", *IEEE Inter. Conf. on Image Processing*,1998.

[8] Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S" An overview of visual cryptography" International Journal of Computational Intelligence Techniques, ISSN: 0976–0466 & E-ISSN: 0976–0474 Volume 1, Issue 1, 2010, PP-32-37

[9] Umaamaheshvari.A and Thanushkodi.K "High Performance and Effective Watermarking Scheme for Medical Images "European Journal of Scientific Research,Vol.67 No.2,2012.

[10] Manimurugan.S and Porkumaran.K" A New fast and Efficient visual cryptography scheme for medical images with forgery detection " proceedings of ICETECT 2011.

[11] Ryo ITO, Hidenori kiwakado, and Hatsukasu tanak ,"Image size invariant visual cryptography',*IEICE TRANS FUNDAMENTALS VOL.E-82 A,NO.10 OCTOBER 1999*.

[12] Stelvio Cimato, Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci "Ideal contrast visual cryptography schemes with reversing", Information Processing Letters 93 (2005) 199–206.

[13] Zhi Zhou, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Giovanni Di Crescenzo," Halftone Visual Cryptography", *IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST 2006*

[14] B.SaiChandana , S.Anuradha," A New Visual Cryptography Scheme for Color Images", International Journal of Engineering Science and Technology Vol. 2(6), 2010, 1997-2000

[15] Mizuho NAKAJIMA andYasushi YAMAGUCHI ,' EXTENDED VISUAL CRYPTOGRAPHY FOR NATURAL IMAGES',wscgpapers-2002

A.Umaamaheshvari,born in Coimbatore District, Tamilnadu state,India in 1974, received the BE in Electrical and Electronics Engineering from Madras University, Chennai. ME in Applied Electronics in Anna University, Chennai and Currently doing Ph.D in Digital Image Processing from Anna University,Coimbatore . Her research interests lie in the area of Computer Networking and Image processing. She has published 8 technical papers in International Journals and presented 4 papers in national and international conferences.She is a member of IAENG,BMESOI,MISTE,MIACSIT.