ISSN:0975-9646
M. Durairaj et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 4047-4053

A Survey on Visual Cryptography for Secret Data Sharing

M. Durairaj[#1], V. Sutharson[*2]

#Assistant Professor, School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli

**Research Scholar, School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli*

***Abstract*- Visual Cryptography (VC) is a special kind of encryption techniques which is applied to hide the data in images. The image can be decrypted by using correct key image. Visual cryptography method is introduced by Moni Naor and Adi Shamir[1]. Visual cryptography scheme (VCS) is a method to encode a secret image into n shadow images called shares. The recovered secret image can be darker or lighter than the background. The secret data or secret information is hiding in the image using several encode and decode technologies. In this paper, the various methods are populated and reviewed their applications.**

***Keywords*- VSS, Pixel expansion, Bounds, Grey-Scale images, Color images, Halftoning**

I. INTRODUCTION

In the information science and technology development process, the transmitting information via Internet is as convenient as clicking a button. Internet is open and used to link more computers and networks that would facilitate free exchange of ideas and information. Simultaneously, the problem of guaranteeing the confidentiality of transmitted messages becomes imperative. Because one of the basic truths behind Internet security is that the Internet itself is not a secure environment.

The messages or information have to be prevented from unsecure environment by using encode and decoding methods. The cryptography is *necessary* for hiding data with the secure communications.

Visual cryptography is a cryptographic technique, this technique uses to be encrypted in such a way that decryption and it allows the visual information (images, text information, etc.). This method is for encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Visual Cryptography (VC) was first introduced by Moni Noar Adi Shamir at Eurocrypt'94 [1]. Moni Naor Y, et ,al.,[1] explained the problem of encrypting the visual information or visual message. A perfect secure way, which can be decoded directly by the human visual system. Now, It is common to transfer the multimedia data through the Internet and networks. This coming era of electronic commerce, an urgent necessary needs to solve the problem of ensuring information safety in increasingly open network environment. An encryption technologies of traditional cryptography are usually using to protect the information security.

Visual cryptography schemes (VCS) are the special kind of secret sharing schemes. Each of the secret is an image in the secret sharing scheme. It was introduced by Tzeng and Hu on 2002 [2]. It assuming *n* number of participants for a set P, the VCS encrypts the secret image into *n* transparencies which is shares given to the *n* participants or shares. The power set of the participants is divided into qualified sets. Finally the participants can visually recover the secret image by stacking their transparencies without any cryptography knowledge. The forbidden sets haven't any information in the secret image.

Ching-Nung Yang, et.al. [5] presented visual secret sharing(VSS) scheme is a perfect secure method that protects a secret image by breaking it into shadow images(called shadows).

Hossein Hajiabolhassan, et.al. [2] explained the visual cryptography, which is investigate the two parameters, which are pixel expansion and contrast. The pixel expansion is based on the number of sub-pixels are used to encode each pixel of the secret image in a single share, and that share should be the small as possible. The contrast measures the "difference" between a black and a white pixel in the reconstructed image which means the resultant image. In this paper, we presented a survey of visual cryptography application on secret data sharing found in the recently published peer reviewed articles. This review clearly analyses the latest trend on Visual Cryptography and its application as well as impacts.

II. VISUAL CRYPTOGRAPHY MECHANISM

In *Visual cryptography*, a plain text is encrypted in the forms of images (Visual Information). The encrypted secret text creates the shares which are passed through internet using channels such as fax or email and the shares are send it to the decryption process. The decryption process contains the human visual system.

The Visual Cryptography performs using the following mechanism for encrypt and decrypt the visual secret messages or visual secret information. The Visual cryptography mechanism is shown in Fig.1.

1. Each pixel of the image is divided into several smaller blocks. That the blocks are the same

number of white and black blocks. It may either horizontally or vertically.

2. If the pixel is divided into two blocks, one is black and the other block will be the white. If the pixel of the image is divided into four blocks, the two blocks will be white and the remaining two blocks will be black.
3. The information pixel will be the completely black blocks, also called the overlay version of pixels.

