Using Color Visual Cryptography Schemes and Watermarking for Sharing Black and White Secret Images

Suju R
Mtech Scholar, Department Of CSE
LBS Institute of Technology for Women
Trivandrum, India

Seena Thomas
Assistant Professor, Department Of CSE
LBS Institute of Technology for Women
Trivandrum, India

ABSTRACT
Visual cryptography is a new secure technology that distributes a secret image by separating it into a number of shares using different visual cryptography schemes (VCS). Early VCS schemes mainly focused on black-and-white secret images. Using a black & white VCS normally degrade the image quality and also suffered from a major drawback of pixel expansion, which means that the size of each secret share is several times larger than that of the original image. The black & white VCS were extended to the colour VCS. The main problem with the colour VCS is larger pixel expansion when number of colours increases. So in order to avoid these drawbacks a scheme called Black&White-Colour Visual Cryptography Scheme (B&W-C VCS) is used here. This scheme exploits the colour model to split a b & w image into coloured shares using a smaller pixel expansion and improved contrast. For any of the VCS, the main issue to be considered is authentication, i.e., there are no means by which one can ensure that the secret recovered is genuine. It would be advantageous to check the fidelity of the shares before they are used to reconstruct the secret. For this purpose, this paper proposes a watermark method to authenticate coloured shares thereby ensuring a successful secret recovery. Unlike other watermarking techniques, the pattern is not directly embedded into the share, but an authentication matrix is generated which checks the authenticity of the shares before they are used for secret recovery.

General Terms
Visual Cryptography, Watermarking, Authentication

Keywords
Secret sharing, Visual cryptography, Threshold schemes, b&w secret images, Color shares,Watermarking

1. INTRODUCTION
With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed. Visual cryptography is a technique used for protecting image based secrets.

As the name suggests, visual cryptography is related to the human visual system. When k shares are stacked together the human eyes do the decryption. Thus the beauty of the scheme is that it allows anyone to use the system without any knowledge of cryptography and without performing any computations. This is an advantage of visual cryptography over the other popular secure cryptography schemes. The mechanism is very secure and very easily implemented. Visual cryptography scheme, or vcs for short, is a special type of secret sharing that allows to share a secret image in such away that the reconstruction of the secret can be performed by the human visual system. The sharing process produces a share for each participant.

Visual cryptography was introduced by first in 1994 Noar and Shamir. For a set of n participants, a secret image S is encoded into n shares .Each participant gets one share. k out of n participants are needed to combine shares and see secret image. The secret image is known by a trusted party, called the dealer. The dealer constructs the *n* shares and distributes one share to each participant. Certain qualified subsets of participants can "visually" recover the secret image. All other sets of participants, called forbidden, have no information on the secret image. .In most cases the qualified set of participants are all the sets with at least *k* participants, while all the sets with less than *k* participants are forbidden. In such cases the schemes are called (*k*,*n*)- threshold.

The important parameters to evaluate visual cryptography schemes are: pixel expansion, m and contrast α.Pixel expansion represents the number of pixels in a share and is the most important measure of goodness of a scheme. The schemes with minimum pixel expansion are called optimal schemes. Contrast is the measure of quality of the reconstructed image. ie, it tells how much the reconstructed image differs from the original one. The relative contrast needs to be as large as possible to ensure visibility.

In Visual Cryptography, each pixel of the image is divided into smaller blocks and always has the same number of black and white (transparent) blocks. For example if a pixel is divided into two parts (2 sub pixels), there will be one white and one black blocks. Similarly if the same pixel is divided into four equal parts (4 sub pixels), there will be two white and two black blocks. Here is a simple example that explains the idea of how visual cryptography works using a Two-Out-Of-Two Scheme (4 sub pixels) .The encoding scheme is to share a binary image into two different shares Share 1 and Share 2. When dividing it into shares, pixel expansion is done. Each pixel in the original image is expanded into 4 sub pixels. The expansion can be done as 1 x 4 or 2 x 2, i.e. Each pixel can be expanded to 4 pixels, two black and two white ones[7]. The possible sub pixel expansion is shown in Figure 3.

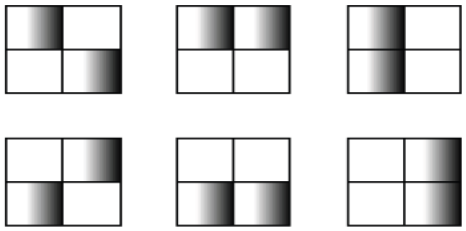


Fig 1: Possible 2 X 2 sub pixel expansion

During the generation of the shares, each pixel of the secret image is considered. If the pixel of the secret image is white, one of the two combinations of sub pixels will be chosen with a probability of 0.5 to represent the pixel in each of the shares. When these shares are placed one on top of the other, the pixel are visually OR ed and hence a white pixel looks gray (half black and half white) to the human eye. The pixels are chosen in a similar manner for the case of a black pixel. But, when the sub pixels are visually OR ed, the black sub pixels placed next to each other appear as a single black pixel. This idea can be applied to images to develop a basic Two-out-of-Two scheme by using 4 sub pixels. The 2 out of 2 visual secret sharing problem can be solved by the following collection of matrices.

