International Journal of Computer Applications Technology and Research
Volume 3– Issue 1, 33 - 38, 2014, ISSN: 2319–8656

A NOVEL METHOD FOR THE CONSTRUCTION OF THRESHOLD MULTIPLE-SECRET VISUAL CRYPTOGRAPHIC SCHEMES BY WITHOUT PIXEL EXPANSION

P. Saranya
Sri Ramakrishna Arts and Science College for Women
Coimbatore, India

G. Sathayavathy
Sri Ramakrishna Arts and Science College for Women
Coimbatore, India

Abstract : The main concept of the original visual secret sharing (VSS) scheme is to encrypt a secret image into n meaningless share images. It cannot leak any information of the shared secret by any combination of the n share images except for all of images. The shared secret image can be revealed by printing the share images on transparencies and stacking the transparencies directly, so that the human visual system can recognize the shared secret image without using any devices. The visual secrets sharing scheme for multiple secrets is called multiple-secret visual cryptographic schemes (MVCSs). This paper proposed general constructions for threshold multiple-secret visual cryptographic schemes (MVCSs) that are capable of encoding s secret images. This presented MVCS schemes utilize a predefined pattern book with pixel expansion to encrypt secret images into share images. In our research, we propose a novel MVCS scheme that can share two binary secret images on two rectangular share images with no pixel expansion, but also has an excellent recovery quality for the secret images.

Keywords: Cryptography, Visual Cryptography, Visual Threshold, Encryption

1. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer [1]. Visual Cryptography (VC) [2, 3, 4, 5, 6] is a variation of the conventional secret sharing scheme. In VC, instead of a numerical secret key, a secret image is shared among participants in the form of images called shares. Each participant possesses his own share which cannot reveal the secret image being alone, making it necessary to stack more than one share of a qualified participant in order to reveal the secret image. Thus in VC the stacking of shares is equivalent to the decryption process, where neither extra computations nor previous knowledge are required to reveal the secret image. Until now some important VC schemes, such as the *(k,n)*-VC scheme, the general access structure for VC and the extended VC (EVC)[7, 8 ,9, 10, 11, 12] have been proposed. Unfortunately all schemes can be cheated, if one or more participants try to generate their fake shares to force the revealed secret image to be a faked one. In this paper, we propose a cheating prevention VC scheme, in which the shares can be identified and authenticated using the EVC scheme and watermarking techniques. Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text.

In the proposed VC scheme, the share of each participant can be identified by its meaningful appearance instead of noise-like image used in the conventional VC scheme. For the purpose of authentication of each share two binary watermark images are encrypted using shift operation. Before the secret image is revealed, the validation of the shares must be carried out, extracting two watermark images. If they can be extracted correctly, the revealed secret image is considered as authentic; otherwise it is determined as a faked one.

1. VCS is a kind of secret sharing scheme that focuses on sharing secret images. The idea of the visual cryptography model is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image.

2. The secret image can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation OR.

3. In general, a traditional VCS takes a secret image as input, and outputs shares that satisfy two conditions: 1) any qualified subset of shares can recover the secret image; 2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image

Visual cryptography was possible to devise a secret sharing scheme in which an image can reconstructed "visually" by superimposing two shares? Each share would consist of a transparency, made up of black and white pixels. (Note that it would be more accurate to say "transparent" rather than "white".) Examination of one share should reveal no information about the image[13, 13, 15].

Naor and Shamir devised the following scheme, illustrated in the figure below. The algorithm specifies how to encode a single pixel, and it would be applied for every pixel in the image to be shared.