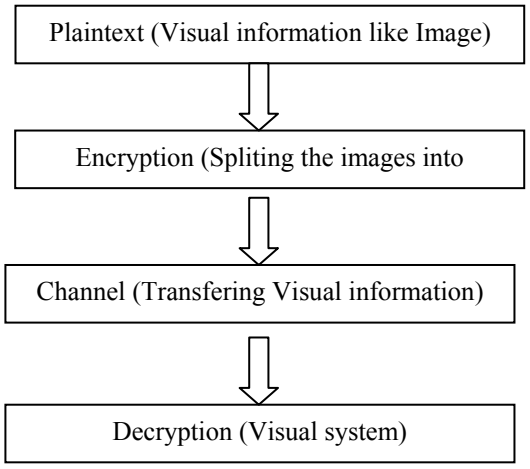

Fig. 1 Visual Cryptography Mechanism

III. REVIEW OF RELATED WORKS

Many types of visual cryptography are examined in this paper. The several Visual Cryptography methods are following to hiding the information in the image from the very first type of visual cryptography techniques right up to the latest development of visual cryptography techniques. The foundations of these all techniques are reviewed and examples provided.

A. Bounds for VSS

Hossein Hajiabolhassan, et.al. [2] proposed a model, in which only minimal qualified sets can recover the secret. Introduced a lower bound for the best pixel expansion of this scheme in terms of minimal qualified sets. The structure of visual cryptography schemes and they prove bounds on the size of the image distributed to the participants in the scheme. They were presented another one lower bound for the best pixel expansion of the scheme. The lower bound method is working based on an induced matching in hypergraph with the different qualified sets. The Visual cryptography technique is proceeds the best pixel expansion using aforementioned model and the traditional model, and it is happening by the basis matrices. The access structures based on the graphs and strong chromatic index is finding an upper bound for the smallest pixel expansion.

B. VSS with Perfect Reconstruction of Black Pixels

Carlo Blundo, et.al. [6] proceeded (k, n) - threshold visual cryptography scheme. This method is encode a secret image (SI) into *n* shadow images called shares such that any *k* or more shares enable the visual recovery of the secret image. But the shares are less than *k* shares, one cannot produce any information on the secret image. The visual recovery consists of coping the shares onto transparencies, and the shadow images are stacking them.

Visual cryptography schemes are classified by two parameters. There are "the pixel expansion" and "the contrast". The pixel expansion is the number of sub pixels of each pixel in the original image encoded. The contrast is measure the difference between a black and a white pixel in the reconstructed image.

In Visual cryptography schemes, the reconstruction of black pixels is perfect. That means, all of the subpixels are associated with a black pixel. The minimum pixel expansion of the such schemes can be simply computed by solving a suitable linear programming problem.

C. Visual Cryptography for Grey Level Images

Carlo Blundo, et.al. [8] explained the image expansion of visual cryptography schemes for grey level images whose pixels have *g* grey levels ranging from 0 (representing a white pixel) to *g-1* (representing a black pixel). Additionally, they give a required and adequate condition for such schemes to exist. It provides a general technique to realize, for any access structure, visual cryptography schemes encoding grey level images.

They are assuming the secret image is contain the collection of pixels. On the collection each pixel is associated with the grey level ranging from white to black. All the pixels are handled separately. Each pixel is appear in *n* versions called as *shares.* Each shares are having *m* black and white subpixels. The resulting structure of the shares can be report by an $n * m$ Boolean matrix,

$S = [sij]$

where, $sij = 1$, If the j^{th} subpixel in the i^{th} transparency is black.

Therefore the grey level of the combined share is obtain by stacking the transparencies $i1, \ldots, is$, are proportional to the Hamming weight $w(V)$ of the m-vector $V = OR(ri1, ..., ris)$, where $ri1, \ldots, ris$ are the rows of S which is associated with the transparencies. This grey level has made by the visual system according to the participants it may as any one of black, grey, or white.

