International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-11)

Research Article | **November 2014**

Visual Cryptography Schemes: A Comprehensive Survey

[1]Mona F. M. Mursi*, [2]May Salama, [3]Manal Mansour
[1]Professor, [2]Assistant Professor, [3]Teaching Assistant
Computer Engineering Dept. Faculty of Engg.,
Benha University, Egypt

Abstract-

Cryptography is study of transforming information in order to make it secure from unintended recipients. Visual Cryptography Scheme (VCS) is a cryptography method that encrypts any information [picture, printed text, etc] such that decryption can be performed using human visual system. The goal of this survey paper is to give the readers an overview of the basic visual cryptography schemes constructions, as well as the new techniques derived from VCS. We also review some applications that take advantage of such secure schemes.

Keywords- Visual cryptography schemes (VCS), Extended Visual Cryptography (EVC), Universal Share, Contrast, Security.

I. INTRODUCTION

Visual Cryptography is a type of encryption technique which was developed to secretly share images and information without using encryption or decryption keys. This technique simply takes the secret image, divides it into parts; each part is called "share". These shares are printed on a special type of papers (transparencies). When these parts are superimposed together, the secret image can be retrieved easily using Human Visual System (HVS) only and no need for calculations or computations. The important point in this idea is that every share alone can reveal no information about the secret image. This makes the encryption safer. Three types of images are used in VC; binary, gray and color images. Many researches included more than one secret in the shares and made the shares more meaningful to distract hackers from realizing that a secret is hidden in the file.

Visual cryptography was first invented by Moni Naor and Adi Shamir in 1995 at [1]. They produced a basic scheme for sharing a secret binary image using their own coding table. The binary image is divided into two shares. If the pixel in the secret image is white, one of the upper two rows of table I is chosen to make share1 and share2. If the pixel of the secret image is black, one of the lower two rows of table 1 is used to make share1 and share2. Every pixel from the secret image is expanded to 4 pixels, so when the shares are generated and superimposed together the reconstructed image will be four times the original secret image size because of this pixel expansion. Also the resolution of the reconstructed image will be less than the original secret image as every white pixel is decomposed into two white & two black pixels. Only one secret could be hidden using this technique. This was further investigated and developed by many researches. This paper surveys related researches that has been carried out on developing various visual cryptography schemes.

TABLE I. NAOR AND SHAMIR'S SCHEME FOR ENCODING A BINARY PIXEL INTO TWO SHARES

pixel		share #1	share #2	superposition of the two shares
	$p = .5$			
	$p = .5$			
	$p = .5$			
	$p = .5$			

The rest of this paper is organized as follows. Section II discusses literature survey for visual cryptography techniques. In section III, a comparison between several techniques is discussed, while section IV shows example application of VC and section V comprises the conclusion and the future work.

II. LITERATURE SURVEY

A. Visual Cryptographic Schemes with Meaningless Shares:

1) Binary Secret Images: Wu and Chen [2] in 1998, were the first researchers to present the visual cryptography schemes to share two secret images in two shares. Two secret binary images were hidden into two random shares, namely share A and share B. The first secret image can be revealed by stacking the two shares, denoted by A⊗ B, and the second secret can be revealed by first rotating share A by angle Θ anticlockwise. The rotation angle Θ was designed to be 90◦. Figure 1 illustrates this scheme.

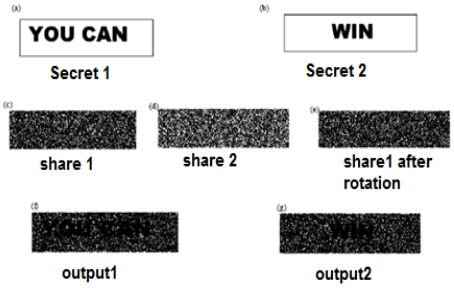
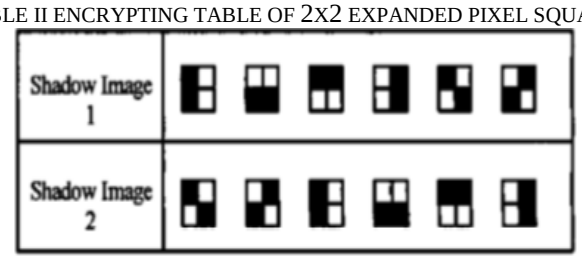


Fig 1 Sample example for hiding two secret images.

