ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Progressive visual cryptography scheme without pixel expansion for color images

Fersna S.[1], Athira V.[2]

PG Student, Electronics and Communication Department, MBCET, Trivandrum, India [1]

Faculty, Electronics and Communication Department, MBCET, Trivandrum, India [2]

Abstract: This paper proposes a new progressive visual cryptography (PVC) scheme for color images without any pixel expansion based on the halftoning technique. PVC is a special encryption technique which can be utilized to recover the secret image gradually by superimposing more and more shares. If we only have a few pieces of shares, we could get an outline of the secret image; by increasing the number of shares being stacked, the details of the hidden information can be revealed progressively. Firstly, a chromatic image is decomposed into three monochromatic images in tones of red, blue and green. These three images are transformed into binary images by halftone technique. The secret image shares from binary images are obtained by the unexpanded VC algorithm. To prevent attack from hackers, the secret image shares are watermarked with different cover images and are transmitted. At the receiving side the cover images are extracted from the shares and stacked one by one which reveals the secret image progressively. This scheme provides a more efficient way to hide color images in different meaningful shares without any pixel expansion, providing high security and recovered images with high contrast.

Keywords: Visual Cryptography (VC), halftoning, color image, PVC, watermarking, shares, Visual Secret Sharing (VSS).

I. Introduction

In this internet era, it is an inevitable trend to digitize data to be published, transmitted, and shared on the Internet. Although the Internet is a very convenient platform, there still exist many potential problems. For example, hackers may misuse the Internet to commit computer crime, resulting in secret data being forged, modified, stolen and so on. In order to ensure the security of the data, the best way to protect the secret information is to encrypt them in advance before sharing them. Complicated calculation and complex math will be used during the encryption/decryption process in order to make sure that the secret information will not be decrypted in a limited time and with limited resources by hackers without knowing the correct keys.

Generally speaking, images, audio, and video files are usually much bigger than text files. Therefore, using complicated conventional cryptography to encrypt/decrypt them seems to be rather wasting processing time.

Visual Cryptography (VC) was first proposed by Naor and Shamir (1994) [1], which encodes a secret image into numerous meaningless share images and each of them alone does not reveal any information about the secret. Precisely, Naor and Shamir presented a concept of k-out-of-n (k, n) VSS, dividing a secret image into n shares and needing to stack at least k shares to reconstruct the original secret image. This is known as (k, n) - threshold mechanism.

Unfortunately, conventional VC-based VSS has three main drawbacks: 1) suffering from pixel expansion, 2) requires sophisticated codebook designed for applications, and 3) managing more and more meaningless shares. On the contrary, progressive visual cryptography (PVC) [6] can be utilized to more shares. Even though no one can obtain any hidden information from a single share, this type of visual cryptography technique is insecure as the shares generated are noise like (random looking) images and 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.

In this paper, a new progressive visual cryptography (PVC) scheme for color images without any pixel expansion based on the halftoning technique is proposed. The proposed scheme has the following advantages: 1) free from pixel expansion, 2) removing the need of sophisticated codebook.

II. Related Works

Naor and Shamir [1] proposed a new cryptography paradigm, called visual cryptography (VC) or visual secret sharing (VSS), which attempts to recover a secret image via the human visual system by stacking two or more transparencies. A basic 2-out-of-2 or (2, 2) VC scheme produces two share images from an original image and must stack both shares to reproduce the original image. More generally, a *(k, n)* scheme produces *n* shares, but only requires combining *k* shares to recover the secret image. To preserve the aspect ratio for the recovered secret image for a (2, 2) scheme, each pixel in the original image can be replaced in the share images by a 2×2 block of sub pixels. As shown in Fig. 2.1, if the original pixel is white, one of six combinations of share pixels is randomly created. Similarly, the possible share combinations for black pixels are also shown. After stacking the shares with white, transparent and black opaque, the original secret

DOI 10.17148/IJARCCE.2015.4641

image will be revealed. Stacking can be viewed as mathematically OR operation, where white is equivalent to 0 and black is equivalent to 1.