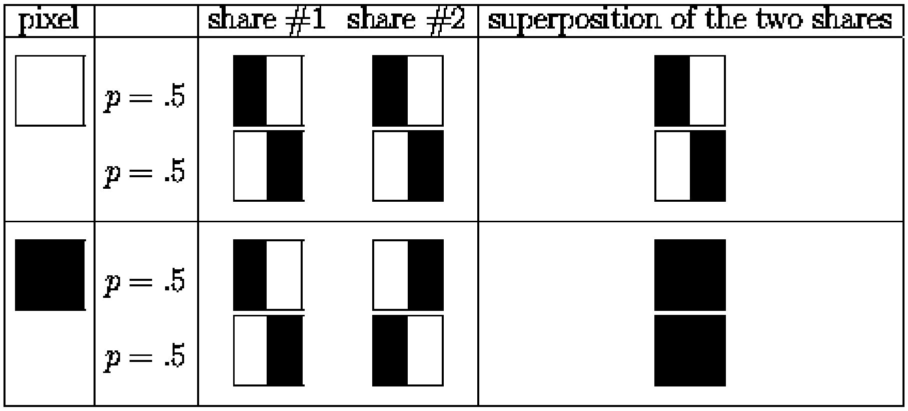

Figure 1.1: Superposition of Two Shares

A pixel P is split into two sub pixels in each of the two shares [18]. If P is white, then a coin toss is used to randomly choose one of the first two rows in the figure 1.1. If P is black, then a coin toss is used to randomly choose one of the last two rows in the figure 1.1. Then the pixel P is encrypted as two sub pixels in each of the two shares, as determined by the chosen row in the figure 1.1. Every pixel is encrypted using a new coin toss.

Suppose we look at a pixel P in the first share. One of the two sub pixels in P is black and the other is white. Moreover, each of the two possibilities "black-white" and "white-black" is equally likely to occur, independent of whether the corresponding pixel in the secret image is black or white. Thus the first share gives no clue as to whether the pixel is black or white. The same argument applies to the second share. Since all the pixels in the secret image were encrypted using independent random coin flips, there is no information to be gained by looking at any group of pixels on a share, either. This demonstrates the security of the scheme.

Now let's consider what happens when we superimpose the two shares (here we refer to the last column of the figure). Consider one pixel P in the image. If P is black, then we get two black sub pixels when we superimpose the two shares; if P is white, then we get one black subpixel and one white subpixel when we superimpose the two shares. Thus, we could say that the reconstructed pixel (consisting of two subpixels) has a grey level of 1 if P is black and a grey level of 1/2 if P is white. There will be a 50% loss of contrast in the reconstructed image, but it should still be visible.

The main focus of this research is to use the visual secret sharing as the part of the cryptography system for getting more the confidentiality, reliability and integrity. With this knowledge, the methods supports for this focus of the research has been considered and dealt.

The main objective of this research is to generate shares of secret image by using no pixel expansion strategy. Then transmit the two secret images with the use of two shares. With stacking two shares, secret image I appear and with stacking one of the shares with 90 degrees rotation in clockwise on other share appears the secret image

2. LITEARTURE SURVEY

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1996[3, 4, 5, 6, 7,8]. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears.

The paper [10, 15] proposed the construction of basis matrices of visual secret sharing schemes for color images under the (t, n)-threshold access structure, where $n \geq t \geq 2$ are arbitrary integers. They treat colors as elements of a bounded semi lattice and regard stacking two colors as the join of the two corresponding elements. They generate n shares from a secret image with K colors by using K matrices called basis matrices. The basis matrices considered in this paper belong to a class of matrices each element of which is represented by a homogeneous polynomial of degree n. They first clarify a condition such that the K matrices corresponding to K homogeneous polynomials become basis matrices. Next, they give an algebraic scheme for the construction of basis matrices. It is shown that under the (t, n)-threshold access structure they can obtain K basis matrices from appropriately chosen $K - 1$ homogeneous polynomials of degree n by using simple algebraic operations. In particular, they give basis matrices that are unknown so far for the cases of $t = 2$, 3 and $n - 1$.