C_0 = {all the matrices obtained by permuting the columns of $\begin{bmatrix}1010\\1010\end{bmatrix}$ }

Thus C_0= { $\begin{bmatrix}1010\\1010\end{bmatrix}\begin{bmatrix}0101\\0101\end{bmatrix}\begin{bmatrix}0011\\0011\end{bmatrix}\begin{bmatrix}1100\\1100\end{bmatrix}\begin{bmatrix}1001\\1001\end{bmatrix}\begin{bmatrix}0110\\0110\end{bmatrix}$ }

C_1= {all the matrices obtained by permuting the columns of $\begin{bmatrix}1010\\0101\end{bmatrix}$ }

Thus C_1= { $\begin{bmatrix}1010\\0110\end{bmatrix}\begin{bmatrix}0101\\1010\end{bmatrix}\begin{bmatrix}0011\\1100\end{bmatrix}\begin{bmatrix}1100\\0011\end{bmatrix}\begin{bmatrix}1001\\0110\end{bmatrix}\begin{bmatrix}0110\\1001\end{bmatrix}$ }

Here C_0 represents sub pixels representing a white pixels and C_1 represents sub pixels representing a black pixels. Also the number of rows represents the number of shares to be divided and number of columns represents the pixel expansion.

A major common disadvantage of b & w VCS scheme is the overall grey effect due to the left over black sub pixels from encoding. This occurred because the decoded image is not an exact reproduction, but an expansion of the original pixel with extra black pixels. Black in the original image remains black in the decoded version, but white pixels become gray. This results in the loss of contrast to the entire image. A major common disadvantage of the colored VCS scheme is that the number of colors and the number of sub pixels determine the resolution of the revealed secret image. So colored-black & white visual cryptography (CBW-VC) is proposed. Ensuring security in a cbw-vc model is a major challenge. The security of the method proposed is based on the watermarking technology, which considers the relationship of pixels selected randomly and their 8- neighbor's pixels.

2. RELATED WORKS

The related work on black-and-white VCS schemes, colored VCS schemes, EVCS schemes and digital watermarking are briefly reviewed. By reviewing these schemes, we find several commonly desirable properties which should be supported by VCS schemes.

2.1 VCS Schemes for Black-and-White Images

In this section, we firstly review Naor-Shamir black-and-white VCS [1]. They introduced the concept of VCS and proposed a general *k*-out-of-*n* threshold VCS for black and white images. Their scheme acts as the building block of other VCS schemes. We also summarize the features of several other black-and-white VCS schemes proposed after Naor-shamir's and show their merits and demerits

2.1.1 Naor-Shamir Black-and-White VCS

Naor and Shamir first proposed a (*k*, *n*)-threshold visual cryptography scheme to share a secret image [1]. In this scheme, a secret image is hidden into *n* share images for participants and can be decrypted by superimposing at least *k* share images but any *k*-1 share cannot reveal it.This scheme not only provides the frontiers of visual cryptography but also inspires researchers to develop various visual cryptography schemes for more flexible applications, various kinds of secret images, meaningful share images, and so on. The (2, 2)–VCS scheme is illustrated to introduce the basic concepts of threshold visual secret sharing schemes. To encode a secret employing a (2, 2) VC Scheme, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two or four sub-pixels. In the decryption process, two corresponding blocks are stacked together to retrieve the secret pixel. Two share blocks of a white secret pixel are the same while those of a black secret pixel are complementary as listed in Figure 2.

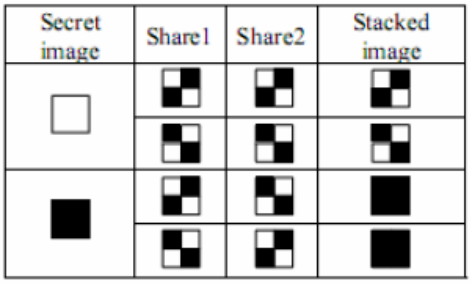
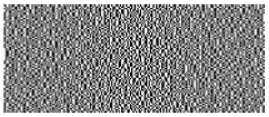


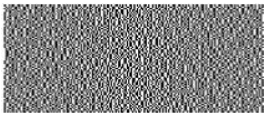
Fig 2: Sharing and Stacking scheme of Black and White Pixel

Consequently, a white secret pixel is represented by a block with the stacked result of half white sub-pixels, and a black secret pixel is all black. An example of the (2,2)–VCS scheme is shown in Figure. 3, where the share images are 2 × 2 times larger than the original secret image. The disadvantage of conventional visual cryptography schemes is that it applied for binary image only. These constructions are provably secure and the pixel expansion rate is getting larger when the values of k and n grow. Moreover, the scheme does not support images of arbitrary number of colors.

