Ideal Contrast Secret Sharing Scheme through Meaningful Shares with Enveloping Digital Watermarking using Bit Plane based *(k,n)*-VCS

Aarti
Dept. of Computer Science
Dr. B. R. Ambedkar NIT,
Jalandhar,India

Harsh K Verma
Professor and Head, CSE
Dr. B. R. Ambedkar NIT,
Jalandhar,India

Pushpendra K Rajput
Dept. of Computer Science
Dr. B. R. Ambedkar NIT,
Jalandhar,India

ABSTRACT

Visual Cryptography Scheme (VCS) is an encryption method that works on human visual system. It encrypts a secret image into *n* shares and decryption can be done only by stacking *k* or more share images without any computation. A new secret sharing scheme with meaningful shares using *(k,n)*-threshold visual cryptography and digital watermarking for grayscale images based on bit plane encoding is proposed in this paper, that encrypts a grayscale secret image in such a way that results of encryption is in the form of shares. Shares do not reflect any information directly, information is scrambled instead. Firstly, an image is decomposed into its bit plane images that generate a binary image at each bit plane. Secondly, the traditional binary secret sharing scheme is used to get the sharing images. Finally, a proposed watermarking technique is used to generate meaningful shares. To decrypt hidden secret image, extract the shares from the cover image and decompose each share into bit planes and then secret grayscale image is reconstructed. This scheme provides a more efficient way to hide images in different meaningful shares. Furthermore, the size of the hidden secret can be recovered by inspecting the blocks in the shares.

General Terms

Secure Secret Sharing on Network

Keywords

visual cryptography scheme (VCS), bit plane encoding, pixel decomposition, digital watermarking, contrast

1. INTRODUCTION

To transfer the multimedia data via the Internet is a common task. The transferrable data may be more important due to which security is a big concern. Many traditional cryptographic techniques can be used to protect information security. But most of them have a lot of computation to decrypt the hidden secret.

Naor and Shamir[1] in 1994 introduced Visual Cryptography (VC), a technique of information security which protect images that has a computation free decryption process. The decryption is done using human Visual System (HVS). In a *(k,n)*-threshold Visual Cryptography Scheme (VCS), one binary secret image was encoded into *n* random looking shares. These *n* shares are printed on *n* transparencies and distributed into a set of *n* participants. When *k* or more participants stacked their shares together, the secret image is visually revealed. But stacking the transparencies less than *k* cannot reveal any information about the secret image.

Besides a lot of work on visual cryptography for black and white images [1-6], some studies [7-10] focused on the practical realization of visual cryptographic schemes for gray-level or color images. Unfortunately, Visual Sharing System (VSS) cannot restore the secret image to its original quality when the original input is a natural image. The VCS can be applied to encrypt continuous tone (grayscale or color) image using halftone technology [12-15]. The contrast of a continuous tone image is reduced because in these cases halftone image is used instead of original information that is a limitation of visual cryptography. To reduce the interest of hackers towards random looking shares many techniques are introduced[16-17] that digitally watermark the random looking shares to produce meaningful shares that are some meaningful images.

Lukac and Plataniotis [18] proposed an image encryption scheme using VCS based on bit planes. The encryption scheme decomposed the gray scale image into 8 bit planes that are equivalent to 8 binary images and applied the VCS to each bit plane in order to get *n* random looking binary images. By stacking the corresponding binary images in bit level, the gray-scale noisy shares can be generated.

This type of visual cryptography technique is insecure as the random looking images have more interest of hackers as they treat them as critical information in the transmission. If the random looking shares are enveloped into some meaningful images the interest of hackers can be reduced. Therefore, we have proposed a technique called digital enveloping. This is nothing but an extended invisible digital watermarking technique. Using this technique, the shares, produced by *k-n* secret sharing visual cryptography introduced by Lukac are embedded into the envelope images by LSB replacement [19-20].

This paper is organized as follows. Section II introduces the fundamental principles of VC, then VC for gray-level images having some idea about halftone technology and bit level based secret sharing. Then the propose scheme is demonstrated in Section III. Section IV illustrates several experiment results. Finally, concluding remarks are given in Section V.