The paper [16, 17, 18] proposed Visual cryptography was introduced by Naor and Shamir. It is a new cryptographic paradigm that enables a secret image to be split into n shares, each share being printed on a transparency. The shares are distributed among n participants of whom only some are qualified to recover the original image. The secret image is reconstructed by stacking a certain number k (2k,n) of these transparencies from the set of qualified participants. If fewer than k transparencies are superimposed, then it is impossible to decode the original image. The resulting cryptographic scheme is called a (k;n) visual threshold scheme (VTS). Since the reconstruction is done by the human visual system, no computations are involved during decoding unlike traditional cryptographic schemes where a fair amount of computation is needed to reconstruct the plain text. It is conceivable that the encryption strategy is such that the color ratios of the different pixels in the reconstructed image are different. In this case, they could define the color ratio of a scheme to be the minimum value of the ratio defined, the minimum being taken over all possible different colored pixels. On the other hand, the encryption strategy could be so regular that each pixel, irrespective of its color, has the same color ratio. In this case, they need not define the color ratio separately for each pixel of the reconstructed image. In such a case, if the color ratio of each pixel is R, they will say that the encoding scheme attains a color ratio R.

The paper [20, 21, 22, 23] A (k; n)-threshold visual cryptography scheme ((k; n)-threshold VCS, for short) is a method to encode a secret image SI into n shadow images called shares such that any k or more shares enable the "visual" recovery of the secret image, but by inspecting less that k share one cannot gain any information on the secret image. The "visual" recovery consists of Xeroxing the shares onto transparencies, and then stacking them. Any k shares will reveal the secret image without any cryptographic computation. In this paper they analyze the contrast of the reconstructed image for (k; n) - threshold VCS. They define a canonical form for (k; n)-threshold VCS and they also provide a characterization of (k; n)-threshold VCS. They completely characterize contrast optimal (n \Gamma 1; n)-threshold VCS in canonical form. Moreover, for n 4, they provide, a contrast optimal (3; n)-threshold VCS in canonical form. They generically transform any *k*out-of-*n* threshold VCS for black-and-white images to color images. During the transformation, they use a probabilistic technique for achieving no pixel expansion. In addition, they also allow the user of the VCS to choose the number of colors that the reconstructed image will have.

3. PROBLEM DEFINITION

A cheating process against a VCS consists of the following two phases:

1. Fake share construction phase: the cheater generates the fake shares;
2. Image reconstruction phase: the fake image appears on the stacking of genuine shares and fake shares.

In order to cheat successfully, honest participants who present their shares for recovering the secret image should not be able to distinguish fake shares from genuine shares. A reconstructed image is perfect black if the sub pixels associated to a black pixel of the secret image are all black.

- More memory space is needed when generating shares by expanding secret image pixels
- Network traffic can be increased when sending shares of secret image over network

3.1 Problem Specification of (k,n,s)-MVCS

Essentially, a (k,n,s) MVCS [25] is capable of encoding secret Images P1,P2,P3…..Ps into shares S1,S2,…Sn which are distributed to the participant in P={1,2…..n} such that each group of k,k+1,….,n shares reveals P1,P2,P3…..Ps respectively, to our eyes when superimposed, but that of less than shares cannot. Here, s=n-k+1 and the cases of s$\leq$n-k+1 can also be generated.

Definition 1

To reveal (or conceal) one pixel ,p$\in$P, either white (0) or black (1) with only two possibilities, in the superimposed result of k (or less than k) shares, the (k,n) -VCS aims at the design of a set of two basis matrices B^0 and B^1 for encoding P=0 or 1, respectively. Now, a set of *corresponding* pixels (p1,p2…ps) , either 0 or 1 for each with totally 2^s possibilities, should be considered in a (k,n,s) -MVCS where pixels ,p1$\in P1, p2 \in P2$,..ps$\in$Ps are regarded as corresponding to each other if their positions in the secret images are all the same. To reveal (or conceal) these corresponding pixels (p1,p2…ps) in the superimposed results of k.k+1,…..n(or less than) shares, respectively, the (k,n,s)-MVCS should rely on a set of nXm 2^s basis matrices $B^{00..0}$,$B^{00..1}$,$B^{11..1}$ to encode (p1,p2…ps) =(0,0,..0),(0,0,…1),…,(1,1,…1) , respectively, into m subpixels for each of the n shares. Assume U={i1,i2….i_u} and V={j1,j2….j_v} Where U,V$\subseteq$ {1,2…n}, and 1$\leq v < k \leq u \leq n$. Let $B^{(p1,p2…ps)}$[U]($B^{(p1,p2…ps)}$[V]) denote the u$\times m(v \times m)$ matrix consists of rows i1,i2….i_u {j1,j2….j_v} in $B^{(p1,p2…ps).}$