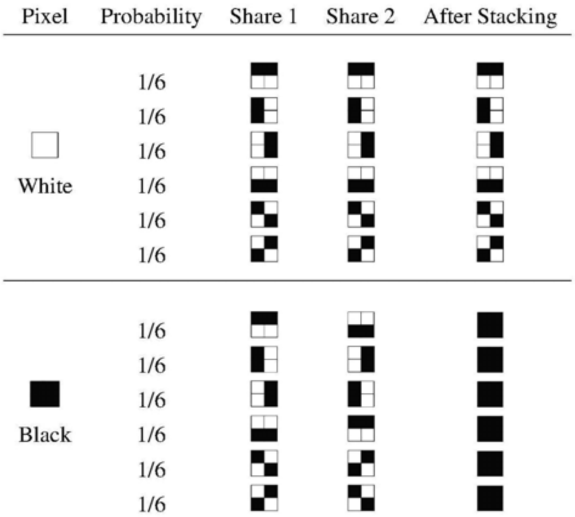


Fig. 2.1. Illustration of a (2, 2) VC scheme with 4 sub pixels.

The process is illustrated in Fig. 2.2. for a simple binary image. Note that the resulting share images and the recovered secret image contain four times as many pixels as the original image (since each pixel of the original image was mapped to 4 subpixels). It may also be noted that the recovered image has a degradation in visual quality (specifically, the contrast between white and black is decreased) since a recovered white pixel is actually comprised of 2 white and 2 black subpixels, while a black pixel is represented by 4 black subpixels in the recovered image. The conventional VC [1] applied the method of pixel expansion to create shares, which would cause a problem of wasting the storage space**.**

In the traditional visual cryptography scheme, shares are created as random patterns of pixels. These shares look like a noise. Noise-like shares arouse the attention of hackers, as hacker may suspect that some data is encrypted in these noise-like images. So it becomes prone to security related issues. It also becomes difficult to manage noise-like shares,as all share looks alike.

Nakajima M. and Yamaguchi Y., developed an Extended visual cryptography scheme (EVS) [2]. An extended visual cryptography (EVC) provides techniques to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in traditional visual cryptography.

However, the aforementioned VSS schemes are completely revealed the secret, but cannot achieve progressive image sharing. In (k, n) visual secret sharing scheme, it is not possible to recover the secret image, though one less than k shares are available. This problem is solved in the progressive visual cryptography scheme developed by D. Jin, W. Q. Yan, and M. S. Kankanhalli [3].

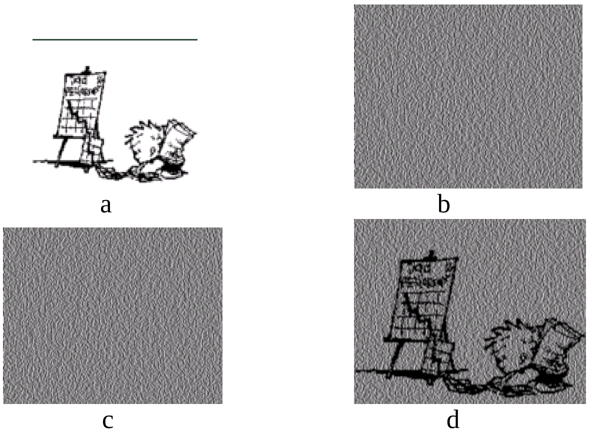


Fig. 2.2. Example of a (2, 2) VC scheme with 4 sub pixels. (a) Secret image. (b) First share. (c) Second share. (d) Reconstructed image.

In progressive visual cryptography scheme, it is not necessary to have at least k shares out of n, as in (k, n) secret sharing scheme. If more than one share obtained, it starts recovering the secret image gradually. The quality of recovered image improves, as the number of shares received increases.

In 2008, Fang [4] combines the progressive VC-based VSS [5] and the friendly VC-based VSS methods to form a new one. Unfortunately, Fang's scheme still suffers the problem of pixel expansion up to four times. Even though Young-Chang Hou and Zen-Yu Quan's PVC method [6] generates noise-like shares. i.e. The generated shares are not meaningful, which are of more interest to hackers as they treat them as critical information in the transmission. Confidential images have no means to be secured when they are transmitted over the network.

This paper proposes a watermarking scheme which overcomes the drawbacks Young-Chang Hou and Zen-Yu Quan's PVC method [6]. And also this paper deals with the color images instead of gray scale images.

III. PROPOSED METHOD

The proposed color image sharing scheme combines the progressive visual cryptography using unexpanded shares method with the digital watermarking scheme. The watermarking method provides a means to generate meaningful shares.

This scheme consists of following steps:

A. At the encryption stage:

1) Chromatic image is decomposed into three monochromatic images in tones of red, blue and green.
2) These three images are transformed into binary images by halftoning technique.
3) Creating the sharing images.
4) Cover images are superimposed on the shares.

