A Survey on Embedded Halftoned Shares in Extended Visual Cryptography Schemes

Amit Chaturvedi, Ph.D
Head, MCA Deptt.
Govt. Engineering College, Ajmer

V.Rama Kanth
Assistant Professor,
Krishna Murhty Institute of Technology and Engineering, Hyderabad.

Abstract
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 was introduced in 1994 Noar and Shamir [1]. With the rapid development of the network technology, multimedia information is transmitted over the Internet conveniently. 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 multimedia images, various image secret sharing schemes have been developed. In this paper, we have proposed a technique of well known secret sharing on both black and white and color images.

Key Words
Visual cryptography scheme (VCS), pixel expansion, contrast, security, accuracy, computational complexity, Secret, Share, Halftoning

1. INTRODUCTION
Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Naor and Shamir in 1994 proposed a new security technique named visual cryptography scheme [1]. In this technique, a secret image of type binary is encoded in a cryptographically manner into random binary patterns which contains n shares in a k-out-of-n scheme. The n shares are distributed among n participants in such a way the each participant's share is not known to another participant. The secret image can be visually revealed by k or more participants by joining all the shares available. Even if computational power decoding is available, cannot be done on the secret image by k-1 or fewer participants. Cryptography is the detailed study of mathematical techniques related aspects of Information Security such as confidentiality, data security, entity authentication and data origin authentication. It is one of the techniques [2] which act as the means of providing information security. Security has become an important aspect as Information technology is dominating the world now.

Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows Visual information (pictures, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system without the Involvement of any complex cryptographic algorithms.

The technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies [3]. In this paper we provide an overview of the emerging Visual Cryptography (VC) and related security research work done in this area. Visual cryptography scheme is a cryptographic technique which allows visual information to be encrypted in such a way that the decryption can be performed by the human visual system without the need of computers.

There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images(either binary or color) and a number of secret images(either single or multiple) encrypted by the scheme. Intent of this paper is on study and performance analysis of the Visual cryptography schemes on the basis of pixel expansion, number of secret images, image format and type of shares generated.

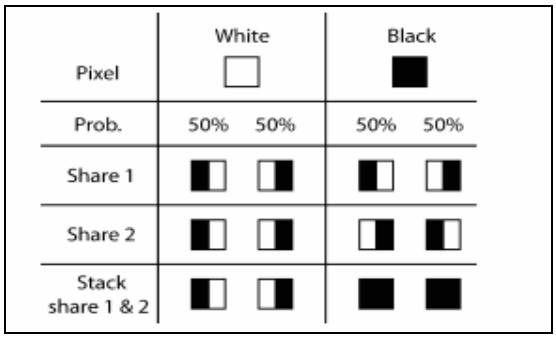

Fig 1: Construction of (2, 2) VC Scheme

Even with the remarkable advance of computer technology, using a computer to decrypt secrets is infeasible in some situations. For example, a security guard checks the badge of an employee or a secret agent recovers an urgent secret at some place where no electronic devices are applied. In these situations the human visual system is one of the most convenient and reliable tools to do checking and secret recovery. Visual cryptography (VC), [6] [9] [14] proposed by Naor and Shamir is a method for protecting image-based secrets that has a computation-free decryption process. In the (2, 2) VC scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed in transparencies. The decryption

process is performed by stacking the two shares and the secret image can be visualized by naked eye without any complex cryptographic computations [7] [19]. In the above basic VC scheme each pixel 'p' of the secret image is encrypted into a pair of sub pixels in each of the two shares. If 'p' is white, one of the two columns under the white pixel in Fig. 1 is selected. If p is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly such that each column has 50% probability to be chosen. Then the first two pairs of sub pixels in the selected column are assigned to share 1 and share 2, respectively. Since, in each share, p is encrypted into a black–white or white–black pair of sub pixels, an individual share gives no clue about the secret image. By stacking the two shares as shown in the last row of Fig. 1, if 'p' is white it always outputs one black and one white sub pixel, irrespective of which column of the sub pixel pairs is chosen during encryption. If 'p' is black, it outputs two black sub pixels. Hence there is a contrast loss in the reconstructed image. However the decrypted image is visible to naked eye since human visual system averages their individual black–white combinations. The important parameters of this scheme are

- Contrast 'α', which is the relative difference between black and white pixels in the reconstructed image. This implies the quality of the reconstructed image.
- Pixel expansion 'm', which refers to the number of pixels in a share used to encrypt a pixel of the secret image. This implies loss of resolution in the reconstructed image.