2. RELATED WORK

2.1 Fundamental principles of Visual Cryptography

Naor and Shamir’s [1] VCS assumes that message consists of a collection of black and white pixels. Each pixel is handled separately and used to generate *n* modified versions (shares), one for each transparency. Each version, which is a collection of *m* black and white subpixels. Let *S* is a binary image having spatial resolution *K1 × K2* and it is encrypted into *n* shares S_1, S_2,….S_n, then each share has the spatial resolution of *mK1×mK2, w*here *m* is known as expansion factor.

Definition 1. A solution to the *k* out of *n* visual secret sharing scheme consists of two collections of *n × m* Boolean matrices *C0* and *C1*. To share a white pixel, the dealer randomly chooses one of the matrices in *C0,* and to share a black pixel, the dealer randomly chooses one of the matrices in *C1*. The chosen matrix defines the color of the m subpixels in each one of the *n* transparencies. The solution is considered valid if the following three conditions are met.

1. For any S in *C0*, the OR V of any *k* of the n rows satisfies $H(V) \le d - \alpha . m$.

2. For any S in *C1*, the OR V of any *k* of the *n* rows satisfies $H(V) \ge d$.

3. For any subset $\{i_1, i_2,….., i_q\}$ of {1, 2,…., n} with q < k, the two collection of q × m matrices D_t for t ϵ {0, 1} obtained by restricting each n × m matrix in C_t (where t =0 ,1) to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Example 1. *(2,2)-Black and white VC: (2,2)*-binary visual cryptography decomposes every pixel in a secret image into a *2 × 2* block in the two transparencies according to the rules in Fig.1. The matrix representation of the rules (shown in Fig. 1) or the basis matrices and collection of the encoding matrices can be written as

C_0 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ }

C_1 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$ }

When a pixel is white choose one of the six combinations for white pixels, one for each transparency; When a pixel is black then chooses one of the six combinations for black pixel, one for each transparency. There are six possible combinations that provide the security of scheme, any combination can be chosen by random number having equal probability.

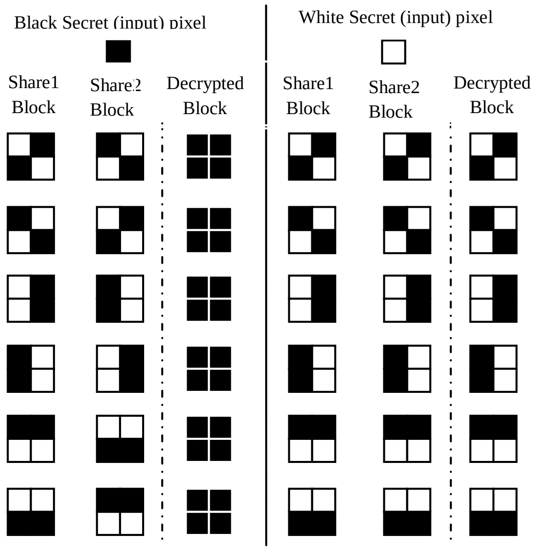


Fig 1: ***(2 ,2)*** **Binary Sharing and Stacking scheme**

The stacking rules for two pixel values are:

$$\textit{Pixel Value} = \begin{cases} \textbf{\textit{White}}, \text{ if both pixels are white} \\ \textbf{\textit{Black}}, \text{ otherwise} \end{cases}$$

By applying this scheme every combination for black pixels produces full black block and that produces half black and half white in the case of white pixel.

2.2 Visual Cryptography for gray-level Images

2.2.1 Halftone visual cryptography

Due to the input requirement of visual cryptography as binary image, It is necessary to convert the gray-level image into the binary image to apply VCS. The one method to convert the continuous tone image into binary image is halftoning. Most of the printers work on the phenomenon that a single pixel should be printed or not to be printed, instead of displaying the gray-level or color tone of an image. The dark area of an image has a large number of dots and bright area has comparatively less. The method that uses the density of the net dots to simulate the gray-level is called “Halftone”[11] that transforms an image with gray-level into a binary image before processing. There have been many published studies[15-20] of visual cryptography that uses halftoning to convert a gray-level or color image into binary image. A simple algorithm to encrypt gray-level image using halftoning is as follows:

1. Transform the gray-level image into a black and white halftone image
2. For each pixel of haltonned image apply conventional VCS.