D. Visual Cryptography for Color Images

Young-Chang Hou, et.al. [4] proposed Visual cryptography for color images having three methods for visual cryptography of gray-level and color images based on past in the black-and-white. These are the methods using in this work are Visual Cryptography method, The Halftone Technology, and The Color Decomposition method. These methods are not only keep the advantages of black-and-white visual cryptography, and also decrypt the secret images by utilize the human visual system without computation. Also have the backward compatibility with the previous results in black-and-white visual cryptography. Black-and-white VC is such as the *t* out of *n* threshold scheme, and it can be applied for the gray-level and color images easily.

E. VSS for Grey-Scale Images and Color Images

Daoshun Wang, et.al. [3] submitted the general probabilistic (k,n)-VSS scheme for grey-scale images and color images. Pixel expansion schemes of the original image can be set to a user-defined value. In the user defined value, when the value is 1, there is no pixel expansion. The quality of reconstructed secret images are deliberated by average contrast. It is equivalent to the contrast of existing deterministic VSS schemes. So the previous probabilistic VSS schemes for black-and-white images can be formed as a special cases in the schemes proposed.

F. A High Contrast and Capacity Efficient VSS

Kai-Hui Lee, et.al. [7] recommended the visual secret sharing for multiple secrets (VSSM), which allows for the encryption of a greater number of secret images into a given image area. Previously, the VSSM schemes incur a very serious pixel expansion that will damage capable of increasing the capacity of secret images encryption. Also, the most of the VSSM schemes will decrease the contrast of the recover images while the amount of secret images encryption is increase. These are the drawbacks, which will limiting suitability of the VSSM schemes. A highly efficient encryption algorithm is used for this high contrast and capacity efficient VSS.

G. Cheating the (2, N) VSS

Yu-Chi Chen, et.al. [10] proposed a method that allows $N-1$ colluding parties to cheat an honest party in visual cryptography. They are taking advantages for knowing the underlying distribution of the pixels in the shares to create new shares that combine with existing shares to form a new secret message of the cheaters choosing.

It is known that two shares are enough to decode the secret images by using human visual systems. But, it examine two shares will give some information about the third share. For an instance, the collaborate participants may examine their shares to conclude when they both have black pixels and use that information to determine that another participant which will also have a black pixel in that location. The black pixels are exist in another party's share that allows them to create a new share. So the new share will combine with the anticipate the shares to form the secret or information. A set of colluding parties that have enough shares to access the secret code can cheat other honest parties in this method.

H. The Halftone Technology

Jose J Tharayil, et.al. [9] initiated for an individual image component, each component consists of 256 different shades of the corresponding channel. The visual cryptography method can encrypt only the binary images that is black or white pixel. That the original continuous tone digital image, is transformed into a binary image consisting of 1's and 0's. This transformation from a continuous tone image to a bitmap representation is called halftoning. There are two types of Halftoning, which are AM Halftoning (Amplitude Modulated) and FM Halftoning (Frequency Modulated). The size of the halftone dots varies, while their spatial frequency is the constant one In AM methods. That means, the halftone dot size is become the bigger like the tone is getting darker. In FM methods, on the other hand, the size of the dot is constant while the frequency (the number of micro dots) varies. In the Hybrid halftoning, in an image's high frequency component is using FM Halftoning and low frequency components using AM Halftoning. Both the technique gives the benefits and better halftoned image. The solution of hybrid Halftoning is preserved and the remaining objects in the image are big enough to exploit human perception.