B. At the decryption stage:

1) Original shares are extracted from the meaningful shares.
2) These shares are split up into three color channels.

DOI 10.17148/IJARCCE.2015.4641

3) Combining the same color channels to obtain gray scale images of red, blue and green.
4) Gray scale images of three channels are combined to get the colored secret image.

Firstly, a chromatic image is decomposed into three monochromatic images in tones of red, green and blue. Secondly, these three images are transformed into binary images by halftone technique.

Halftone technique is a method to display a gray image with black-and-white spots. Fig. 3.1 shows the basic principle of the halftone technique. The more black spots the image includes, the more the image will be alike the true gray image. Construct the other two binary images shown in Fig. 3.1 (c) and Fig. 3.1 (d) and Fig. 3.1 (b) is closest to the gray image.

In this paper, we use the Floyd-Steinberg Algorithm to get the halftone images. For an 8-bit grayscale image, the gray value of the image is from 0 (black) to 255 (white).

Letting b=0,
w=255,
t= int [(b+w)/2] =128.

Assuming g is the gray value of the image, which location is $P\ (x,\ y)$; e is the difference between the computed value and the correct value. Then the Floyd-Steinberg Algorithm can be described as follows:

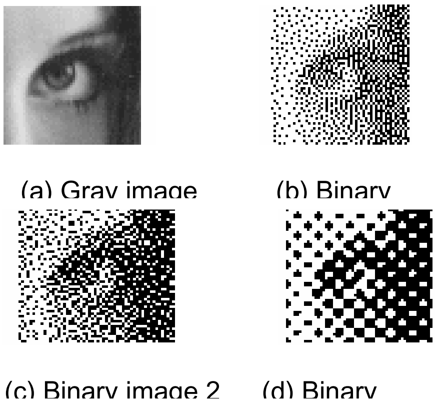

(a) Gray image (b) Binary
(c) Binary image 2 (d) Binary

Fig. 3.1. Basic principle of halftone technique

```
If      g > t then
        Print white;
        e=g-w;
        Else
        Print black;
        e=g-b;
        (3/8 × e) is added to P (x+1, y);
        (3/8 × e) is added to P (x, y+1);
        (1/4 × e) is added to P (x+1, y+1);
    End if
```

For example, a point with the gray value of 130 in an image should be gray pointed. Since the intensity of general image changes continuously, so the values of adjacent pixels is likely close to 130, and the surrounding region is also gray.

According to the Algorithm, the number 130 is bigger than 128, then a white point is printed on the new image. But 130 are away from the real white 255. While -46 (-125 multiplied by 3/8) added to adjacent pixel, the value of adjacent pixel is close to 0; the adjacent pixel comes to black. Next time, e also become positive, the adjacent pixel comes to white, so a white one after a black one, gray is demonstrated. If not transmitting the error, the pixel in the new image is white. Take another example; if the gray value of a point is 250, it should be white in gray image, and e equals to -5, it has little impact on the adjacent pixel. This certificates the correctness of the algorithm.

Then to generate n shares of secret image, Young-Chang Hou and Zen-Yu Quan's progressive VC method [6] is used. For each of the three monochromatic images, this method is used to generate n shares with the same color.

The algorithm for creating shares is explained below and then, we can choose any three different colors of which to compose them into n colored shares.

First design two $n \times n$ matrices denoted by C^0 and C^1, which represents the sharing matrix of white and black pixels of the secret image, respectively. Each row in matrix C^0 or C^1 represents a sharing method, and each column represents the value assigned to every participant (0 is for white, 1 is for black).

In matrix C^0, the first row is assigned to 1, and other rows are all 0. On the contrary, matrix C^1 is a diagonal matrix, which means 1 is assigned to the diagonal line and the rest elements are all 0. Therefore, each pixel on the shares will have only $1/n$ chance to occur as black disregarding it is dispatched from white or black pixels of the secret image.

Random numbers ranging from 1 to n are needed to create shares. To share a white pixel of the input image, we choose a random number l, and distribute the values of the l^{th} row vector of C^0 For every share, which means that the first value of the row vector $[C^0\ (l,\ 1)]$ is distributed to share 1, and the second value $[C^0\ (l,\ 2)]$ is distributed to share 2, and so on. By the same token, C^1 is applied to share a black pixel with the same sharing steps as sharing a white pixel.