(a) Original Binary Image



(b) Share 1



(c) Share 2

(d) Decrypted Image obtained by stacking Share 1 & Share 2

Fig 3: (2,2) Visual Cryptography Scheme a)Original Binary Image; b)Share1; c)Share2; d) Decrypted Image obtained by stacking Share 1 & Share 2

2.1.2 Other Black-and-White VCS Schemes

Since the introduction of VCS, there have been many other schemes proposed. In 2003, by removing the same column which appears in both Basic Matrices, Blundo et al. [8] proposed VCS schemes with optimal contrast. In [8], they improved the contrast of (n - 1)-out-of-n (where n > 3) and 3-out-of-n schemes. They also conjectured that the k-out-of-n scheme, where k=4 or 5, had an optimal contrast. In 2004, Adhikari et al. [7] proposed a VCS which achieved a better result from the pixel expansion's point of view than [1]. They compared Naor-Shamir k-out-of-n VCS scheme with the k-out-of-n VCS scheme obtained from their method and showed that their pixel expansion was less in almost all cases. In [13], Yang proposed another one which achieved no pixel expansion by using the frequency of white pixels to show the contrast of the recovered image. Yang's scheme can be easily implemented on the black-and-white VCS with pixel expansion. All the above schemes only support black-and-white images.

2.2 VCS Schemes for Color Images

The secret images are not only limited to black and white binary images, but extended to the color images also. Verheul and Tilborg firstly provided a visual cryptography scheme for images with c colors in 1997 [10].They proposed a general construction for colored (k,n) threshold VCS.For a C-color image, each pixel is expanded to C subpixels on two images.For each subpixel, it is divided into C regions. One fixed region for one color. If the subpixel is assigned color C_1 , only the region belonged to C_1 will have the color, other regions are left black. The pixel expansion of the scheme is $c*3$. The main disadvantage of this scheme is that the number of colors and sub-pixels determine the quality of recovered secret image. If the number of colors is large, the pixel expansion is very serious and the contrast is low. In order to solve this problem, a colored VCS scheme was proposed in 2005, which only supports 2-out-of-2 threshold setting and have pixel expansion. Another colored VCS scheme proposed in 2006 applies any k-out-of-n black-and-white VCS on decomposed images of the original secret image so that it supports the general k-outof-n threshold setting. The scheme has less pixel expansion compared with previous ones while it has relatively good quality of superimposed image. Hou and Tu's colored VCS supports k-out-of-n threshold setting with no pixel expansion. Dithering is required for preprocessing the original image before secret sharing and the number of colors supported is fixed on 8.In the scheme, the number of colors of a secret image is without any limitation, and the expansion of shares only depends on the choice of black-and-white VCS. Although the scheme achieves the target of no pixel expansion, but it is only applicable to (2, 2) threshold visual cryptography scheme, and then it cannot be extended to the (k, n) threshold visual cryptography scheme. After, Wang presents two approaches to construct the (2, n)-VCS for color image while one approach uses halftone technology and the other uses bit level processing. The proposed scheme have low computational complexity and almost ideal contrast. Cimato et al.'s scheme [5], at the cost of large pixel expansion, solves the problem that superimposing many pixels of the same color results in a dark version of the color.

2.3 Extended Visual Cryptography Schemes

A k-out-of-n EVCS is an extension of the k-out-of-n VCS. It encodes n independently chosen meaningful images into n meaningful shares so that by superimposing any k or more shares, the original secret image, which is embedded in these shares, will be recovered.Any k-1 or less shares are with no trace of the secret image. An example of a 2-out-of-2 EVCS is shown in. Figure. 4.

Fig 4: The Black-and-White Meaningful Images: Sailboat and Peppers

Fig 5: Two Shares and Their Superimposed Image

Figure 4 shows the two meaningful images (Sailboatand Peppers) which are to be used for embedding secret shares of Lena .Figure 5 shows the two shares and the superimposed image by applying Ateniese et al.'s 2-out-of-2 EVCS scheme [6]. Each share carries a meaningful image. From any one of the shares, no information about the secret image is revealed. The secret image can be recovered only by superimposing the shares.