Young-Chang Hou, et.al. [4] suggested that according to the physical characteristics, the different kinds of media is use in the different ways to represent the color level of images. The computer screens are using electric current to control the lightness of the pixels of the images. The various of the lightness is generated different color levels. The general and the normal printers, such as laser printers, dot matrix printers, and the jet printers can only control the single pixel to print which means it print the black pixel or it is not able to print the white pixel which means it is not print the white pixel, instead of that is displaying the gray level or the color tone of an image directly. Such the way to represent the gray level of images is to use the density of printed dots. For example, the printed dots in the bright part of an image are sparse, and those in the dark part are dense. The method that uses the density of the net dots to simulate the gray level is called "Halftone" and transforms an image with gray level into a binary image before it is processing. Each and every pixel of transformed halftone image has only two possible color levels such as black or white. Because of the human eyes can't identify too tiny and small printed dots. A dot, tend to cover it's near of the dots. It can be simulated by the various gray levels through the density of the printed dots. Even though, the transform image actually has only two colors such that the black and white. The gray-level visual cryptography, since most of the printers have to transform the gray-level images into halftone ones before it is printing, and the transformed halftone images are the black-and-white only, such as the format of an image is very suitable for the traditional method to generate the shares of visual cryptography. In this paper, the transformed halftoning images are used to generate the visual cryptography for gray-level images.

IV. THE DEMONSTRATION OF VISUAL CRYPTOGRAPHY

Visual Cryptography (VC) was first introduced by Moni Noar and Shamir at Eurocrypt'94. It breaking up the original image into n shares as shown in Fig.1.

Fig. 2 Breaking up the image into n shares

Each pixel of an images is divided into smaller blocks. There are always the same number of white and black blocks. On the pixels the white may be the transparent. If a pixel is divided into two blocks, one part is white block and another one part is black block. If the pixel is divided into four parts, then it contain two white blocks and two black blocks. The image is divided into four parts as an example images as shown in Fig.3.

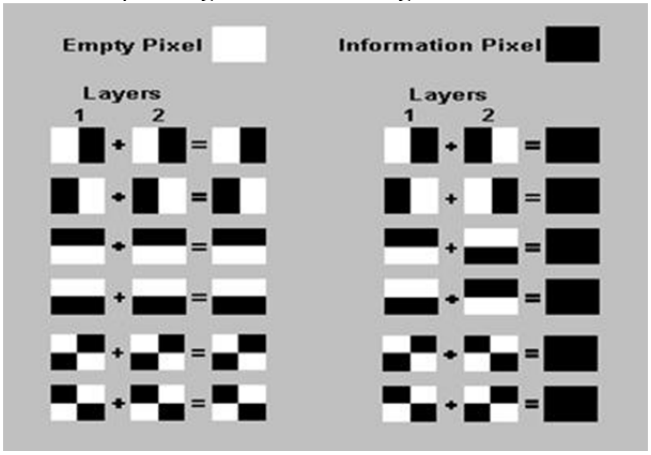

Fig. 3 Pixel divided into four parts

So that only someone with all *n* shares could decrypt the image by overlaying each of the shares over each other. 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 as shown in Fig.3.

All the pixels in the original image are encrypted similarly using this scheme. These all are the shares can be either Vertical or Horizontal or Diagonal Share as shown in the Fig.4.

Fig. 4 Images are encrypted using shares

Every pixel from the secret image is encoded into multiple sub-pixels in each share image using a matrix to determine the color of the pixels. In the (2,N) case, a white pixel in the secret image is encoded using a matrix from the following set, where each of the row gives the sub-pixel pattern for one of the components.

In the *(t, n)=(*2, 4*)* case, one of the several possible choices for the white matrix [**M0**] and the black matrix [**M1**] is to use

$$\text{All permutations of the columns : } [M_0] = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

While, in the secret image a black pixel is encoded by the using a matrix from the following set:

$$\text{All permutations of the columns : } [M_1] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

For instance in the (2,2) sharing case it means the secret is split into 2 shares and both shares are required to decode the secret. The complementary matrices to share a black pixel and identical matrices to share a white pixel. Stacking the shares all the sub-pixels associated with the black pixel now black while 50% of the sub-pixels associated with the white pixel remain white.

In the uses of those two transparent images in Visual Cryptography, one image contains the random pixels and the other image contains the secret information or message. It is not possible to retrieve the secret information from one of the images. Because, both of the transparent images or layers that are required to reveal the secret information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet shown in the Fig.5.