2. Visual Cryptography Scheme for Secret Hiding

Using Visual cryptography, image is encrypted in such a way that no one apart from the sender and intended recipient even realize the original image, this is a form of security through obscurity [3]. Cryptography hides the secret image in other images, but it does not reveal the fact that it is not the actual image to others besides the sender and the recipient. Based on cryptography, 'n' images are encoded and only the human naked eye can decrypt the hidden message without any cryptographic computations. This is achieved when encrypted image shares are stacked one over other using Visual Cryptography. An improved algorithm based on Chang's and Yu visual cryptography scheme is proposed to hide a colored image in the form of multiple colored cover images by computing F (ki, Ґp). As 'I' image encrypted into 'k' number of shares and the function denotes each share by ki and Ґp is to perform the image shared operation [8] [17]. Original image is encrypted into shares, and the shares are also layered one after another to reveal secret image. Using 'S' matrix and the shares we form original image without computation. This mechanism or approach results loss less recovery and the noise reduction techniques are efficient enough in covering the images without adding any computational complexity. This is the basic principle, which is developed for further improvement of visual cryptography schemes.

3. VCS and Halftoning Technique

In this section the conventional VCS and Half toning technique are described before presenting the proposed scheme in the next section [13] [17]. In traditional VCS the participants of secret sharing scheme are represented as V = {0, 1, 2… n-1). The qualified and forbidden subsets are represented as (ΓQual, ΓForb). The minimal qualified access structure and the maximum forbidden access structure are computed as follows:

Γm = {Aε ΓQual: ∀B∀ A→ B! ε ΓQual} and
ΓM = {Aε ΓForb: ∀B∀ A→ B! ε ΓForb}

3.1. Half toning Technique using Dithering Matrix

The drawbacks of VCSs proposed in [3] [6] [7] and [14] is that they can't work with gray scale image. The VCS that works with gray scale images was proposed by MacPherson [20]. Its main drawback is that it has long pixel expansion. Another technique introduced to work with gray scale images for visual cryptography is known as half toning technique used in [9] [16] and [21]. The half toning technique is also known as dithering technique. It is best used to covert a gray scale image into a binary image. This approach is every effective as the binary image allows the VCS to be applied as described in [3] [7] [6] and [14]. There are many types of algorithms existed on halftone technique. However, in this paper we make use of a technique known as dithering [19]. It makes use of certain amount of black and white pixels in the form of patterns in order to achieve the grayscale. The percentages of black and white pixels represent different grayness.

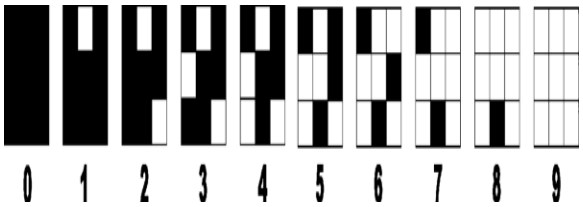

Fig 2: Half toned patterns of dithering matrix with gray levels 0 to 9

The process of half toning is to map the pixels of gray scale from the original image into the black pixels with patterns. However, this process needs lot of memory. To overcome this problem, we use dithering matrix which a kind of integer matrix. The half toning process is described in algorithm 1 and the half toned patterns of dithering matrix with gray levels 0 to 9 is visualized in fig. 6.