The restriction of the rectangular shape image is that it can only decrypt two shadow images by overlapping them at angles of 0°, 90°, 180° and 270°. Consequently, to overcome the angle restriction presented in [2], Hsu et al [3] proposed another scheme in 2004. The scheme hides two secret images in two share images with arbitrary rotating angles. Two confidential data sets are encrypted into shadow images under different overlapping angle using the encrypting Table II of 2x2 expanded pixel squares.

TABLE II ENCRYPTING TABLE OF 2X2 EXPANDED PIXEL SQUARE.



After encoding, the data will turn into two shadow images. The first confidential data will appear directly after overlapping the shadow images. To decrypt the second confidential data, one shadow image is fastened and the other is spun in X degrees (X is the factors of 360). Figure 2 describes the scheme.

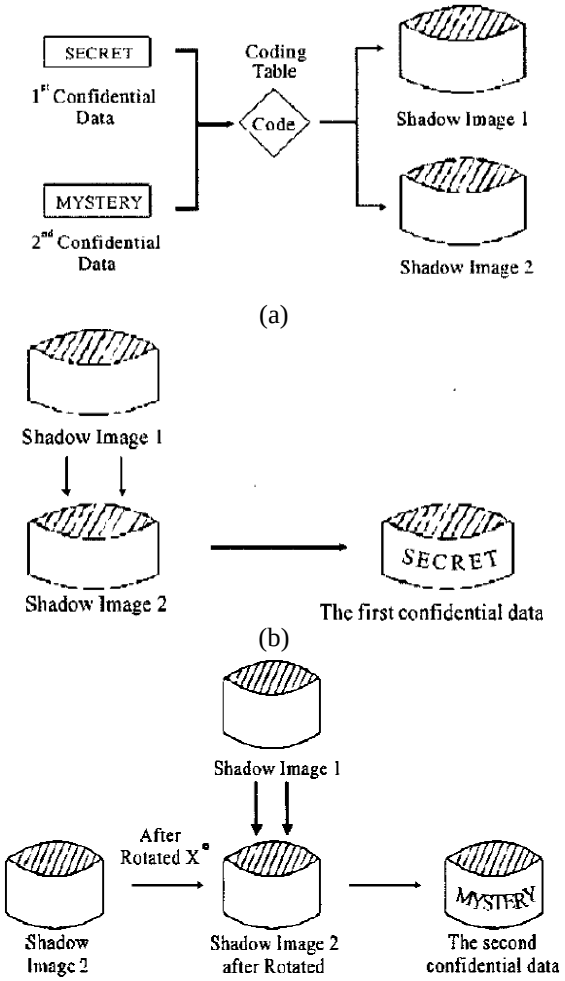


Fig 2 (a) Encryption phase (b) Decryption of the first confidential data (c) Decryption of the second data.

The result of this scheme is seen darker as in Figure 3, as the white pixel is represented by three black and one white pixel, the black pixel is represented by four black pixels.

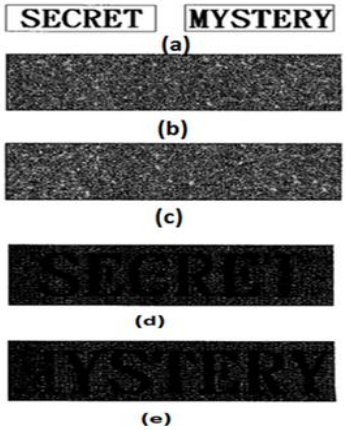


Fig 3 (a) Secret images, (b) Shadow image 1, (c) Shadow image 2, (d) overlap the shadow images 1and 2, (e) Shadow image 2 rotates 72° and overlaps with image1.

In 2005, circular visual cryptography was introduced by [4]. In this scheme, circular shadow image can hide two or more confidential data sets into circular images and display them at both the inner and outer region of the circular images. However, it can only produce a circular shadow image without the central part causing a low resolution on the images at the inner portion as seen in figure 4. It encrypts data into two ringed shadow images allowing hiding two confidential data sets simultaneously.

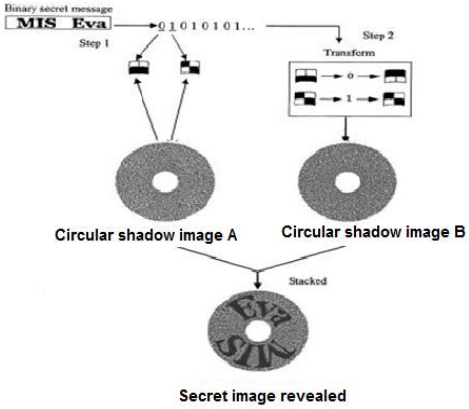


Fig 4: Flow for reconstructing the image

In [5], a new idea called hierarchical visual cryptography (HVC) is provided this is expansion less scheme but it can consider only binary images. The idea is that the shares are produced in levels. The system takes the secret image, divides it into two shares by the traditional method of [1]. Two shares (S1, S2) are produced at this level, which is level one. Each share is then divided into two shares by the same methodology to (S11, S12), (S21, S22). This is level two of (HVC) where four shares are produced. Any three shares are taken to produce the key share according to table III.