2.2.2 Bit level based secret sharing

Lukac and Plataniotis propose an image encryption algorithm that decrypt the image with real size and ideal contrast. The algorithm divides the grayscale secret image into 8 bit planes which are binary images. Then by applying *(k,n)*-thresold VCS on each bit plane image, share can be generated.. In the decryption phase the shares are decomposed into bit planes and corresponding bit planes from k shares are stacked to generate k or more binary hidden secret image. Now apply inspection function to find the real size of image and combine all the binary hidden secret to reveal the hidden secret image.

3. THE PROPOSE SCHEME

The random looking shares generated by the many visual cryptography schemes have more interest of hackers and it is difficult to recognize that which share belong to which participant. To recover these difficulties the propose scheme uses enveloping the random looking shares that are some meaningful images and provides more security to the visual cryptography. To find the real contrast of the recovered image a bit plane based VCS is used to generate random looking shares. Our propose scheme can share one grayscale secret image into *n* random meaningful shares using the bit plane encoding for each channel, and then digital watermarking, while *k* or more random looking shares can perfectly reconstruct the secret image. The flowchart of the proposed scheme is illustrated in figure 2 and figure 3 (Encryption and Decryption phase respectively). Detailed description of the proposed scheme is formulated in the following phases.

3.1 Random-Looking Share Generation

We consider a $w \times h$ grayscale secret image (denoted as S) with *8* bits per pixel. A single pixel value *S (i, j)* with *8* bits image can be represented in a binary form using Eq.(l). Grayscale image is decomposed into its *8* 1-bit plane and every bit plane is a binary image containing a level of information.

$$\mathrm{S}(i,j) = S_{b1}\,(i,j).\,2^{N-1} + S_{b2}\,(i,j).\,2^{N-2} + \cdots$$
$$\ldots. + S_{b(N-1)}\,(i,j).\,2 \; + S_{b8}\,(i,j) \qquad (1)$$

Here, S_{bi} *(i, j)* represents the pixel value in location *(i, j)* in *i-th* bit plane of each channel, and S_{bl}*(i, j)* is the most significant bit plane. Therefore, a channel can be divided into *N* binary images using Eq.(l).

Then, every pixel of all the binary images generated from the bit plane is expanded into a 2× 2 block to which a black or white color is assigned according to the model presented in Fig. 1. Every block of the sharing images therefore includes two white pixels and two black pixels so that the entropy reaches its maximum to conceal the content of the secret image.

The *(k-n)* threshold VCS can be expressed in the form of equation (2).

$$F_{VCS}(P_{ij}) = \begin{cases} [S^1, S^2, S^3, \ldots S^n] \in S_0, P_{ij} = 0 \\ \\ [S^1, S^2, S^3 \ldots . S^n] \in S_0, P_{ij} = 1 \end{cases} \qquad (2)$$

Where,

S_0 = {all the matrices obtained by permuting the columns of basis matrix B_0, which meets the requirement in Definition I}

and,

S_1 = {all the matrices obtained by permuting the columns of basis matrix B_l, which meets the requirement in Definition I}.

3.1.1 Algorithm of share generation

1. Decompose the *8* -bit image into its *8 1*-bit planes.

//a bit plane works as a binary image.

2. For each bit plane of a image, do the following:
   (i) Generate *n* shares of each bit plane by applying *(k-n)* threshold VCS for binary images.
   (ii) Stack the corresponding binary shares in bit level to achieve *n* shares

$$CSH^j\,(x,y) = BSH_1^j\,(x,y)2^{N-1} + \cdots + BSH_8^j(x,y)$$

$\boldsymbol{CSH^j}$***(x, y)***- the j^th^ share of R, G or B channel and,

$\boldsymbol{BSH_i^j}$***(x, y)*** – the jth binary share obtained from the i-th bit plane of the channel.