Definiton 2

A set of 2_s n$\times m$ Boolean basis matrices $B^{0..00}$,$B^{0..01}$..,$B^{1…11}$, in which the result of a column permutation of $B^{(p1,p2…ps)}$ defines the color of the m subpixels in each one of the shares when sharing corresponding pixels (p1,p2…ps) $\in \{0,1\}$ in p1,p2…ps, respectively, constitutes a (k,n,s)-MVCS where s=n-k+1 if the following conditions are met:

1) For each set of t+(k-1) participants U$\subseteq$ Pwhere 1<T<S And k<|U|(=t+(k-1))<n ,

2)For each set of less than k participants V$\subseteq$ P(1$\leq |V| \leq k-1), H(B_V^{p1,p2…ps}$)= $H(B_V^{p1',p2'…ps'}$) , for p1,p2…ps $\neq p1', p2' … ps'$

where $p_{i,}p_j$’ $\in$\{0,1\} and 1$\leq$i,j$\leq$s.

4. PROPOSED SYSTEM

In this research, we have proposed a novel MVCS scheme for sharing two binary secret images in two share images S_1 and S_2 with no pixel expansion, and have achieved an excellent recovery quality for the revealed secret images. During the encrypting process, the proposed scheme generated share images without any pre-defined pattern books. This process was different from any existing MVCS schemes. By directly stacking the two share images, S_1 and S_2 , the first secret SE_1 could be revealed and be recognized by the human visual system, and the second secret SE_2 could be revealed by stacking one share image and the other with a rotation angle of 180 degree. Neither of the two share images leaked any information of the two secret images. Our proposed MVCS scheme has resolved the pixel expansion problem existing in MVCS schemes, whether sharing one or multiple secrets, and has increased the contrast quality of the revealed secret image by adopting the appropriate encrypting process.

4.2 Proposed Algorithm

Through the DSP, SP, and CMP processes, two secret images were encrypted into two share images. The two share images camouflaged by the proposed camouflaging process with maximum block density were meaningless images. From the above description, a patterns book was not adopted during the process for generating the two share images. All processes were executed block by block for the initially generated share images with h × w size. So, two secret images with h × w size were encrypted into two share images with h × w size. The size of the share image was equal to the size of the secret image. The critical pixel expansion of the visual multiple secrets sharing scheme was solved by our proposed scheme. A complete algorithm for sharing two secrets is shown as follows:

Algorithm 1: Encrypting process of MSCV with no pixel expansion

```
Input: Two h × w secret images SE 1, SE2, block size: n × n, threshold of block density: $d_{TH}$
Output: Two h × w share images $S_1$, $S_2$
Step 1: b p;k i;j $b_{i,j}^{p,k} \leftarrow 0$; ∀i; j; k; p.
Step 2: Randomly generate 4 matrixes $C^1$, C2, C3, C4 by the conditions
    $a_{i,j}^{1,k} = c_{i,j}^{1} + c_{i,j}^{2},$
    $a_{i,j}^{2,k} = c_{i,j}^{3} + c_{i,j}^{4},$
    $|H(C^1) - H(C^2)| \leqslant 1$ and $|H(C^3) - H(C^4)| \leqslant 1, \quad \forall k.$
Step3: Let $b_{i,j}^{1,k} \leftarrow c_{i,j}^{1} \mathrm{v} c_{i,j}^{2}$, $b_{ij}^{2,k} \leftarrow b_{i,j}^{2,k} \mathrm{v} c_{i,j}^{2}$ and
    $b_{n+1-i,n+1-j}^{2,k+1-k}$ ‹ $b_{n+1-i,n+1-j}^{2,k+1-k} \mathrm{v} c_{i,j}^{4} \forall k$
Step 4: if $H(F^{p,k})/n^2 \geq dTH$
    Then $d^{p,k} \leftarrow H(B^{p,k})/H(F^{p,k})$ else $d^{p,k} \leftarrow 0, \forall$ k,p
Step 5: $d_{max}^{p} \leftarrow \max d^{p,k}, \forall p,k; d \leftarrow \max d_{max}^{p}, \forall p$
Step 6: $d^{p,k} \leftarrow d_{max}^{p}, \forall k, p$
Step 7: $k \leftarrow 1$
Step 8: Repeat
    Step 8.1: $r_w^{p,k} \leftarrow \lfloor \bar{d}^{p,k}(n^2 - H(F^{p,k})) \rfloor,$
        $r_w^{p,K+1-k} \leftarrow \lfloor \bar{d}^{p,K+1-k}(n^2 - H(F^{p,K+1-k})) \rfloor, \forall p$
    Step 8.2: $r_w \leftarrow \lfloor n^2 . \bar{d} \rfloor$
    Step 8.3: Randomly generate a camouflaging matrix $C^1$with n × n by the condition
        $H(C^1)=r_w$
    Step 8.4: Repeat
        Step 8.4.1: Randomly select one element $C_{i,j}^{1} \neq 0$ from $C^1$
        Step 8.4.2: if $r_w^{p,k} > 0$ and $f_{i,j}^{p,k}=0$ then $b_{i,j}^{p,k} \leftarrow 1, r_w^{p,k} \leftarrow r_w^{p,k} - 1, \forall p$
        Step 8.4.3: if $r_w^{p,K+1-k}>0$ and $f_{n+1-i,n+1-j}^{p,K+1-k}=0$ then $b_{n+1-i,n+1-j}^{p,K+1-k} \leftarrow 1, r_w^{p,K+1-k} \leftarrow r_w^{p,K+1-k}-1, \forall p$
        Step 8.4.4: $c_{i,j}^{1} \leftarrow 0, r_w \leftarrow r_w - 1$
        Step 8.4.5: until $r_w=0$
    Step 8.5: $k \leftarrow k+1$.
    Step 8.6: until k>K/2
Step 9: Repeat
    Step 9.1: Randomly select one element $b_{i,j}^{p,k}=0$ if $r_w^{p,k} > 0$ and $f_{i,j}^{p,k}=0$ then
        $b_{i,j}^{p,k}$ ‹ $1, r_w^{p,k} \leftarrow r_w^{p,k} - 1$
    Step 9.2: until $r_w^{p,k}=0 \forall k,p$
Step 10: $r_b^{p,k} \leftarrow \lfloor \bar{d}^{p,k} \cdot H(F^{p,k}) - H(B^{p,k}) \rfloor.$
Step 11: Repeat
    Step 11.1: Randomly select one element $b_{i,j}^{p,k}=0$, if $r_b^{p,k} > 0$ and $f_{i,j}^{p,k}=1$
        Then $b_{i,j}^{p,k} \leftarrow 1, r_b^{p,k} \leftarrow r_b^{p,k} - 1$
    Step 11.2: until $r_b^{p,k} \leq 0, \forall k, p$
Step 12: Output share images $S_1$, S2 by $B^{p,k}$
```

5. RESULTS AND DISCUSSION

Applications of this technology is very vast with respect to the security for Possible applications are paper trail on electronic voting which shown by Chaum and encryption of financial documents shown by Hawkes and many other application is possible for example the computer logon by using the one share is in user USB drive and one share is with computer and when user insert the USB computer stacked the images and use image analysis to retrieve the password and allow to logon.