2.4 Digital Watermarking

Practical uses for visual cryptography come in the form of digital watermarking. Hwang [3] created the first and typical idea for a digital image copyright protection based on the visual cryptography. The method use a simple (2, 2) visual threshold scheme defined by Naor-Shamir [1]. Referring to Hwang's algorithm, the owner must select h × n black/white image as his/her watermark pattern P and a key S which must be kept securely. Then, verification information V is generated from the original k × 1 image M and the watermark pattern P using the key S; as follows:

1) Use S (the secret key) as the seed to generate h x n different random numbers over the interval [0, k × 1]. (Ri represents the i-th random number).

2) Assign the i-th pair (vi_1, vi_2) of the verification information V based on the following Table 1:

Collect all the (vi_1, vi_2) pairs to construct the verification information V. This verification information must be kept by neutral organization. When the owner of an image M wants to claim the ownership of an image M' as a copy of the original image M, the owner has to provide the secret key S, and the watermark pattern P is restored using the image M' and verification information V as follows:

1) Use S as a seed to generate h × n different random numbers over the interval [0, k × 1]. (Ri represents the i-th random number).

2) Assign the color of the i-th pixel of the watermark pattern P' based on the image M' as follows:

Get the left-most bit, b, of the Ri-th pixel of image M', and if b is 1 then, assign fi = (1, 0); otherwise assign fi = (0, 1).

If fi is equal to i-th pair of V then assigns the color of the i-th pixel of P' to be white; otherwise, assign it to be black.

3) If P' can be recognized as P through the human, the neutral organization shall adjudge that the image M' is a copy of M.

Table 1.The rules to assign the values of verification information

The color of the i-th pixel in watermark pattern is	The left most bit of the Ri-th pixel of Image M is	Assign the i-th pair, (vi1, vi2), of *verification information V* to be
Black	"1"	(0,1)
Black	"0"	(1,0)
White	"1"	(1,0)
White	"0"	(0,1)

This method and also the other related methods are strongly related to the values of the most significant bits of pixels selected randomly from the original digital image; therefore, if the most significant bit to some pixels selected randomly has been changed, the modified image M' will fail to retrieve the watermark pattern P successfully. Also, since the method does not consider the relationship between pixels and its neighbors, the watermark pattern would not be retrieved, if part of image has been cropped. The watermark pattern P might be restored successfully, despite the image X is not the same as the image M.

3. PROPOSED METHOD

In order to overcome the shortcomings of both the black & white and the colour VCS, the Black&White-Colour Visual Cryptography Scheme (B&W-C VCS) is used here. A major common problem with the black& white VCS scheme is the overall grey effect due to the left over black sub pixels from encoding. The extra black sub pixels causes the image to become distorted. This results in loss of contrast to entire image. In a color VCS, the number of colors and the number of subpixels determine the resolution of the revealed secret image; which is its major drawback. If the number of colors is large, the pixel expansion is very serious and the contrast is low. The B&W-C VCS generates color shares, from a black & white image, which when superimposed gives a perfect black secret within a color background, thereby improving the contrast.

VC provides a way to share secrets and this secret is in the form of an image which is encoded into a number of shares. Here, a main question that arises is how is it possible to know whether the secret that is being shared is genuine. Therefore it would be advantageous to check the fidelity of all shares before they are used to reconstruct the secret image. This prevents a secret sharing participant from incidental or intentional provision of false share data, causing unsuccessful secret recovery. Many methods attempt to provide authentication via a set of additional shares, which are used to check the authenticity. These methods do have an advantage of using an additional share for verification purpose, but using an additional share is rather cumbersome and impractical. One way to include such an authentication capacity in the secret sharing scheme is to use an authentication logo. This paper attempts to authenticate the shares by generating authentication information. This way no additional share is required and also the authentication information is got from some random positions in the original image based on a secret key.

In the proposed authentication method, firstly the secret image is divided into two shares using (2,2) B&W-C secret sharing visual cryptography scheme such that both the shares are needed to reconstruct the encrypted image. The authentication logo is then embedded into the shares generated. Unlike any other authentication methods the logo is not embedded into the shares directly, but an authentication information is generated which is used to verify the share authenticity during decryption. Both the shares generated are taken and verification is performed. The secret image is produced if share authentication is successful. The authentication method proposed is divided into two phases: the visual cryptography encryption and visual cryptography decryption.