3.2 Digital Watermarking to Produce Meaning Shares

The meaningless shares are easy target for attackers. So these are watermarked on some cover images to generate meaningful shares. The cover images are color images that can be represented by *24* bits. The random looking shares are of grayscale that can be represented with *8* bits. Our scheme digitally watermarks these *8* bits of a pixel into the *24* bits of the cover image pixel. This can be done by replacing the *b* Least Significant Bits (LSB) of each channel (represented with *8* bits) of the *24*-bit color image.

3.2.1 Algorithm of share generation

1. Repeat for all shares
2. Repeat for each pixel of share
   (i) Generate an array S[0......8] that contain the bits of the pixel value.
   (ii) Decompose the color cover image into its three component Red, Green, and Blue and store the bits of each component into three arrays R[0...8], G[0...8], and B[0...8] respectively.
   (iii) Find that which channel can contain more information i.e. which color has less effect in the cover image.
   (iv) Replace the 2 least significant bits of rest two channels with the share pixel value and 4 least significant bits of the channel that have less effect.
3. Stop.

3.3 Extracting Original Shares and Secret Revealing Phase

Decryption phase of proposed scheme mainly consists of two sub phases:

1. Extracting original shares from the cover images.
2. Reconstruction of the secret by stacking k or more shares.

The extracting of original shares is to retrieve the 8 bit from the three channels of the cover images. Extract the same number of bits as embedded in the watermarking phase. The reconstruction of the hidden secret is done as follows:

When any $q \geq k$ of n gray shares are extracted, they are broke into their planes. The *8* bit planes of each shares is generated. Then, all the binary shares at the same bit plane are stacked. Stack operation can be implemented by conducting the OR operation using to get a revealed binary secret image.