TABLE III KEY SHARE GENERATION.

Share12	Share21	Share22	Key Share
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

The output from this system is the remaining share and the key share. Figure 5 shows the result of this scheme.

Fig 5 (a) Secret image

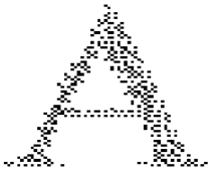


Fig 5 (b) recovered secret image.

2) Gray-Colored Images: In [6], the idea of decomposing the gray level image was discussed. The expansion was based on 9 pixels. In 2005, Lukac and Plataniotis [7] proposed an encryption technique that deals with gray level image but the pixel expansion was 4 pixels only. Their algorithm is summarized by splitting the gray scale secret image into 8 bit planes denoted as Sb_i where i is from 1 to 8. Sb_8 and Sb_1 are least significant bit plane and most significant bit plane respectively and are binary images as shown in Figure 6.

Fig 6 Bit plane decomposition of Gray scale image (N=8) (a) Lena image, (b)-(i) bit plane 1-8.

The 8n binary shares are created, for each of the bit plane, denoted as $BSH_{,i,j}$ where i = 1, ... ,8 and j = 1, ... , n where i is the i^{th} bit plane and j is the j^{th} binary share. Stacking the corresponding 8 binary shares (BSH i = 1, ... ,8) in bit level to get the j^{th} grayscale noisy share. Finally: n grayscale random-looking hares are generated.

In the decryption phase, each of the n grayscale noisy shares needs to be broken into 8 bit planes, namely $BSH_{,i,\,j}$. The bit plane of secret image is decrypted by considering the corresponding pixel values of the n binary shares. Figure 7 shows the result of this scheme.

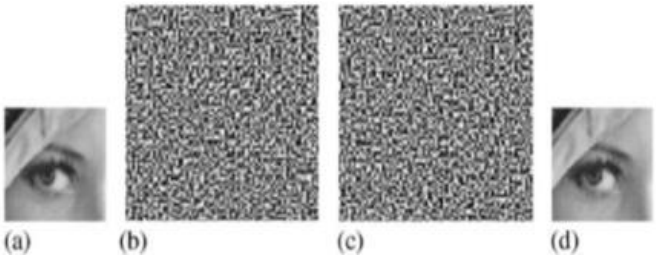


Fig 7 (a) Original secret gray level image of size KxK ,(b) –(c) two noisy shares with size 2K x 2K ,(d) reconstructed image

First trial dealing with the colored image was in [8]. A color visual secret sharing scheme for limited color images was proposed. Suppose the number of colors is (P). Each pixel in the secret image is expanded to p sections; each section is divided into p sub pixels and produces n shares with p sections.

When the shares are stacked together, the p-color secret image is revealed. If p is large, then the pixel expansion is large. Unfortunately, this scheme tends to produce many blocks with large numbers of black sub pixels, the visual quality of the recovered image is weak and the shares are meaningless.

In 2008, a new scheme was introduced to share multiple images [9]. In this research, a visual secret sharing (VSS) scheme for encoding multi-secrets is described. The proposed scheme aims at encoding an original secret image (SI) by extending traditional VCS in such a way that extra secret images (ESIs) can be further encoded into the same two share images, say share A (S_A) and share B (S_B). In decoding process, all secret images can be retrieved by shifting operations.

The proposed scheme comprises three major phases: decomposition phase, encoding phase, and decoding phase. In decomposition process, the original secret image SI is divided into n sub-blocks with the same size. In Encoding phase, SI is turned into two share images (2, 2) VSS. In decoding process, all secret images can be disclosed by a way of shifting operations. Figure 8 shows the steps of the shifting process, Figure 9 shows the result .

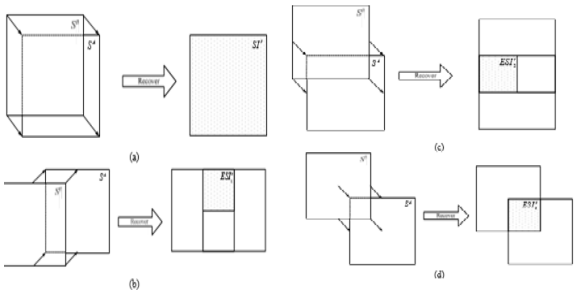


Fig 8 (a) Recovering the original secret, (b)-(d) recovering the extra secrets by shifting.