3.2. Embedding VCS into the Covering Shares

Once meaningful covering shares are generated using the dithering matrices, the realization of embedding process is described in algorithm 2 as shown in fig.3. Embedding process is described in fig. 3. According to this embedding does mean that the pixels found in the embedding positions are replaced by share matrix's sub pixels. First of all the covering share is divided into blocks and sub pixels.

In case if the PQ is not multiple of t, padding is applied. In each t sub pixels, m positions are chosen. Such positions are known as embedding positions in this paper [7] [17]. All of the embedding positions must be same in order to support decode secret image correctly. By stacking embedded shares, the unused sub pixels are always black. The m pixels that are not participated in embedding process can recover secret image as part of VCS. The embedding process is visualized in the. The result of the embedding is the collection of meaningful covering shares. By stacking a subset of covering shares, it is possible to obtain secret image as shown in fig 8.

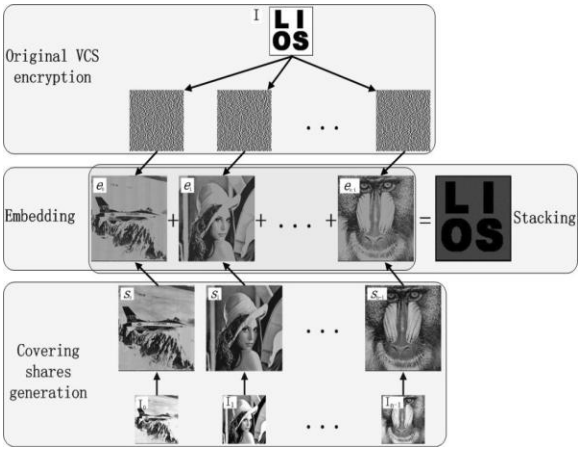

Fig 3: Shows result of the algorithm

As can be seen in the below figure, it is evident that first of all original VCS encryption is applied on secret image in order to generate random shares which have no visual meaning. Then the converting shares are generated by taking some images as input. Afterwards, the random shares are embedded into covering shares by following steps given in algorithm 2

3.3. Halftone Visual Cryptography via Error Diffusion

Naor proposed an algorithm for visual cryptography in which secret image is Obtained by just stacking shares without computation. Secret image is encoded into 'n' shares as shown in fig-2. Any share is nothing but a random binary pattern. All these 'n' shares are copied on to transparencies respectively, and distributed among 'n' meaningful images. Bundling all the transparencies together, will reveal the secret image without any computation being required as shown in fig-3.

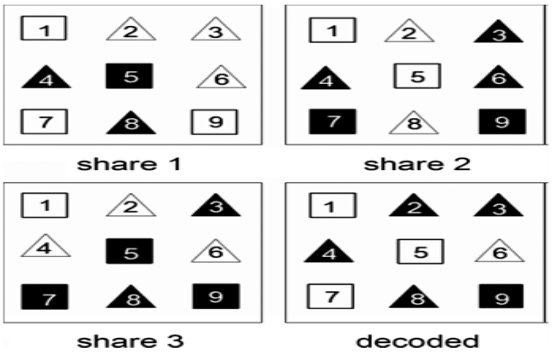

Fig 4: Example of halftone cells with size q=9 in a 3-out-of-3 scheme

However, by inspecting less than the specified shares, no one can gain any information about the secret image even if higher computational power is available for image processing.

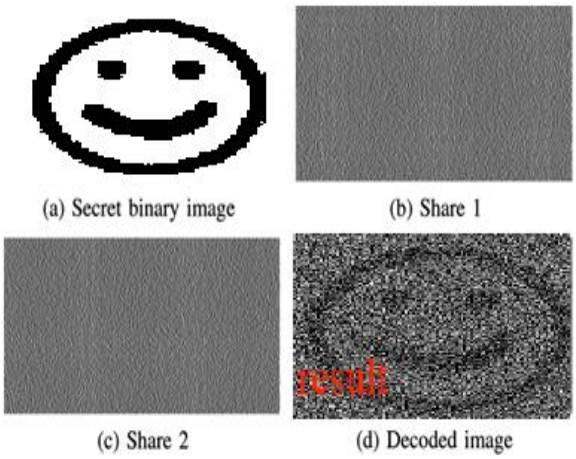

Fig 5: Random Pattern of encoded image with two shares. Resulted image is decoded image by the overlaying of generated transparencies