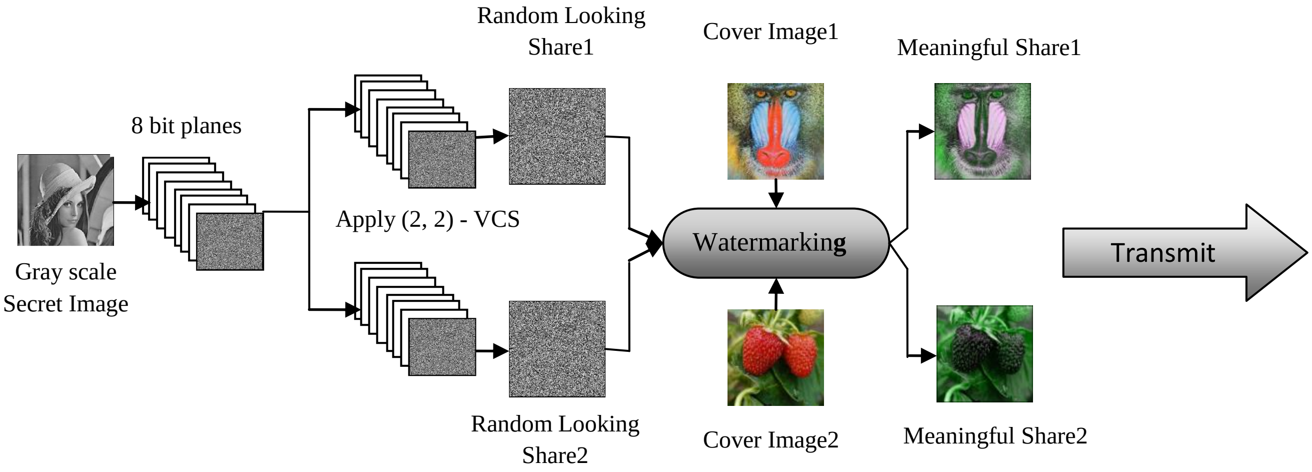


Fig 2: Flow Chart of Share Generation (Encryption) Phase

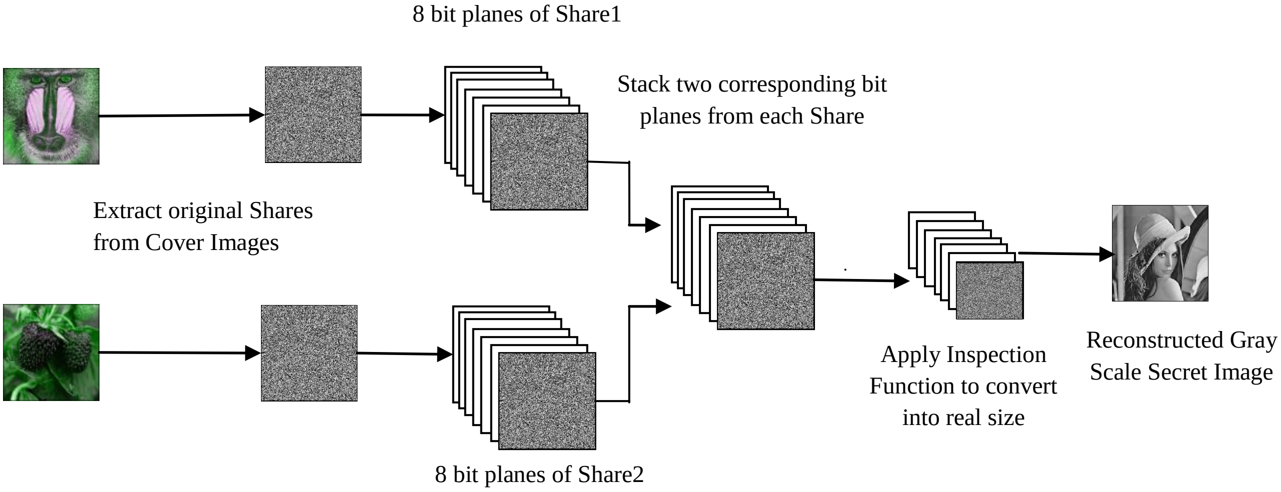


Fig 3: Flow Chart of Secret revealing (Decryption) Phase

Let $HI_b(i,j)$ is a pixel of b^{th} bit plane hidden secret at i^{th} row and j^{th} column.

```
FOR i→1: Weight
    FOR j→ Height
        FOR s→1: q
            IF (SH(i, j) == 0)
                White++;
        END;
        IF (White≥ k)
            HI_b(i,j) = 0;
        ELSE
            HI_b(i,j) = 1;
    END;
END;
```

Furthermore, the revealed binary secret image HI_b are segmented into blocks with the same size as $s^j_i(l \le i \le N, l \le j \le q)$ in the sharing phase. The i-th original secret bit plane SI_b can be recovered by inspecting the corresponding blocks in HI_b. The inspecting function is formulated in Eq.(3).

$$SI_b(i,j) = \begin{cases} 1, HB \ge d \\ 0, \text{otherwise} \end{cases} \qquad (3)$$

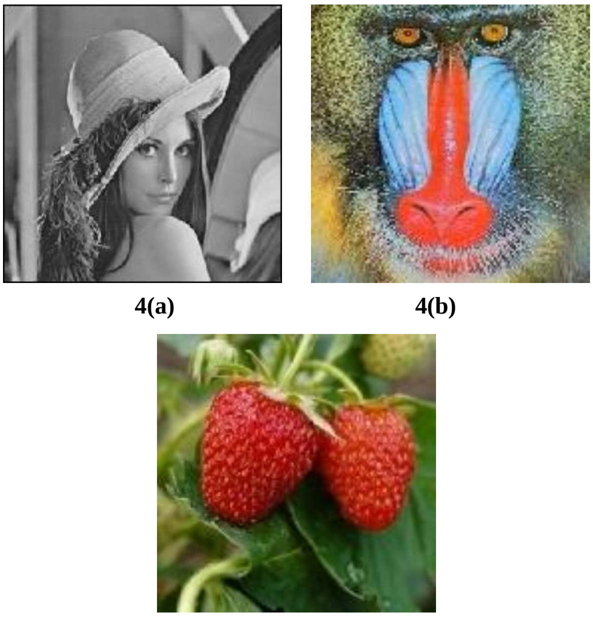
Where HB is the hamming weight of the blocks in $HI_b(i,j)$ associated to location (i,j). For example, the first block of HI_b associate with the pixel SI_b(l,l) and d is the threshold in Definition 1.