The detail algorithm of the design is presented in Fig. 3.2. Then we can choose three different colors of shares and compose them to form n colored shares. The generated shares are then watermarked using a simple watermarking algorithm for each of the channels, i.e. red, blue and green channel. i.e. Each share, thus produced is then superimposed with a cover image to generate a meaningful share, which is then transmitted. The watermarking algorithm is explained in Fig. 3.3.

TABLE I: Two N×N Secret Sharing Matrices

$$C^0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n\times n} \qquad C^1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n\times n}$$

DOI 10.17148/IJARCCE.2015.4641

```
Algorithm:
Input: A W × H halftone secret image P where p (i, j) ϵ P
Output: n shares $S^m$, m=1, 2, …. ,and n
Process:
1). Generate sharing matrices $C^0$, and $C^1$
2). For each pixel p (i, j),$1 \leq i \leq W$ ,$1 \leq j \leq H$
3).   Randomly choose a value $l$, range from 1 to n
4).   For m=1, 2, and n
    4.1) If the pixel p (i, j) = 0 (white), the pixel value
            $S^m(i,j) = C^0(l,m)$
    4.2) If the pixel p (i, j) = 1 (black), the pixel value
            $S^m(i,j) = C^1(l,m)$
```

Fig. 3.2. Progressive and unexpanded VC algorithm

In the decryption phase, original shares are extracted from the meaningful shares. For each of the watermarked shares, extract the height and width values of secret image from the watermarked share pixels. For each watermarked share pixel, if the LSB of pixel is 0, set secret share pixel at 0; else as 1, likewise we get the entire black and white secret image shares. This procedure is to be carried out for each of the color channels. Then these shares are split up into three color channels and then combining the same color channels to obtain gray scale images of red, blue and green progressively. If we have only a few pieces of shares, we could get an outline of the secret image (gray scale image); by increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively. Then these gray scale images of three channels are combined to get the colored secret image.

Progressive visual cryptography with unexpanded shares solves the main problems such as the leak of secret information, pixel expansion, and bad quality of recovered images and also deals with the color image. The problem was that the method couldn't generate meaningful shares, which can be solved using watermarking the shares. The objective of this concept is to provide a more efficient way to hide natural images in different meaningful shares so that highly secure and clear recovered images with high contrast can be assured. This concept can be used for the applications such as privacy and authentication of fingerprint and face templates.

```
Algorithm:
Input: n secret image shares, n cover images
Output: n watermarked shares
Process:
1. Do for each secret image share
        a. Read respective cover image
        b. Do for each pixel
                i. If share pixel is black
                        i.a. Set LSB of cover image
                        pixel to 1
                ii. If share pixel is white
                        ii.a. Set LSB of cover image
                        pixel to 0
```

Fig. 3.3. Watermarking Algorithm

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The input image, peppers of size 512× 384 pixels, for the experiment is shown in Fig. 4.1 (a). Halftone technique is applied to obtain a halftone image as shown in Fig. 4.1 (b).

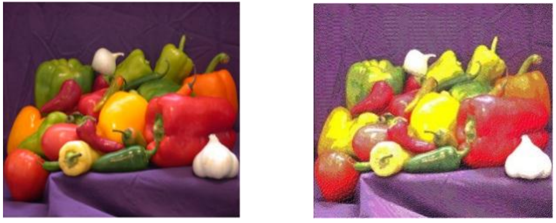


Fig. 4.1. (a) Secret image (b) Halftone image

We consider every monochromatic image as a secret image and to generate n shares of the same color of that image, Young-Chang Hou and Zen-Yu Quan's progressive VC method [6] is used and then we can choose three different colors of shares and compose them to form n colored shares. Here we are considering n=4. So each color of the halftone image is converted into 4 shares and then, we choose three different colors and combine them to form four colored shares S1, S2, S3 and S4 as shown in Fig. 4.2 (a), (b), (c) and (d).

After creating the shares, they are embedded into different cover images by LSB watermarking. The cover images and the watermarked shares are shown in Fig. 4.3 and Fig. 4.4 respectively. These watermarked shares are transmitted and in the decryption phase. Original shares are extracted from the meaningful shares. Then these shares are split up into three color channels and then combining the same color channels to obtain gray scale images of red, blue and green progressively. If there is only one share R1, there is no secret image. When two shares are stacked together, Fig. 4.5 (b) is obtained.