3.4. Embedded Extended Visual Cryptography Schemes

Embedded Extended Visual Cryptography EVCS can also be treated as a technique of Steganography. To avoid custom inspections on the encrypted images or shares EVCS is used because the shares of EVCS are not just shares but meaningful images, hence there are fewer chances for the shares to be suspected and detected [14]. Proposed tool for Embedded Half toned shares provides a user-friendly environment to work with images. This application supports .gif and .png (portable network graphics) formatted images and this application has been developed using swing and applet technologies, hence provides a friendly environment to users. Problem Definition: Whenever user transmits the data (image) in the network, any unauthenticated person can read data (image). In order to provide security to data (image) generally sender will encrypt the data (image) and send it the intended person and the receiver will decrypt the encrypted data (image) and uses it.

3.5. Sharing Multiple Secrets Using Visual Cryptography

To generate perfect ciphers or secret images Visual Cryptography is used. An image can be divided into multiple shares, and that multiple shares can be stacked again to get original image. Using VC the encrypted messages can be decrypted directly by the human visual system. Without computation VC can generate the original image and this is a distinguishing quality of the VC. The previous works on visual cryptography assume that the image or message is a collection of black and white pixels where in each pixel is handled individually. The encryption technique evaluates using 'k' shares out of 'n' secret shares. For a given image or message, 'n' transparencies are generated. If any 'k' of them is stacked together then the original image (message) is visible. The image will not appear or be made visible to end-user if less than 'k' transparencies are stacked.

Visual cryptography shares binary images only. Research works introduced halftone and color halftone mechanisms in visual cryptography in order to share color and grayscale images. Rather than considering only one secret, it will focus on how to share multiple secrets using visual cryptography. This mechanism will merge two secrets into shares using the master key, and then combine the two shares to form a new

share 'S1'. After that, master key [17] is modified to generate a key share 'S2'. The new share 'S1' and the key share 'S2' are employed to recover the secrets by shifting the key share 'S2' to various positions on 'S1'.

For sharing individually, this mechanism has one key and two secrets. With the same master key the secrets are encrypted and placed one after another. When the key is used on the secret the first secret is made visible to user. The same is true for the second secret. In order to open the next secret, the key has to be shifted by the images width or height. All secrets can be revealed using the same key. The joint sharing scheme works in a similar way of the above process. Shares are generated using the master key. All shares are read row by row and merged as single image by writing these read rows from the encrypted shares. When the key share is used on the merged image, the first secret share is revealed to end user, when the key is shifted down, the second secret is revealed.

4. Color Visual Cryptography Scheme

Hou proposed three color VC methods where the same technique is used to decompose the color secret image into three separate images that are respectively colored cyan (C), magenta (M) and yellow (Y). Then the halftone technique is used to translate the three color images into halftone images. Finally, by combining the three halftone images, a color halftone image can be generated. The color halftone image generation process is shown in Fig. The color halftone image takes eight different colors to display: cyan, magenta, yellow, black, red, green, blue and white [16]. The three methods proposed take the color halftone image as the secret image. Here, we focus on the second method and describe the details of this method. For each pixel of the color halftone image, the following process must be done. First, 2×2 blocks are built according to Share 1, and the four pixels C, M, Y and W are randomly permuted.