3.1 Visual cryptography Encryption

Visual cryptography encryption consists of generation of shares using any visual cryptography schemes. Figure 6 shows the encryption process. In Black&White-Colour (B&W-C) Visual Cryptography Scheme, the secret image consists of black and white pixels, the shares constructed are color and the reconstructed secret is black within a color background. To deal with colored pixels, the RGB color model is used .Color is represented as a triple (x,y,z), with $0 \leq x,y,z \leq L$,for a fixed threshold L, where x, y and z are respectively the amount of red, green and blue light present in the color. When two color pixels $c_1=(x_1,y_1,z_1)$ and $c_2=(x_2, y_2, z_2)$ are superimposed the resulting color is a function of the two color pixels. The resulting color is given by the following operator *add*: [2]

$$add\ (c_1,c_2)= \left(int\left(\frac{x1x2}{L}\right), int\left(\frac{y1y2}{L}\right), int\left(\frac{z1z2}{L}\right)\right)$$

where int function approximates its arguments to the nearest integer. Operator *add* defines the "color superposition". The *add* operation can be extended to any number of colors. The *add* operation is commutative and thus the order in which we superpose the colors is irrelevant [5].

For L=1, $add(c_1,c_2)=(x_1x_2, y_1y_2, z_1z_2)$

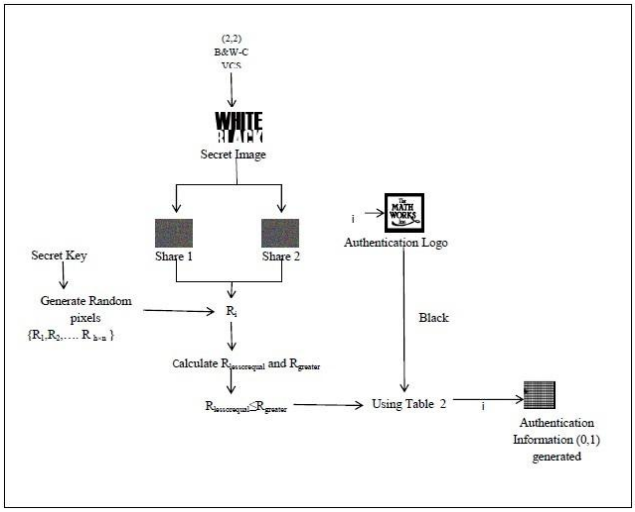


Fig 6: Visual Cryptography Encryption

3.1.1 Share Generation using B&W-C VCS

During encryption, pixels in the secret image is scanned. The B&W-C VCS is described by two collections C_W and C_K of $n \times m$ matrices with elements in *Cal*, where C_W and C_K represents the collection matrices for white and black respectively; *Cal* is the universe of all colors.ie, *Cal* = {(x,y,z)|0<x,y,z<1}. Each pixel is an element of *Cal*. A matrix *D* in one of such collections is called a distribution matrix. A distribution matrix is just a representation of the pixels in the shares: each row corresponds to a share and the *m* elements of the row provide the colors of the *m* pixels into which the secret pixel has to be expanded. The *m* pixels in a row are called "subpixels" because, taken together, they represent the secret pixel in a share. The superposition operation is given by the add of the rows corresponding to the shares. For example, below is a matrix *B* with full intensity colors and the resulting add (*B*):

$$B=\begin{bmatrix}(0.7,0.3,1) & (0.5,1,1) & (0,0.3,0.6)\\ (1,0.1,0.1) & (0.8,0.6,0.6) & (0,1,0)\\ (0.5,0.4,1) & (1,0.5,1) & (0.8,0.8,0)\end{bmatrix}$$

add (B) = (0.35,0.2,0.1) (0.4,0.3,0.6) (0,0.24,0)

Fig 7: Example for add (B)

The threshold scheme being used is the (2,2) threshold scheme. There are several ways to implement a (2,2)-threshold B&W-C VCS. Here, the 3 colors R, G and B are used. In the Scheme (2,2)-RGB, the following collections of distribution matrices describe a (2,2)-threshold B&W-C VCS with a shares palette equal to {R,G,B} and pixel expansion m=1.

$$C_W = \{\begin{bmatrix}R\\R\end{bmatrix},\begin{bmatrix}G\\G\end{bmatrix},\begin{bmatrix}B\\B\end{bmatrix}\}$$

$$C_K = \{\begin{bmatrix}R\\G\end{bmatrix},\begin{bmatrix}G\\R\end{bmatrix},\begin{bmatrix}R\\B\end{bmatrix},\begin{bmatrix}B\\R\end{bmatrix},\begin{bmatrix}G\\B\end{bmatrix},\begin{bmatrix}B\\G\end{bmatrix}\}$$

Here, when we reconstruct a black pixel we obtain a black pixel, while when we reconstruct a white pixel we obtain either R, G or B.The scheme is used in the following ways: if the secret pixel is white (resp.black), then the dealer randomly chooses one of the matrices in C_W (resp.C_K) and uses it as the distribution matrix. The matrices C_W and C_K should satisfy the following two properties:

The security property guarantees that forbidden sets of participants have no information about which collection has been used to encode the pixel because with the information provided by the shares, any of the collections is equally likely to have been used to encode the pixel. The contrast property guarantees that the reconstructed image is visible. The contrast property requires that in the reconstruction of a white pixel the number of black sub pixels is sufficiently small, whereas in the reconstruction of a black pixel the number of black sub pixels is sufficiently large. The contrast property makes the following characterization for the reconstructed pixels: a black sub-pixel contributes to the interpretation of the reconstructed pixel as black and any non-black subpixel contributes to the interpretation of the reconstructed pixel as white. That is, the only distinction made on reconstructed (sub) pixels is black and non-black. This fact, together with the observation that one can get black only by having color components equal to 0, suggests that one can use only full intensity colors. The use of full intensity colors helps to attain optimal contrast. The scheme makes use of full intensity colors. The only distinction made on reconstructed (sub) pixels is black and non-black. Let c=(x,y,z) be a color. The make-full transformation produces c= (x',y',z')= make-full(c) as follows:

$$x'=\begin{cases}0 \; if \; x=0\\ 1 \; if \; x>0\end{cases} \quad y'=\begin{cases}0 \; if \; y=0\\ 1 \; if \; y>0\end{cases} \quad z'=\begin{cases}0 \; if \; z=0\\ 1 \; if \; z>0\end{cases}$$

that is, any non-zero component is changed to 1. A color component of the superposition goes to 0 only when superposing a pixel that has 0 for that component. So the actual value of a non-zero component does not matter.Let B' = make_full (B). Thus

$$B'=\begin{bmatrix}(1,1,1) & (1,1,1) & (0,1,1)\\ (1,1,1) & (1,1,1) & (0,1,0)\\ (1,1,1) & (1,1,1) & (1,1,0)\end{bmatrix}$$

add (B')= (1,1,1) (1,1,1) (0,1,0)

Fig 8 Example: make-full transformation operation

3.1.2 Generating Authentication Information

This is the second step in encryption which generates the authentication information. The method uses the relationship between 8-neighbours pixels of a pixel *P(x,y)* as a base for generating the authentication information. Suppose the black & white secret image, *I* and the colour share *H* be of size $k \times l$ and let the Authentication Logo, *L* which is also black & white image of size $h \times n$. The authentication information is generated using the following steps:

Step Generating-1: Select number S randomly as the secret key of the share *H*

Step Generating -2: Use S as the seed to generate $h \times n$ different random numbers R over the interval [0, k × 1]. (R_i denotes the i-th random number)

Step Generating -3: Calculate the number of Ri-th pixel's neighbours pixels from its 8-nieghbours pixels that are less than or equal to the Ri-th pixel, this number is represented as $R_{lessorequal}$. Also, calculate the number of Ri-th pixel's nieghbour pixels from its 8-nieghbour pixels that are greater than Ri-th pixel, this number is represented as $R_{greater}$.

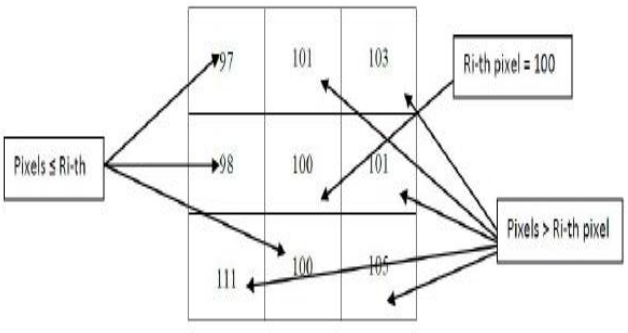


Fig 9 Example of Ri-th pixel's neighbors

Step Generating -4: Find the i-th pair (a_{i1}, a_{i2}) of the authentication information A based on Table 2.

Table 2. Rules to assign the value of Authentication information A

Colour of the i-th pixel *authentication* in the authentication logo L is	Relation between $R_{lessorequal}$ and $R_{greater}$	Assign the i-th pair,(ai1,ai2),of the *information A* to be
Black	$R_{lessorequal} \leq R_{greater}$	(0,1)
White	$R_{lessorequal} \leq R_{greater}$	(1,0)
Black	$R_{lessorequal} > R_{greater}$	(1,0)
White	$R_{lessorequal} > R_{greater}$	(0,1)

Step Generating -5: Assemble all the (a_{i1}, a_{i2}) pairs to create the authentication information A. The authentication information A generated from Step Generating -5 must be given to a trusted authority. The sender has to provide the secret key S to the trusted authority to generate the authentication information to verify the shares.