3.3.1 *Algorithm of secret revealing phase:*

1. For each received share, do the following:
    (a) Decompose the color shares into its component R, G and B channel.
    (b) Extract the original share's bits from three components.
2. Decompose each original share into its bit planes.
3. Apply "OR" to the corresponding bit planes of every share.
4. Stack the corresponding binary hidden secret in bit level to achieve grayscale secret image.

4. EXPERIMENTAL RESULTS

In this section, experimental results of proposed scheme are demonstrated. The input to the experiment are three images: a 256 × 256 pixels grayscale secret image is used to be encrypted which is shown in Figure.4 (a), and two color cover images of 512 × 512 that are used to enveloping the shares shown in Figure.4(b), and 4(c).

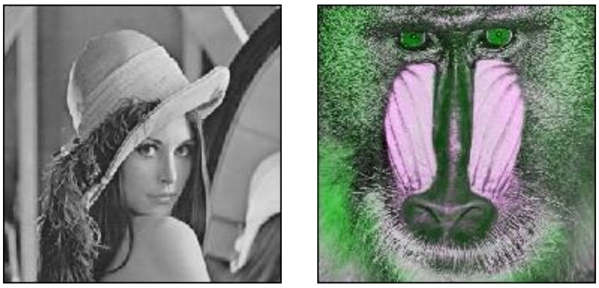


4(a) **4(b)**

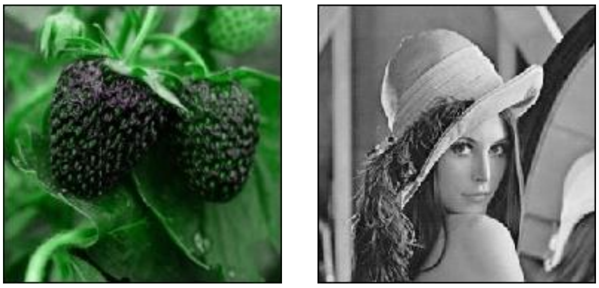
4(c)

Fig 4: Input Images, (a) Grayscale Secret Image, (b) Cover Image1, (c) Cover Image2

A (2,2)-threshold VCS and proposed digital watermarking is implemented using MATLAB R2009b in this experiment. Figure.5 (b) and 5(c) show the output shares of the proposed sharing scheme. When the two shares are collected, the secret image can be perfectly recovered shown in figure 5(d).



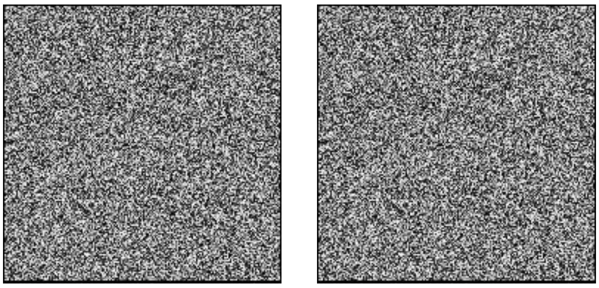
5(a) **5(b)**



5(c) **5(d)**

Fig 5: The proposed scheme using (2,2)-threshold VCS.(a)The secret image Lena,(b) share 1,(c) share 2, (d) the recovered image by stacking two shares.

Figure.6(a) and 6(b) illustrate the shares generated from Lukac and Plataniotis's scheme. Although their scheme can reconstruct ideal image but shares generated are with random-looking having a great interest of hackers.



6(a) **6(b)**

Fig 6: Random looking shares generated by Lukac and Plataniotis's scheme, (a) Share1, (b) Share2

However, the shares from the propose scheme are some meaningful images that envelop the random looking shares. Participants can easily recognize their shares and manage them in the case that a single participant has several shares.