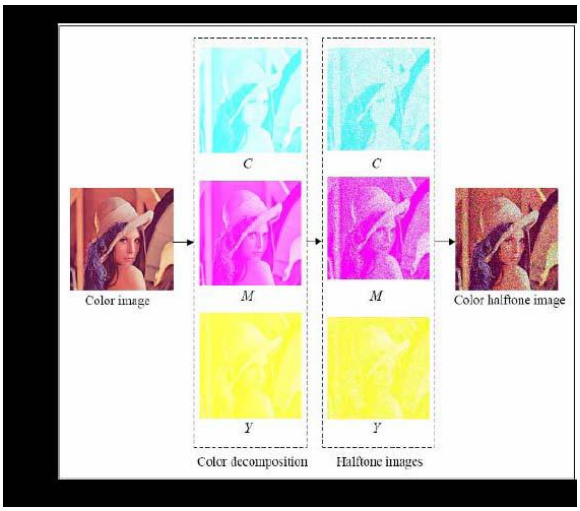

Fig 6: Color decomposition

For example, if one pixel of the color halftone image is green, then the pixel's color ratio would be 100%, 0% and 100% for *C*, *M* and *Y*, respectively. Thus, block in *Share* 1 is the permutation of pixels: cyan, magenta, yellow and white [10]. Then, the above information is applied, and the coding table will be referred to produce block of *Share* 2, where the permutation of the pixels is yellow, magenta, cyan and white. When all the pixels are done processed, two shares are produced. Each block of the two shares will be composed of *C*, *M*, *Y* and *W*.

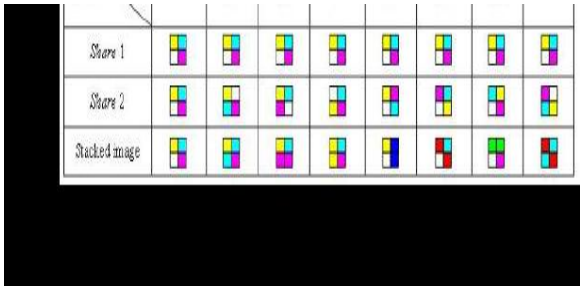

Fig 7: Color Halftone Transformation

The secret image can be readily recognized visually when the two shares are stacked together.

4.1. Color Visual Cryptography Schemes Sharing Single Secret

Until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg [17]. Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. In c-colorful visual cryptography scheme one pixel is transformed into m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black.

The color of one pixel depends on the interrelations between the stacked sub pixels. For a colored visual cryptography scheme with c colors, the pixel expansion m is c× 3. Yang and Laih [18] improved the pixel expansion to c × 2 of Verheul and Van Tilborg [17]. But in both of these schemes share generated were meaningless. For sharing a secret color image and also to generate the meaningful share to transmit secret color image Chang and Tsai [19] anticipated color visual cryptography scheme. For a secret color image two significant color images are selected as cover images which are the same size as the secret color image. Then according to a predefined Color Index Table, the secret color image will be hidden into two camouflage images. One disadvantage of this scheme is that extra space is required to accumulate the Color Index Table.

In this scheme also number of sub pixels is in proportional to the number of colors in the secret image as in Verheul and Van Tilborg [17] Yang and Laih [18] schemes. When more colors are there in the secret image the larger the size of shares will become. To overcome this limitation Chin- Chen Chang et al [20] developed a secret color image sharing scheme based on modified visual cryptography. This scheme provides a more efficient way to hide a gray image in different shares. In this scheme size of the shares is fixed; it does not vary when the number of colors appearing in the secret image differs. Scheme does not require any predefined Color Index Table. Though pixel expansion is a fixed in [20] this scheme is not suitable for true color secret image.

To share true-color image Lukac and Plataniotis [21] introduced bit-level based scheme by operating directly on S-bit planes of a secret image. To hide a color secret image into multiple colored images it is desired that the generated camouflage images contain less noise. For this purpose R.Youmaran et al [21] invented an improved visual

cryptography scheme for hiding a colored image into multiple colored cover images. This scheme provides improvement in the signal to noise ratio of the camouflage images by producing images with similar quality to the originals. For reducing pixel expansion in color visual cryptography scheme S.J.Shyu [19] advised a more efficient colored visual secret sharing scheme with pixel expansion where m is the pixel expansion of the exploited binary scheme. By considering color image transmission over bandwidth constraint channels a cost effective visual cryptography scheme was invented by Mohsen Heidarinejad et al [20]. The solution offers perfect reconstruction while producing shares with size smaller than that of the input image using maximum distance separable.