3.2 Visual Cryptography Decryption

It would be advantageous to check the fidelity of all shares before they are used to reconstruct the secret image. This prevents a secret sharing participant from incidental or intentional provision of false share data, causing unsuccessful secret recovery. The Verification steps can be concluded directly from Table 2 which displays the rules to assign the value of verification information. In this phase color shares obtained are verified. The secret will not be revealed unless the verification steps are performed. Figure 10 shows the decryption process:

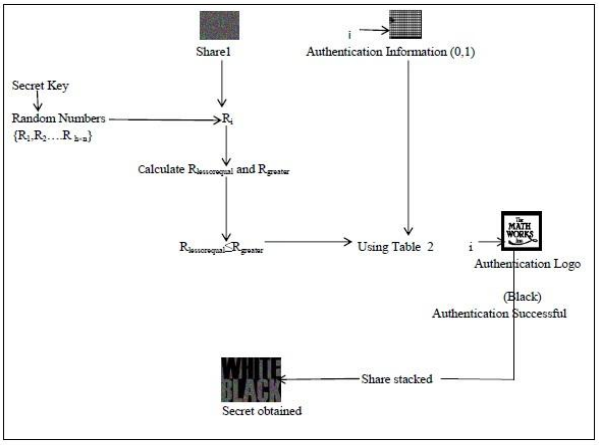


Fig 10: Visual Cryptography Decryption

The verification steps are as follows:

Step Verification-1: Use S as the seed to generate $h \times n$ different random numbers over the interval [0, k × 1].

Step Verification-2: Assign the color of the i-th pixel of the authentication logo *L* based on the share H' as follows:

If ($R_{lessorequal} \leq R_{greater}$) **AND** (the i-th pair, (a_{i1}, a_{i2}), of authentication information A = (0,1)) **then**

Assign the color of the i-th pixel of L ' to be Black

Else If ($R_{lessorequal} \leq R_{greater}$) **AND** (the i-th pair, (a_{i1}, a_{i2}), of authentication information A= (1,0)) **then**

Assign the color of the i-th pixel of L' to be White

Else If ($R_{lessorequal} > R_{greater}$) **AND** (the i-th pair, (a_{i1}, a_{i2}), of authentication information A= (1,0)) **then**

Assign the color of the i-th pixel of L ' to be Black

Else If ($R_{lessorequal} > R_{greater}$) **AND** (the i-th pair, (a_{i1}, a_{i2}), of authentication information A= (0,1)) **then**

Assign the color of the i-th pixel of L ' to be White

Step Verification-3: If the authentication information can be retrieved, the authentication logo can be successfully extracted proving that the shares are authenticated. Once the logo is extracted the shares are overlapped revealing the secret image. Thus the result of this phase will be the secret image.

4. EXPERIMENTAL RESULTS

The proposed scheme is studied using MATLAB 12. Both the secret image and the authentication logo are black and white images as shown in Figure 11 .The color shares are constructed using the B&W-C VCS and is shown in Figure 12.

Fig 11: Secret Image and Authentication Logo

Fig 12: Constructed Shares 1&2

The authentication logo is not embedded directly into the secret image, but is used to generate the authentication information. The secret image is reconstructed, as in Figure 13, if the authentication is successful. This is made possible only by knowing the secret key. Thus, at no point of time, the authentication logo is passed in the transmission channel, thereby providing maximum security.

Fig 13: Reconstructed Secret after authentication

The proposed method is tested against noise attacks for different levels of noise density. The noise density is selected as 0,0.25,0.75.The results for applying the noise attacks on at least one share and on both the shares are shown in Tables 3 & 4.

Table 3. Comparison of Reconstructed Secret when at least one Share is modified

Noise Density	Share 1	Share 2	Reconstructed Secret
0			
0.25			
0.5			
0.75			

Table 3 shows the case when atleast one of the share is modified by an attacker. As the density of noise increases, degradation is noticed in the quality of reconstructed secret. This means that a change in any one of the shares also leads to a authentication failure.

Table 4. Comparison of Reconstructed Secret when both Shares are modified

Noise Density	Share 1	Share 2	Reconstructed Secret
0			
0.25			
0.5			
0.75			

Table 4 shows the case when both the shares are modified by an attacker. The degradation in the quality of reconstructed secret can be noticed when both the shares have a noise density of 0.75.Thus it can be seen that, any change in the share will cause change of the authentication information and authentication fails thus avoiding a false secret recovery. As noticed, the proposed method can withstand noise attacks.