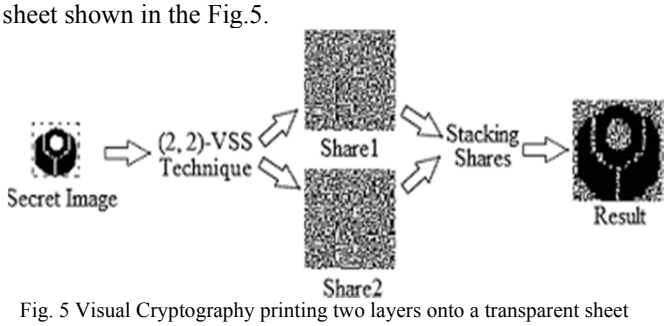

Fig. 5 Visual Cryptography printing two layers onto a transparent sheet

V. ADVANTAGES OF VISUAL CRYPTOGRAPHY

No knowledge of cryptography is required to get the secret message from shared images. This method can be used by anybody. The lower computational cost since the secret message is recognized only by human eyes and not cryptographically computed. The property of binary uses the robust method against the loss of compression and distortion. The cipher text can send through fax or email. The visual cryptography technique is easy and simple to implement.

Image data protection and image-based authentication techniques offer efficient solutions for controlling how private the data and images are made available only to the selected people or the authenticated users. It is necessary to design the system to manage an images that contain the sensitive data, such as the financial transactions, an electronic voting systems, and the medical records.

Cryptographic technique is using for the secretly transferring text documents, financial documents, text images, internet voting etc. The decryption algorithm is not required for this secure method. So a person may be unknown about cryptography, but even can decrypt the message. Visual Cryptography is not required to dependent the NP-Hard problem dependency for encryption.

VI. APPLICATIONS OF VISUAL CRYPTOGRAPHY

The Visual Cryptography is securing the information very effectively. So this methodology is using in several applications for the different purpose.

1. The Visual cryptography methods are effectively use in banks for the customer identification.
2. Anti spam-bot measure is using the visual cryptography.
3. Visual cryptography is using in electronic voting machines or remote voting machines for verify receipts.
4. Visual Cryptography is using to make colored digital watermarks.

VII. RESULT AND DISCUSSIONS

Hajiabolhassan, et.al. [2] concluded for the Bounds for VSS, a lower bound for the best pixel expansion of this scheme in the terms of minimal qualified sets. The lower bound method is working based on an induced matching in hypergraph with the different qualified sets. Visual cryptography is proceed the best pixel expansion using aforementioned model and the traditional model, and the cryptography is happening by the basis matrices.

Ching-Nung Yang, et.al. [6] concluded for the VSS with perfect reconstruction of black pixels, in the techniques of the visual cryptography the secret schemes are in which the reconstruction of black pixels is perfect. That means, all the subpixels are associated with a black pixel are black. The minimum or the lowest pixel expansion of the such schemes can be simply computed by solving a suitable linear programming problem.

Blundo, et.al. [8] concluded for the visual cryptography for Grey level images that the image expansion of visual cryptography schemes for grey level images whose pixels have g grey levels ranging from 0 (representing a white pixel) to *g-1* (representing a black pixel). Additionally, they give a require and adequate condition for such schemes to exist. It provides a general techniques to realize for any access structure, and the visual cryptography schemes can be encoded the grey level images. Each pixel is associated with the grey level ranging from white to black in the collection. The grey level combined share is obtain by stacking the transparencies. This grey level is produce by the visual system according to the participants it may as any one of black, grey, or white.

Young-Chang Hou, et.al. [4] concluded the methods for Visual Cryptography color images such as the Halftone Technology, and to process the Color Decomposition method. The visual cryptography methods are not only keep the advantages of black-and-white visual cryptography but also utilize the human visual system to decrypt the secret images without computation. Also have the backward compatibility with the previous results in black-and-white visual cryptography.

Daoshun Wang, et.al. [3] concluded the general probabilistic (k,n)-VSS scheme for grey-scale images and color images. In this schemes, the pixel expansion can be set to a user-defined value. In that user defined value when the value is 1, there is no pixel expansion. The quality of reconstructed secret images, deliberated by average contrast.