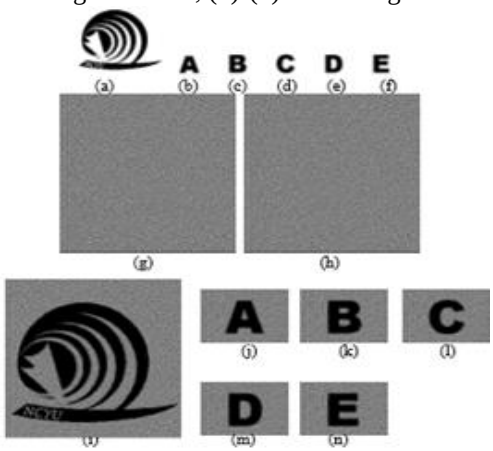


Fig 9 (a)original image, (b)-(f) Extra secrets , (g)(h) two shares , (i)-(n) recovered secrets

In [10], there was a trial to modify the pixel expansion to be CxM, where C is the number of colors in the secret image and M is the pixel expansion for each color. The result of this scheme improved the visual quality of the retrieved image but the shares were still meaningless.

In [11], the colored secret images are decomposed to three channels: Cyan, Magenta and Yellow CMY. The halftone technique is applied to transfer each channel to half tone image as shown in figure 10 After decomposition, each primitive-color image is dithered so that each image will have two color levels (zero or one), namely the presence of corresponding primitive color or the absence of it.

Fig10 Dithered C,M andY Components

A black mask with double height and double width of the original image is created (expansion is four), then three other shares (CMY and W) are created from the old one-bit dithered shares, the result shares are in Figure 11. The following table illustrates the encoding process.

TABLE IV GENERATION OF (C,M,Y) SHARES.

Mask	Orignal Pixel (C, M, Y)	Share 1 (C)	Share 2 (M)	Share 3 (Y)	Superimposed Pixel
	(0, 0, 0)				
	(1, 0, 0)				
	(0, 1, 0)				
	(0, 0, 1)				
	(1, 1, 0)				
	(0, 1, 1)				
	(1, 0, 1)				
	(1, 1, 1)				

Fig11 Black Mask With the three shares

Here, there are two levels for security because as long as the manager of a company gives C,M,Y shares and keep the black mask secret no information can be revealed from the image , as soon as the black mask is present, even if one of the shares is absent, some information can be revealed from the reconstructed image.

B. Extended Visual Cryptography With Meaningful Shares

In the above listed schemes, the shares were meaningless. Meaningless shares attract the attackers to decrypt these noisy shares. It was the concern of the researchers to make the shares meaningful in order to distract the attackers' attention.

1) Binary Images: The first trial to make meaningful shares was in [12]. The objective was to share a W×H secret two images between two participants. The system uses the two-out-of-two visual secret sharing technique to construct two shares, Share-1 and Share-2, of 2W × 2H, which means that the expansion is still 4 times the original image. Each secret bit is expanded to a block with 2×2 pixels. If a secret bit is"1", all the pixels in the block are black in color. Otherwise, the block will have two black pixels and two white pixels. After the share construction process, they can obtain Share-1 and Share-2. Then, the two shares are embedded into two gray-level cover images C1 and C2. The image size of each cover image is 2W×2H pixels .Two methods were proposed for the embedding. Method 1: after generating the two shares, one secret bit from a secret share is randomly embedded into the r_i-th least significant bit ($LSBr_i$) of a cover image. The scheme uses a pseudo random number generator (PRNG) with a secret seed SD to generate a sequence of random numbers{ r_1, r_2,..., r_m}, where m = (2W×2H) and $r_i \leq L$. Here, L is the number of least significant bits decided by the user. Figure 12 shows the embedding procedure of Method 1, when L =3. For example, if r =2, then the LSB2 of a cover pixel is replaced with a secret bit. Although those three bits are changed, the image quality still remains the same.