This scheme provides pixel expansion less than one. To improve the speed of encoding Haibo Zhang et al [19] presented a multi-pixel encoding which can encode variable number of pixels for each run. F. Liu et al [17] developed a colour visual cryptography scheme under the visual Cryptography model of Naor and Shamir with no pixel expansion. In this scheme the increase in the number of colors of recovered secret image does not increase pixel expansion. Wei Qiao et al [17] suggested visual cryptography scheme for color images based on halftone technique. A secret image sharing scheme for true-color secret images devised by Du-Shiau Tsai et al [18]. In the proposed scheme through combination of neural networks and variant. Visual secret sharing, the quality of the reconstructed secret image and camouflage images are visually the same as the corresponding original images.

4.2. Color Halftone Transformation and Pixel Extraction

Before encoding happens, this scheme applies color halftone transformation to produce color halftone images out of *CA*, *CB* and *SI*. Thus, *CA*, *CB* and *SI* are transformed into color halftone images *CA*', *CB*' and *SI*', respectively. The translation procedure is shown. Next, the pixel extraction procedure is utilized for reducing the size of the color halftone image [15].

The proposed scheme extracts some pixels from the color halftone image as important information for later coding. For each halftone image generated, the pixels from the odd-numbered rows, or those from the even-numbered rows, can be extracted out to make the extracted image, which means the size of the extracted image is N*N/2. In such a way, *CA*', *CB*' and *SI*' are pixels extracted to generate *EA*, *EB* and *ES*. In other words, our new scheme can have the secret image restored with only half. Before encoding happens, this scheme applies color halftone transformation to produce color halftone images out of *CA*, *CB* and *SI*. Thus, *CA*, *CB* and *SI* are transformed into color halftone images *CA*', *CB*' and *SI*', respectively. The translation procedure is shown. Next, the pixel extraction procedure is utilized for reducing the size of the color halftone image.

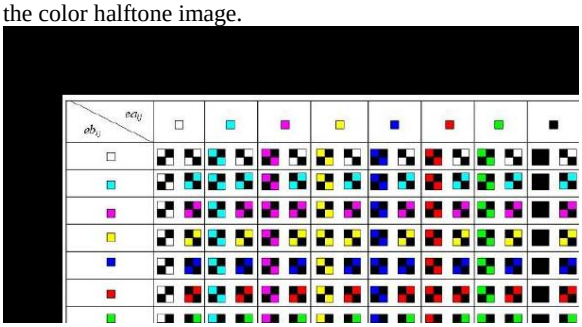

Fig 8: Cover Coding Table (CCT)

5. Related work

When pixels *eaij* and *ebij* are on an odd row (*I* mod 2 = 0), replace region I in pattern 1 with block 1, and replace region I in pattern 2 with block 2. In contrast, if pixel *eaij* and *ebij* are on an even row (*i* mod 2 =1), replace region II in pattern 1 with block 1, and replace region II in pattern 2 with block 2. Now the encoding procedure for *EA* and *EA* is completed [2] .For the encoding of *ES*, the proposed scheme needs to analyze the color ratio of the pixels. Then, according to the color ratio with the SCT (table) referred to, block 3 and block 4 can be generated. The position *esij* in *ES* is defined, where 0 <=*i*<*N* and 0<*j*<=*N/2*. When pixel *esij* is on an odd row (i.e. *i* mod 2 =0), replace region II in pattern 1 with block 3, and replace region II in pattern 2 with block 4. In contrast, if pixel *esij* is on an even row (i.e. *i* mod 2 =1), replace region I in pattern 1 with block 3, and replace region I in pattern 2 with block 4. After completing pattern 1 and pattern 2, we put them in the matching positions in Share 1 and Share 2, respectively. When all the pixels of *EA*, *EB* and *ES* are done processed the production of *Share* 1 and *Share* 2 is completed. In the decryption process, we stack *Share* 1 and *Share* 2 together to reconstruct the secret image. Also, blocks representing *eaij* and *ebij* become black after the stacking, but will not affect the block which represents *esij*. Meanwhile, this can improve the contrast of the secret image and make the image clearer.