Kai-Hui Lee, et.al. [7] concluded for A high contrast and capacity efficient VSS, which incur a very serious pixel expansion that will damage capable of increasing the capacity of secret images encryption. It also, the most of the VSSM schemes will decrease the contrast of the recover images while the amount of secret images encryption is increase. These are the drawbacks limiting suitability of the VSSM schemes. A highly efficient encryption algorithm is using for this high contrast and capacity efficient VSS.

Yu-Chi Chen, et.al. [10] concluded for Cheating the (2,N) VSS, the distribution of the pixels in shares to create new shares that combine with existing shares to form a new secret message of the cheaters are choosing. It is enough the two shares are to decode the secret images by the using of human visual systems. The secret shares are combined with the anticipate shares to form the secret information. In the cheating way, a set of colluding parties that have enough shares to access the secret code can cheat other honest parties.

Jose J Tharayil, et.al. [9] concluded for the halftone technology in which Hybrid halftoning. The high frequency components of an image are using FM Halftoning and the low frequency components of an image are using AM Halftoning. Both the techniques are give the benefits and better halftoned image. The solvent of the hybrid Halftoning is maintained and the remaining objects in the image are big enough to exploit human perception. The method that uses the density of the net dots to simulate the gray level is called "Halftone" and transforms an image with gray level into a binary image before it is processing. Each pixel of the transformed halftone image has only two possible color levels such as black or white.

A. Comparison Table

The Visual Cryptography technique is following the several methods and techniques for secure the visual data. The comparison of the techniques are shown in Table 1.

TABLE I
COMPARISON TABLE OF VC TECHNIQUES

TECHNIQUES	OBJECTIVES	PIXEL EXPANSIONS	METHODS	RESULTS
Bounds for VSS	Determining the best visual contrast (regardless of pixel expansion) is completely resolve. For the sake of completeness, it is interesting to find the bound for the pixel expansion.	The secret image consists of a collection of black and white pixels	Lower bound for the best pixel expansion, An upper bound for the smallest pixel expansion	The best pixel expansion
VSS with perfect reconstruction of black pixels	The minimum pixel expansion	The shares onto transparencies	Computed by solving a suitable linear programming problem	Construction for (3, n)-threshold VCS, (n-1, n)-threshold VCS
Visual Cryptography for Grey level images	Define and analyze the visual cryptography schemes for grey level images	Images whose pixels have g grey levels ranging from 0 (representing a white pixel) to g - 1 (representing a black pixel)	(rQual, rForb)((rQual, rForb, m, g)-GVCS, for short) with the relative differences α0, α1, . . . , αg-1. (rQual, rForb,m,g)-GVCS with relative differences $\alpha_0, \alpha_1, \ldots, \alpha_{g-1}$. The optimality of (k, k, m, g) -GVCS, the pixel expansion and the relative differences $\alpha_0, \alpha_1, \ldots, \alpha_{g-1}$	Defined and analyzed visual cryptography schemes for grey level images. Given the necessary and sufficient conditions for the such schemes for exist. Finally it proved optimality of (k, k, m, g) - GVCS
Visual cryptography for color images	To combine three methods for visual cryptography such as the gray-level and color images based on past black-and-white VC, the halftoning technology, and the color decomposition method	Each pixel of the color secret image is expanded into a 2×2 block to form two share images. Each 2×2 block of the sharing images are filled with the colors red, green, blue and white (transparent) respectively	The t out of n threshold scheme ($t \leq n$)	This methods are not only retain the advantages of black-and-white VC. It exploits the human visual system to decrypt the secret images without any computation. Also have the backward compatibility with the previous results in black-and-white visual cryptography
VSS for grey-scale images and color images	The quality of the reconstructed secret images are measured by an average contrast, that is equivalent to the contrast of existing deterministic VSS schemes	Pixel expansion in a deterministic VSS schemes is constant, and the pixel expansion is variable	Binary (k,n)-VSS scheme , General probabilistic (k,n)-VSS scheme for grey-scale images and another scheme for color images.	The quality of the reconstructed image, measured in terms of contrast is the same as the conventional deterministic VSS schemes
A high contrast and capacity efficient VSS	Increase the capacity efficient for VSSM schemes, and maintains an excellent level of contrast	Each secret pixel within a secret image is encrypted a block consisting of β sub-pixels in each share image. The area of a share image is β times that of the original image. A sub-pixel is associated with a given black or white secret pixel must contain the same number of black pixels	A highly efficient encryption algorithm. This algorithm adopts a novel hybrid encryption approach that includes a VC-based encryption and a camouflaging process	The experimental result is demonstrate the approach, it is not only increase the capacity efficient for VSSM schemes, it is also maintain an excellent level of contrast in the recovered secret images.
Cheating the (2,N) VSS	Region Cheating Attack (RCA) as a result of the properties of HVS.	Several adjacent pixels as a unit	Deterministic white-to-black attack (DWtBA)	Point out that a well-known cheating immune scheme
The halftone technology	To increase the capacity of secret images	Divided into component colors	Apply hybrid halftoning, FM and AM halftones are Separating Homogeneous and Non-Homogeneous Areas	Inter-pixel exchanging to hide the information