5. CONCLUSION AND FUTURE WORK

Visual cryptography is the current area of research where lot of scope exists. Currently this particular cryptographic technique is being used by several countries for secret transfer of hand written documents, financial documents, text images, internet voting etc. There are various innovative ideas and extensions for the visual cryptographic models introduced till now. Allowing the shares to be color images ,using the Black&White-Color (B&W-C) visual cryptography scheme provides a smaller pixel expansion (compared to the schemes that one can obtain using only black and white shares). When shares are superimposed there is no guarantee that the secret which appears is same as the one which was shared. In order to check the fidelity of all shares before they are used to reconstruct the secret image, an authentication method is used. The main characteristic of the proposed method is that the authentication logo does not have to be directly embedded into the shares, but authentication information is generated to check the fidelity of the shares.

During decryption, it would always be hard to detect the pixel values in authentication logo without secret key which is kept secretly by the owner. Also the logo can never be retrieved unless the retriever has the secret key and the authentication information simultaneously. The proposed method achieves effective share creation, stacking of shares and maximum share authentication. The future work can be extended for providing authentication during a multisecret transmission.

6. ACKNOWLEDGMENTS

I am greatly indebted to **Dr. K.C Raveendranathan**, *Principal, LBS Institute Of Technology For Women* and **Dr. Shreelekshmi R**, *Head of Department, Dept. of Computer Science & Engineering*, for providing all the required resources for the successful completion of the seminar. I would like to sincerely thank my guide**, Mrs Seena Thomas**, *Assistant Professor, Dept. of Computer Science & Engineering* for her valuable suggestions and guidance in the preparation of the seminar report. I would like to express my sincere gratitude to all teachers of computer science department for their moral and technical support throughout the course of this seminar

7. REFERENCES

[1] M. Naor, A. Shamir," Visual cryptography", in: EUROCRYPT'94, LNCS, vol. 950, Springer-Verlag, 1995,pp. 1–12

[2] R. De Prisco and A. De Santis, "Color Visual Cryptography Schemes for Black and White Secret Images", *Theoretical Computer Science*, vol. *510, Elsevier, 28 October 2013, pp. 63-86.*

[3] R.-H. Hwang, "A Digital Image Copyright Protection Scheme Based on Visual cryptography," *Tamkang Journal of science and Engineering*, Vol. 3, No. 2, 2002, pp. 97-106.

[4] Adel Hammad Abusitta " A Visual Cryptography Based Digital Image Copyright Protection" *J. Information Security*, 2012,vol. 3, 96-104

[5] S. Cimato, R. D. Prisco, and A. D. Santis, "Colored visual cryptography without color darkening",*Theoretical Computer Science, Elsevier, 374:261–276, 2007.*

[6] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson,"Visual cryptography for general access structures",*Inf. Comput., Elsevier ,129(2):86–106, 1996*.

[7] A. Adhikari, T. K. Dutta, and B. Roy,"A new black and white visual cryptographic scheme for general access structures", *In Progress in Cryptology – INDOCRYPT2004, pages 399–413, 2004. Lecture Notes in Computer Science, Vol. 3348.*

[8] C. Blundo and A. D. Santis,"Visual cryptography schemes with perfect reconstruction of black pixels", *Computers and Graphics, Elsevier, 22(4):449–455, August 1998*.

[9] P. A. Eisen and D. R. Stinson ,"Threshold visual cryptography schemes with specifiedwhiteness levels of reconstructed pixels",*Des. Codes Cryptography, Elsevier, 25(1):15–61, 2002.*

[10] E. Verheul and H. van Tilborg ,"Construction and properties of k out of n visual secret sharing schemes", *Designs Codes Cryptogr, Elsevier, (11):179–196, 1997.*

[11] Y. C. Hou and S. F. Tu.,"A visual cryptographic technique for chromatic images using multi-pixel encoding method", *Journal of Research and Practice in Information Technology, 37(2):179–191, May 2005.*

[12] J.Weir and W.Q .Yan, "Sharing Multiple Secrets Using Visual Cryptography", *Proceedings of the IEEE International Symposium on Circuits and Systems*, Taipei,24-27 May 2009,pp.509-512 .

[13] C.N.Yang, C.A.Laih, "New colored visual secret sharing schemes", *Des. Codes Cryptogr., Elsevier* ,20 (2000)325-335

[14] Mahmoud A Hassan and Mohammed A Khalili, "Self Watermarking based on Visual Cryptography", *Proceedings of World Academy of Science, Engineering and Technology* 8:159-162, October 2005.

[15] Young-Chang Hou and Pei-Min Chen, "An Asymmetric Watermarking Scheme based on Visual Cryptography", *WCCC-ICSP 5th International Conference on Signal Processing Proceedings*, 2:992-995, 2000