5.1 Comparison Graph Based On CPU Execution Time for Encryption of Images

The experimental result on CPU time can be obtained for proposed system over existing system is shown in the following chart:

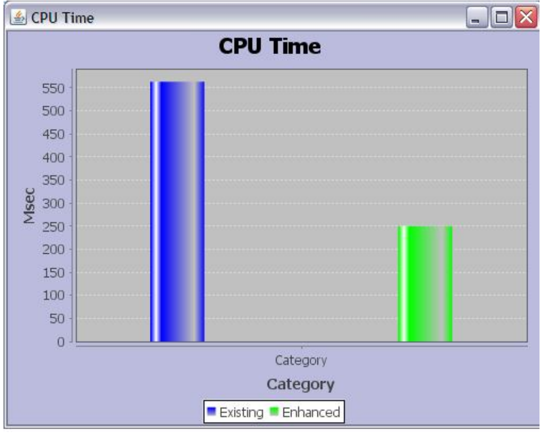

Fig 5.1 CPU Time Comparison for Existing System Vs Proposed System

5.2 Comparison Graph Based On Pixel Size of Encrypted Shares of Source Images

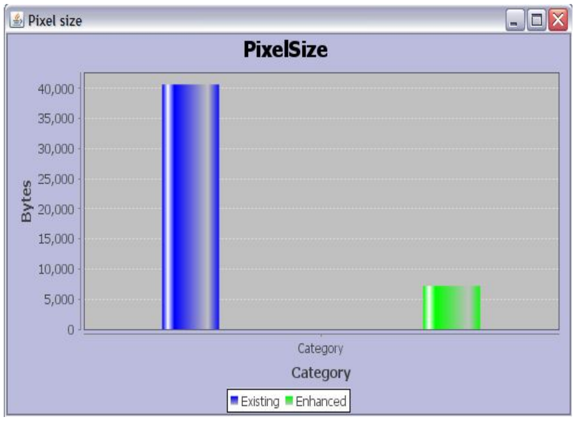

Fig 5.2 pixel size comparison for existing system Vs proposed system

The above graph shows the pixel size for existing and proposed research. The existing system uses pixel expansion so the result returns largest pixel size. Thus the proposed system works on the no pixel expansion and thus returns the smallest pixel size in the result.

6. CONCLUSION & FUTURE ENCHANCEMENT

Visual Cryptography is an image encryption technique used to hide the secure information in images. It allows the encryption of secret image into n number of shares and distributed into n number of participants. For example in (k, n) secret sharing problem the secret image can be visually recover by stacking together any k or more transparencies of the shares. But cannot reveal any secrete information by stacking less than k transparencies together. A novel MVCS scheme that can share two binary secret images on two rectangular share images with no pixel expansion, but also has an excellent recovery quality for the secret images.

FUTURE WORK

In future we can propose a scheme to hide some extra confidential data in transparencies during secret image encryption in visual cryptography. The secret image is multitude into several levels first. An extended non-expansion visual secret sharing model is employed, i.e. size of transparencies is equal to that of the secret image. Thus less time and space are needed for transparencies transmission and storage.

7. REFERENCES

[1] Ateniese.G, Blundo.C, De. Santis.A, and Stinson.D.R, “Extended capabilities for visual cryptography,” *Theoretical Computer Sci.*, vol. 250, pp. 143–161, 2001.

[2] Ateniese.G, Blundo.C, De. Santis.A, and Stinson.D.R, “Visual cryptography for general access structures,” *Inf. Computat.*, vol. 129, pp. 86–106, 1996.

[3] Ateniese.G, Blundo.C, De. Santis.A, and Stinson.D.R, “Constructions and bounds for visual cryptography,” *Lecture Notes Computer Sci.*, vol. 1099, pp. 416–428, 1996.

[4] Blakley.G.R, “Safeguarding cryptographic keys,” in *Proc. Nat. Computer Conf.*, 1979, vol. 48, pp. 313–317.

[5] Blundo.C, De. Santis.A, and Stinson.D.R, “On the contrast in visual cryptography,” *J. Cryptology*, vol. 12, pp. 261–289, 1999.

[6] Blundo.C, D’Arco.P, De. Santis.A, and Stinson.D.R, “Contrast optimal threshold visual cryptography schemes,” *SIAM J. Discrete Math.*, vol. 16, pp. 224–261, 2003.