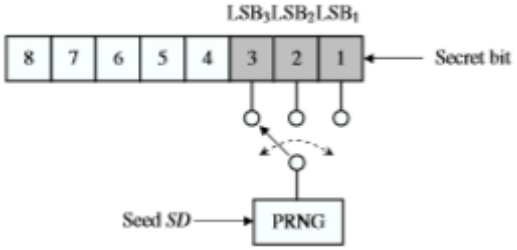


Fig 12 The embedding system of the random bit replacement

Method 2: one secret bit from a secret share is embedded into the 4-th bit of a cover image as in Figure 13

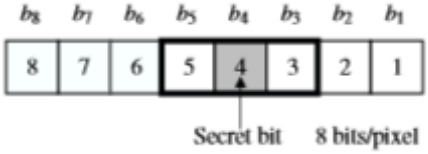
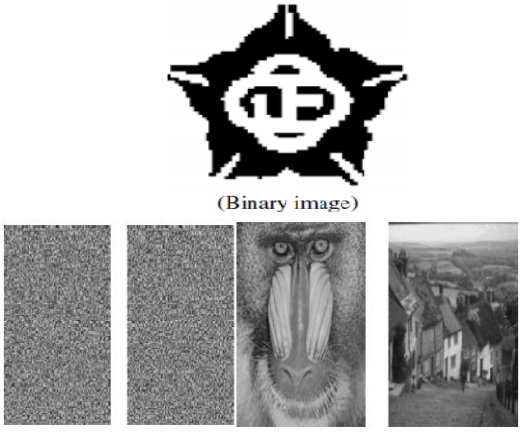


Fig 13 The embedding strategy of Method 2.

When the two participants want to decode the two secret images, two secret shares are first extracted from two stego images which are the cover images containing the secret pixels. Figure 14 shows the result.



stacking result
Fig 14 Result of using method 2

The advantage of method 1 over method 2 is its better image quality. That is because Method 1 does not affect the significant bits of a pixel. However, method 1 cannot resist modifications such as JPEG compression. In terms of robustness, method 2 is better than method 1.In 2010, another idea for VC was introduced by [13]. Here, the share is produced from the secret image and can be revealed by copying the share, shifting the copy and superimposing the shifted copy and the original share together, as shown in Figure 15.

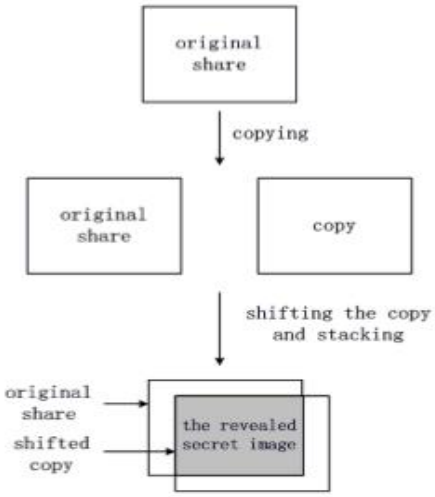
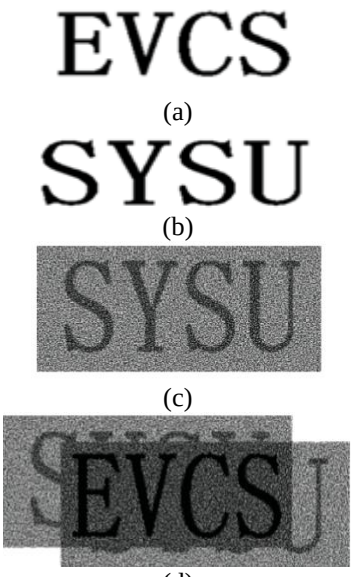


Fig 15 Decryption of the proposed scheme

The input to this scheme is the secret image (m*n pixels), cover image C (M*N pixels). The output from this system is Innocent-looking share (2M * 2N pixels). result is shown in Figure 16. The secret image is 80 *200 pixels and the cover image is 100* 250 pixels.



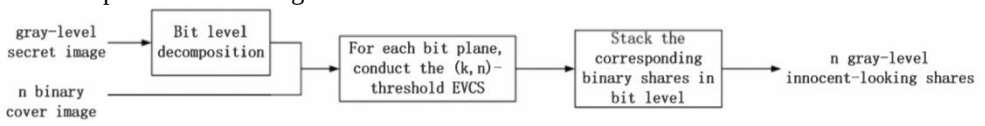
(a)
(b)
(c)
(d)

Fig 16 (a) Secret image (b) cover image (c) produced share with acceptable look (d) Reconstructed secret image