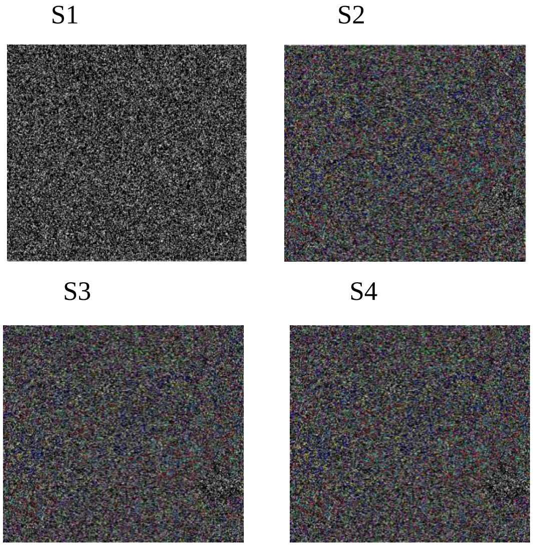


Fig. 4.2. Colored shares

Likewise, if there are four shares, we get the grayscale image of red as shown in Fig. 4.5 (d). Similarly gray scale images of green and blue is obtained progressively and is shown in Fig. 4.6 (a) and Fig. 4.6 (b) respectively. Then these gray scale images of three channels are combined to get the colored secret image and is shown in fig. 4.7.

PSNR is the peak signal-to-noise ratio in decibels (dB). The PSNR is only meaningful for data encoded in terms of bits per sample, or bits per pixel. For example, an image with 8 bits per pixel contains integers from 0 to 255.

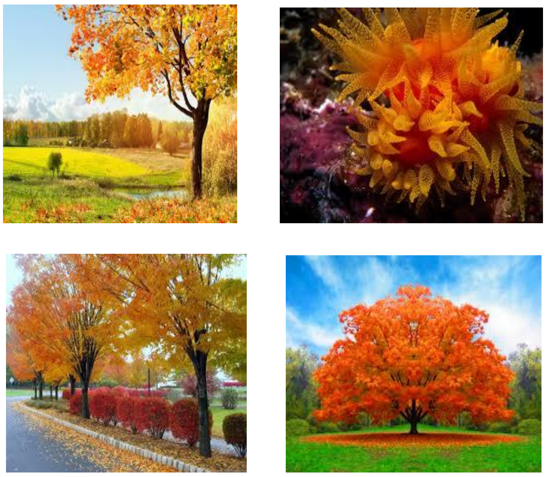


Fig. 4.3. Cover images

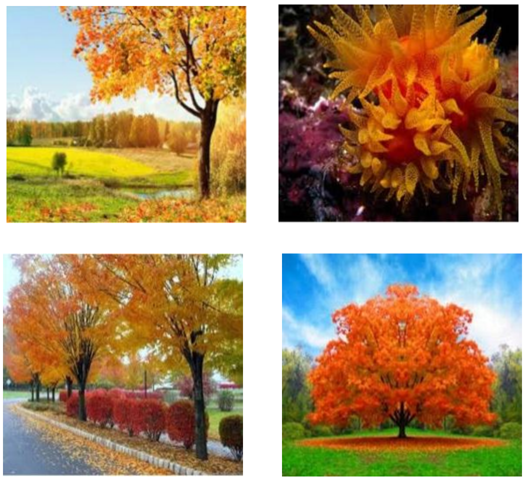


Fig. 4.4. Watermarked shares

The following equation defines the PSNR:

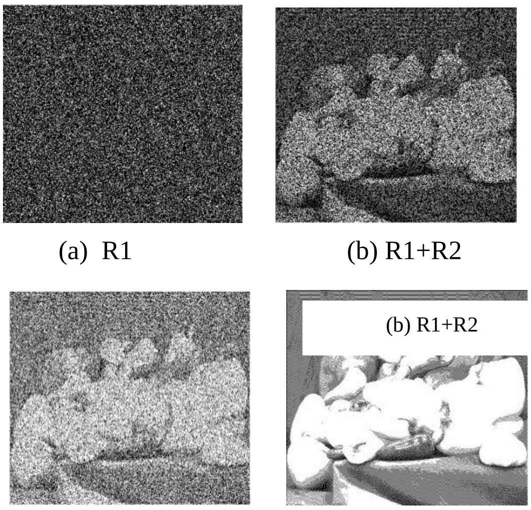
$$PSNR = 20\log_{10}\frac{2^B-1}{\sqrt{MSE}} \qquad (1)$$

where MSE represents the mean square error and B represents the bits per sample.