5. CONCLUSION

A bit plane of an image is a binary image that carries visual information of original images so as to retain the original pixel values the same before and after encryption. In visual cryptography if a person gets sufficient k number of shares; the image can be easily decrypted. This paper develops an encryption method to construct grayscale VC scheme with using bit plane encoding and a simple enveloping technique where the secret shares are enveloped within apparently innocent covers of digital pictures using LSB replacement digital watermarking. This adds security to visual cryptography technique from illicit attack as it befools the hackers' eye. The meaningful shares can be easily managed and recognized by the participants.It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share. The size and contrast of the decrypted image using the propose scheme are real.

6. REFERENCES

[1] Naor, M. and Shamir A, 1995 Visual cryptography, in: A. De Santis (Ed.), Advances in Cryptology: Eurpocrypt' 94, Lecture Notes in Computer Science, vol. 95, pp. 1–12.

[2] Ateniese G., Blundo C. and Stinson D. R.,1996 Constructions and bounds for visual cryptography in

23rd International Colloquium on Automata, Languages and Programming, ser. Lecture Notes in Computer Science, F. M. auf der Heide and B. Monien, Eds., vol. 1099. Berlin: Springer-Verlag, pp. 416-428.

[3] Stinson D. R., 1997 An introduction to visual cryptography, Presented at Public Key Solutions ’97, Toronto, Canada, April 28–30.

[4] Verheul E.R., and Van Tilborg H.C.A., 1997 Constructions and properties of k out of n visual secret sharing schemes, Des. Codes Cryptogr. 11 179–196.

[5] Blundo C., Santis A. D, and Stinson D.R. 1999 On the contrast in visual Cryptography schemes Cryptology 12 261–289.

[6] Ateniese G., Blundo C., Santis A. D., and Stinson D. R. 1996 Visual Cryptography for general access structures Inf. Comput., vol. 129, no. 2, pp. 86–106.

[7] Lin C.C., and Tsai W.-H. 2003 Visual cryptography for grey-level images by dithering techniques in Pattern Recognition Lett. 24 349–358.

[8] Shyu S.J. 2006 Efficient visual secret sharing scheme for color images in Pattern Recognition 39 866–880.

[9] Wu C.C., and Chen L.H. 1998. A study on visual cryptography, Master Thesis, Institute of Computer and Information Science in National Chiao Tung University, Taiwan, R.O.C.

[10] Wu H.C., Chang C.C. 2005 Sharing visual multi-secrets using circle shares Comput. Stand. Interfaces 134 (28) 123–135.

[11] Poynton C.A. “Frequently asked questions about color”, http://www.inforamp.net/∼ poynton.

[12] Zhou Z. 2006 Halftone Visual Cryptography. In IEEE Transactions on image processing, vol.15, No.8, .

[13] Hou Y. C. 2003 Visual cryptography for color images in Pattern Recognit. , vol. 36, pp. 1619–1629.

[14] Chin-Chen Chang, Jun-Chou Chuang,Pei-Yu Lin 2005 Sharing A Secret Two Tone Image In Two Gray Level Images. In Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05).

[15] Kang I., Arce G R., Lee H. K., 2011 Color Extended Visual Cryptography Using Error Diffusion in IEEE Transactions on image processing, vol.20, No.1.

[16] Kumari K, and Bhatia S 2010 Multi-pixel Visual Cryptography for color images with Meaningful Shares in International Journal of Engineering Science and Technology vol. 2(6), 2398-2407.

[17] Mandal J K, Ghatak S 2011 Secert Image/Message Transmission through Meaningful shares using (2,2) Visual Cryptography (SITMSVC) in IEEE International Conference on Recent Trends in Information Technology, 978-1-4577-0590/11.

[18] Lukac R and Plataniotis K. 2005 Bit-level based secret sharing for image encryption in Pattern Recognition, vol. 38, no. 5, pp. 767-772.

[19] Chandramouli R, and Menon N. 2011 Analysis of LSB based image steganography Techniques In *Proc. Of ICIP*, thissaloniki, Greece, pp. 1019-1022.

[20] Nameer, N. EL-Emam 2007 Hiding a large amount of data with high security using stegnagraphy algorithm Journal of Computer science ISSN 1549-3636, vol. 3, No.4,pp. 355-372.