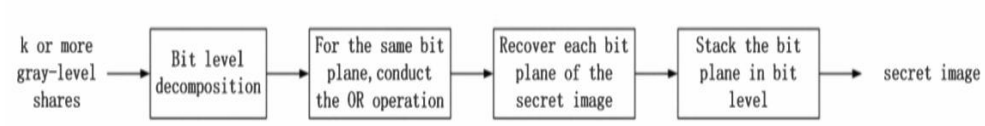
2) Gray-Colored Images: In 2010 Chen et al [14] proposed a new scheme which combines the two shares having more than one secret and makes them meaningful. Most importantly, no extra steps are needed for extracting the shares as it is not a kind of steganography. Four black and white images are considered, all of them with the same size. Two of them

are considered as secret images and the other two images are considered as the cover images. When overlapping the two cover images directly, the first secret image will be constructed directly. When rotating the first cover image 90°anticlockwise, it will construct the second secret image. So there are 5 pixels to be considered for every pixel encoded: two pixels of the cover images, two pixels of the secret image and the pixel of the first cover after rotation].

In [15], a scheme is proposed that removes the main drawback of [7] which was the noisy shares. The scheme proposes a bit plane based image sharing scheme that can share one grayscale secret image into n innocent-looking shadows to reduce the disadvantages of random looking share. Any k out of n shadows can perfectly reconstruct the secret image. Figure 17 illustrates the process of creating the shares.



(a)



(b)

Fig 17 (a) Creating the shares (b) revealing the secret

In [17], the proposed scheme was also targeting to make the shares meaningful and the expansion of the reconstructed image is twice the secret image. The algorithm consists of four steps. Firstly, a secret colored halftone image is made from the given secret image. Secondly, t the pixels from the colored half tone image are extracted as important information to reduce the size of the secret image for later coding if the size of the original secret is NxN, then after extracting the odd or even rows which considered as important values the size will be NxN/2. The encoding process comes in the third step, where the shares are generated. The shares will be 2Nx2N each. Finally, when these two shares are stacked together the secret image will be generated with twice the size of the original image as in Figure 18. This algorithm contains two Cover Coding Tables (CCT) for encoding the cover images and Secret Coding Table (SCT) for encoding the secret image as in figure19.

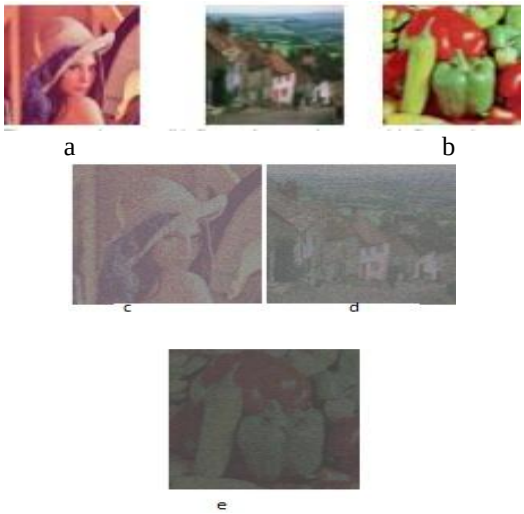


Fig 18 (a) two cover images (b) secret image (c-d) cover images containing the secret (e) recovered secret image.

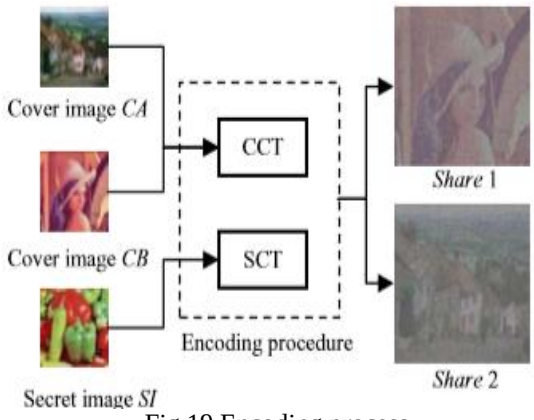


Fig 19 Encoding process

C. Key Based VC

This technique simulates the idea of public and private key[21]. If someone wants to share 100 images with others, he has to obtain 100 shares, one for each image, which is very difficult to manage. So this scheme solves this problem without the need of complex computation or mathematical calculation, where that person keeps only one share image and decrypts all other secret images with this share. A new scheme is discussed in [18]. This share is known as "UNIVERSAL SHARE". Figure 20 illustrates the idea.