[7] Blundo.C, Cimato.S, and De Santis.A, “Visual cryptography schemes with optimal pixel expansion,” *Theoretical Computer Sci.*, vol. 369, pp. 169–182, 2006.

[8] Blundo.C, DeBonis.A, and DeSantis.A,“Improvedschemesfor visual cryptography,” *Designs, Codes and Cryptography*, vol. 24, pp. 255–278, 2001.

[9] Bose.M and Mukerjee.R, “Optimal visual cryptographic schemes for general ,” *Designs, Codes and Cryptography*, vol. 55, pp. 19–35, 2010.

[10] Climato.S, R. D. Prisco, and A. De. Santis, “Optimal colored threshold visual cryptography schemes,” *Designs, Codes and Cryptography*, vol. 35, pp. 311–335, 2005.

[11] Chen.T.H and Tsai.D.S, “Owner-customer right protection mechanism using a watermarking scheme and a watermarking protocol,” Pattern Recognit., vol. 39, pp. 1530–1541, 2006.

[12] Droste.S, “New results on visual cryptography,” *Advances in Cryptog- raphy-CRYPTO’96, Lecture Notes in Computer Science*, vol. 1109, pp. 401–415, 1996.

[13] Eisen.P.A and D. R. Stinson, “Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels,” *Designs, Codes and Cryptography*, vol. 25, pp. 15–61, 2002.

[14] Embedded Extended Visual Cryptography Schemes F Liu… - … Forensics and Security, IEEE Transactions on, 2011 - ieeexplore.ieee.org.

[15] Free Software Foundation, lp_solve Reference Guide Menu [Online]. Available: http://lpsolve.sourceforge.net/5.5, since Feb. 1999.

[16] Hofmeister.T, M. Krause, and H. U. Simon, “Contrast-optimal Out of secret sharing schemes in visual cryptography,” *Lecture Notes in Computer Sci.*, vol. 1276, pp. 176–185, 1997.

[17] Jin.D, Yan.W.Q, and Kankanhalli.M.S, “Progressive color visual cryptography,” Electron.J. Imag., vol. 14, no. 3, p. 033019, 2005.

[18] Lin.C.C and Tsai.W.H, “Visual cryptography for graylevel images by dithering techniques,” Pattern Recognit. Lett., vol. 24, no. 1-3, pp. 349–358, 2003.

[19] MacPherson.L.A, “Grey Level Visual Cryptography for General Access Structures,”Master Thesis, University ofWaterloo,Waterloo, ON, Canada, 2002.

[20] Nakajima.M and Yamaguchi.Y, “Extended visual cryptography for natural images,” in Proc. WSCG Conf. 2002, 2002, pp. 303–412.

[21] Naor.M and Pinkas.B, “Visual authentication and identification,” in Proc. CRYPTO’97, 1997, vol. 1294, pp. 322– 336, Springer-Verlag LNCS.

[22] Naor.M and Shamir.A, “Visual cryptography,” in Proc. OCRYPT’ 94, Berlin, Germany, 1995, vol. 950, pp. 1–12,Springer-Verlag, LNCS.

[23] Tuyls.P, Kevenaar.T, Schrijen.G.J, Staring.T, and Van Dijk.M,“Security displays enabling secure communications,” in Proc. First Int. Conf. Pervasive Computing, Boppard Germany, Springer-Verlag Berlin LNCS, 2004, vol. 2802, pp. 271–284.

[24] Tsai.D.S, Chenc.T, and Horng.G, “On generating meaningful shares in visual secret sharing scheme,” Imag. Sci. J., vol. 56, pp. 49–55, 2008.

[25] Wang.Z.M, Arce.G.R, and Di Crescenzo.G, “Halftone visual cryptography via error diffusion,” IEEE Trans. Inf. Forensics Security, vol.4, no. 3, pp. 383–396, Sep. 2009 .

[26] Zhou.Z, Arce.Z.R, and Di Crescenzo.G, “Halftone visual cryptography,”IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453,Aug. 2006.