6. Conclusion

The dealer or sender takes one secret image and verification image. These two images are encoded into shares, after encoding sends one secret share and one verification share to the participants. Each participant verifies the share and other participant secret share reveals the secret image. In this way cheating may be avoided.

In this paper, we have proposed a technique of well known secret sharing on both black and white and color images. At the time of dividing an image into n number of shares, we have used random number generator, which is a new technique not available till date. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images. This technique only checks ‘1’ at the bit position and divide that ‘1’ into (n-k+1) shares using random numbers. In most of our experimental results, each share reflects very little or even no information regarding the original image to human eye. But the main drawback of the algorithm is in its number of loops. For n=6, k=5 and a 32 bit pixel with 50% ‘1’, number of loop operation required is 32. For n=6, k=4 with other conditions same, number of loop operation required is 48. For n=6, k=3 with other conditions same, number of loop operation required is 64.

REFERENCES

[1] M. Noar and A. Shamir, "Visual cryptography," Advances in Cryptology - EUROCRYPT'94, pp. 1-12, 1995.

[2] D. S. Tsai, T. Chenc, and G. Horng, “On generating meaningful shares in visual secret sharing scheme,” 2008.

[3] S. J. Shyu, S. Y. Huang, Y. K. Lee,R. Z.Wang, and K.Chen, “Sharing multiple secrets in visual cryptography,” 2007.

[4] L. Feng, W. Chuankun, "Embedded Extended Visual Cryptography Schemes," IEEE Transactions on Information Forensics and Security, June 2011.

[5] Z.M.Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, Sep. 2009.

[6] F. Liu, C. K. Wu, and X. J. Lin, "Color visual cryptography schemes," IET Inf. Security, 2008.

[7] D. S. Wang, F. Yi, and X. B. Li, "On general construction for extended visual cryptography schemes," 2009.

[8] Z.M.Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via direct binary search," Sep. 2006.

[9] D. Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," 2005.74

[10] P. Tuyls, T. Kevenaar, G. J. Schrijen, T. Staring, and M. Van Dijk, "Security displays enable secure communications," 2004.

[11] M. Nakajima and Y. Yamaguchi, "Extended Visual Cryptography for Natural Images,"2002

[12] Visual Cryptography Application originally developed by Johannes boble, university of

[13] Regensburg. Source is from http://www-sec.uniregensburg.de/vc. Source modified for the purpose of application in plain java files. Error Filtering Schemes for Color Images in Visual Cryptography *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 11, 2011*

[14] P. A. Eisen and D. R. Stinson, "Threshold Visual Cryptography Schemes With Specified Whiteness Levels of Reconstructed Pixels," 2002.

[15] Z. M. Wang and G. R. Arce, "Halftone visual cryptography through error diffusion," in IEEE Int. Conf. Image Processing, 2006,

[16] C. Blundo, A. De Bonis, and A. De Santis, "Improved Schemes for Visual Cryptography," 2001.

[17] S. Droste, "New Results on Visual Cryptography," 1996.

[18] G. J. Simmons, W. Jackson, and K. Martin, "The geometry of shared secret schemes," 1991.

[19] An overview of visual cryptography International Journal of Computational Intelligence Techniques, ISSN: 0976–0466 & E-ISSN: 0976–0474 Volume 1, Issue 1, 2010, PP-32-37

[20] An Implementation of Algorithms in Visual Cryptography in Images International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013 1 ISSN 2250-3153

[21] Secure Visual Cryptography *International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 2 Issue 1 Jan 2013 Page No. 265-303*