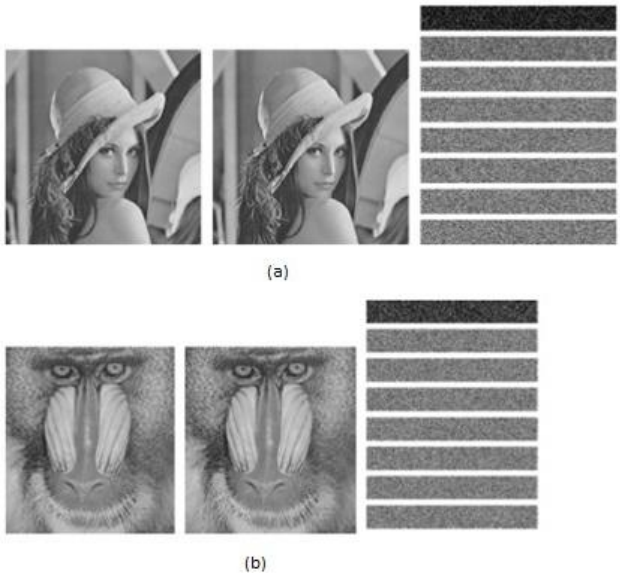


Fig 20 two images with their shares where the first top shares in (a) is identical to the top share in (b) which is called universal share

In 2014, a scheme was presented [19] aiming to achieve key safeguarding and secret image sharing. Mathematical calculations were used to generate an image acting as Key Image. This Key is generated from the secret image and some chosen securing images (p). To reconstruct the secret color image, the Key image and q securing images are used where q<p. This is called (p,q) threshold scheme. The example in Figure 21 is for (5, 3) threshold scheme. Out of the 5 securing images, any three images with the key image can regenerate the secret.

Fig 21 (a) Secret image (b) five securing images (c) Key image (d) re-constructed image

III. COMPARISON BETWEEN VC SCHEMES

Table V summarizes the features, pros and cons of each of the reviewed technique above. Enhancing the shares generated from the binary secret images was the main objective in [2-5]. The first trial to hide more than one secret image in the same two shares was done in [2]. The disadvantage of this scheme is the bandwidth needed which is four times the secret and it was angle restricted. In [3], the angle restriction is solved but the reconstructed image is still four times the size of the secret and it seems to be darker as it uses coding table II that represents the white pixel by three black pixels and only one white pixel. The problem of the expansion is solved in [5] by considering blocks, each of four pixels instead coding pixel by pixel The result secret is highly contrasted and it leads to removal of graying effect observed in basic Shamir scheme and other coding tables which makes it suitable only for handwritten words. In [7], although bit Plan decomposition is used, which divides the gray level image into 8 binary images, it is not time consuming as the experimental result indicates that it uses 0.931s per 256×256 gray-scale image for encryption and 1.473s for decryption. In the case of a 256×256 color image, the execution requires 2.914s for encryption and 4.462s for decryption. This scheme [7] supports gray level or colored images which makes it suitable for natural images and faces. Enhancing the visual cryptography was done in [12-19] by creating meaningful shares to avoid attacks by means of steganography or different algorithms. In [12], steganography was used to provide level of security but it lost an important rule of VC as the secret can't be retrieved by only human visual system. Resisting distortion was accomplished in [13] as one secret image was hidden into one innocent-looking share. High security level is achieved in [14] where two colored images are hidden into two shares. The recovered secret images were darker in color. However, human vision system is more than enough to recognize the decrypted information. Table V gives a quick comparison between these schemes.

TABLE V. COMPARISON BETWEEN SEVERAL SCHEMES. c INDICATES NUMBER OF COLORS IN VISUAL CRYPTOGRAPHY SCHEMES, n IS THE NUMBER OF SECRETS.

Author	Year	Ref	No Secret Images	Pixel Expansion	Image Format	Share generated	contrast	Brief description
Noar and Shamir	1995	[1]	1	4	Binary	Meaningless	Low	Use coding table to generate the shares.
Wu and Chen	1998	[2]	2	4	Binary	Meaningless	Low	Angle Restriction to create the second secrets.
Hwa-Chiug Hsu , Tung-Shou Chen, Yu-Hsuan Lm	2004	[3]	2	4	Binary	Meaningless	Low	Arbitrary angle rotation to create the second secret.
Pallavi Vijay Chavan1, D. Mohammad Atique and D.Latesh Malik3	2014	[5]	1	Expansion Less	Binary	Meaningless	Graying effect is reduced to zero	Hierarchical Visual Cryptography used to generate a share and a key from the other three shares.
Tzung-Her Chen, Kai-Hsiang Tsao, Kuo-Chen Wei	2008	[9]	n>=2	4	Binary, Gray, Color	Meaningless	Low	turn more secret images into the same share images.
Lukac and Plataniotis	2005	[7]	1	4	Gray-Level	Meaningless	Medium	Decomposing the gray image to 8 bit plane.
E.R. Verheul and van Tilborg	1997	[8]	1	cx 3^(k−1)	Colored	Meaningless	Low	
Yang and Laih	2000	[10]	1	cx 2^(k−1)	Colored	Meaningless	Medium	Use access structure to construct the (k, n) colored VSS scheme.
Young-Chang Hou	2003	[11]	1	4	Colored	Meaningless	High	Create four shares C,M,Y,B The secret won't be retrieved without the black one.
Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin	2005	[12]	1	4	Binary	Meaningful	Low	The shares are created then the steganography is employed to hide the noise shares