The mean square error (MSE) is the squared norm of the difference between the data and the approximation divided by the number of elements.
The mean square error between image, X, and an approximation, Y, is the squared norm of the difference divided by the number of elements in the image:

$$\frac{\|X-Y\|^2}{N} \qquad (2)$$

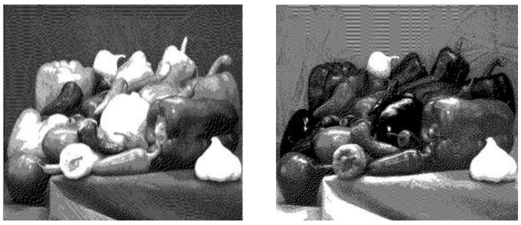
When the PSNR is calculated from halftone image and reconstructed image, we get infinity. So from this we can conclude that both the images are of the same quality and half toned image could be perfectly reconstructed at the decryption stage.



(a) R1 (b) R1+R2

(c) R1+R2+R3 (d) R1+R2+R3+R4

Fig. 4.5. Gray scale images of red.



(a) (b)

Fig. 4.6. (a) Gray scale image of green.
(b) Gray scale image of blue.

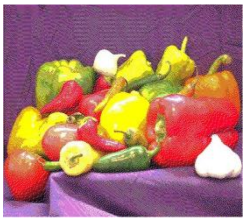


Fig. 4.7. Reconstructed image

When the PSNR is calculated from cover image and watermarked image, we get 51.1427.
After embedding the secret shares into cover image, the quality of the cover image is not much affected and visually they are identical.

V. CONCLUSION

A new progressive visual cryptography (PVC) scheme for color images without any pixel expansion based on the halftoning technique is proposed here and a watermarking algorithm is used to generate meaningful shares.

From the analysis, we can conclude that halftone image could be perfectly reconstructed at the decryption stage. And also after embedding the secret shares into cover image, the quality of the cover image is not much affected and visually they are identical.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of Mar Baselios College of Engineering and Technology in this work.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," *in Proc. Adv. Cryptol:* EUROCRYPT, Vol. 950. 1995, pp. 1–12.

[2] Nakajima M. and Yamaguchi Y., "Extended visual cryptography for natural images" *Journal of WSCG*, Vol. 10, No. 2, pp. 303310, 2002.

[3] D. Jin, W. Q. Yan, M. S. Kankanhalli, "Progressive color visual cryptography, *"Journal of Electronic Imaging,* Vol. 14, 2005, pp.033019.

[4] W. P. Fang, "Friendly progressive visual secret sharing," *Pattern Recognition,* Vol. 41, 2008, pp.1410 – 1414.

[5] W. P. Fang and J.C. Lin, "Progressive viewing and sharing of sensitive images," *Pattern Recognition and Image Analysis*, Vol. 16, No. 4, 2006, pp. 632-636.

[6] Young-Chang Hou and Zen-Yu Quan, "Progressive Visual Cryptography with Unexpanded Shares," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 21, No.11, November 2011.

[7] G. Ateniese, C. Blundo, A. D. Santis, and D. R Stinson, "Extended capabilities for visual cryptography," *Theoretical Computer Science,* Vol.250, 2001, pp.143-161.

[8] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone Visual Cryptography", *IEEE Transactions on Image Processing*, Vol. 15, Issue 8, 2006, pp. 2441-2453.

[9] D. S. Tsai, T. H. Chen, and G. Horng, "On generating meaningful shares in visual secret sharing scheme, *"The Imaging Science Journal*, Vol.56, 2008, pp. 49-55.

[10] Jithi, P.V.; Nair, A.T., "Progressive visual cryptography with watermarking for meaningful shares," *International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s),* Vol., No., pp.394, 401, 22-23 March 2013.

[11] Aarti, Harsh K. Verma and Pushpendra K. Rajput, "Ideal Contrast Secret Sharing Scheme through Meaningful Shares with Enveloping Digital Watermarking using Bit Plane based (k, n)-VCS," *International Journal of Computer Applications* (09758887) Vol. 46, No. 9, May 2012.

[12] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography,"*IEEE Trans. Image Process*., Vol. 15, No. 8, pp.2441-2453, Aug 2006.

[13] Z. M. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics, Security*, Vol. 4, No. 3, pp. 383–396, Sep. 2009.

DOI 10.17148/IJARCCE.2015.4641