VIII. CONCLUSIONS

Visual cryptography is a technique where the visual information in the form of the text, an image etc., which are encrypted in such a way that decryption does not need computer as it is just a mechanical operation. The Visual Cryptography methods are provide the secure ways to transfer multimedia data such as images over the Internet. The advantage of the visual cryptography is which exploits human eyes to decrypt the secret images. Visual cryptography, which concentrate on black-and-white images, and color images decomposition to construct methods that can deal with both gray level and color visual cryptography. Cryptographic technique is being used by several countries for secretly transfer the hand written documents, the text images, an internet and electronic voting, the financial documents etc. The different kinds of innovative ideas and extensions are exist for the basic visual cryptographic model introduced till now.

REFERENCES

[1] Moni Naor y and Adi Shamir z, in: A. De Santis (Ed.), *Visual Cryptography*, in Proceedings of Advances in Cryptology: Eurocrypt'94, Lecture Notes in Computer Science, Vol. 950, Springer, Verlag, 1994, pp. 1-12.

[2] Hossein Hajiabolhassan, Abbas Cheraghi, *Bounds for Visual Cryptography Schemes*, Discrete Applied Mathematics 158 (2010) 659_665.

[3] Daoshun Wang, Feng Yi, Xiaobo Li, *Probabilistic Visual Secret Sharing Schemes for Grey-Scale Images and Color Images*, Information Sciences 181 (2011) 2189–2208.

[4] Young-Chang Hou, *Visual Cryptography for Color Images*, Pattern Recognition 36 (2003) 1619 – 1629.

[5] Ching-Nung Yang, *New Visual Secret Sharing Schemes Using Probabilistic Method*, Pattern Recognition Letters 25 (2004) 481–494.

[6] Carlo Blundo, Alfredo De Santis, *Visual Cryptography Schemes with Perfect Reconstruction of Black Pixels*, Comput. & Graphics, Vol. 22, No. 4, 1998, pp. 449-455.

[7] Kai-Hui Lee, Pei-Ling Chiu, A High Contrast and Capacity Efficient Visual Cryptography Scheme for the Encryption of Multiple Secret Images, Optics Communications 284 (2011) 2730–2741.

[8] Carlo Blundo, Alfredo De Santis, Moni Naor, *Visual Cryptography for Grey Level Images*, Information Processing Letters 75 (2000) 255–259.

[9] Jose J Tharayil, E.S.Karthik Kumar, Neena Susan Alex, *Visual Cryptography Using Hybrid Halftoning*, Procedia Engineering 38 (2012) 2117 – 2123.

[10] Yu-Chi Chen, Gwoboa Horng and Du-Shiau Tsai, *Cheating Human Vision in Visual Secret Sharing*.