Xiaotian Wu,Wei Sun	2010	[15]	1		Gray	Meaningful	Medium	Bit Plane Decomposition is applied , (k,n) threshold method
Hsien- Chu Wu, Hao-Cheng Wang, Rui-Wen Yu	2008	[17]	1	2	Colored	Meaningful	Medium	Use the Halftone technique and two coding tables one for repairing cover images, other for coding the secret image.
Wen-Pinn Fang , Chen Lin	2007	[18]	N	$1–(1–n^{-1})/K\times 100\%$ of the input secret size	Gray	Meaningless	Low	This scheme simulates the public and private key algorithm.
Qin Chen, Xiaorong Lv,Min Zhang, Chu	2010	[14]	2	4	Binary-Gray-Colored	Meaningful	Medium	The algorithm uses five pixels two pixels of the cover images, two pixels of the secret image, the pixel of the first cover after rotation [coding table is used to create the shares].

IV. APPLICATIONS

Visual cryptography has several applications. The following are a few of them.

A. Online payment system

In [20], steganography and visual cryptography are used to produce online payment system to minimize the information sent to the online merchant. The password of the customer is hidden inside cover text by means of steganography technique, then the account number is placed above this text. A snapshot is taken and the shares are produced. One of these shares is taken by the customer and the other is saved in the data base of the certification, CA. During the payment process, the shopper sends his own share and the merchant submits his own account details to CA which collects his share with the shopper share to get the original image which contains the password and other details. The information is sent to the bank for comparison. If ok, the bank transfers the fund. Figure22 illustrates the system.

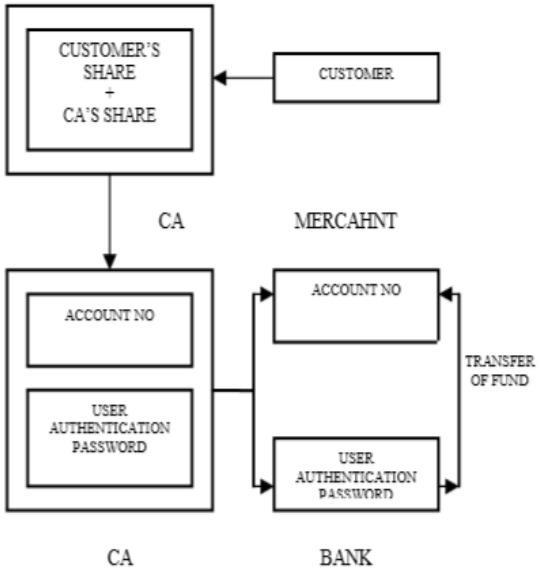


Fig 22 Payment system

B. Anti- Phishing Framework

Phishing websites aim to steal personal information such as passwords, credit cards numbers …etc. They trick customers by making identical web site to a real one where the customer submits his information. The work of [22] solves this problem by using visual cryptography technique. The customer can ensure if this is the genuine web site or not by typing his user name. The server will send a share from its database. The client will superimpose his own share with the one sent by the site to ensure this is not phishing page and type his information. Figure 23 illustrates the process.

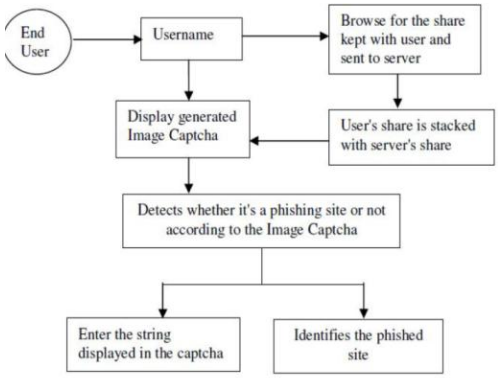


Fig 23 System Architecture Diagrams

C. Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography (HVC)

Instead of using traditional signature for authenticating employees the system in [23] uses HVC to make the authentication done by shares to prevent the systems from some attacks such as brute force attack on the system, An academic institute is considered in this paper as an application. Firstly, employees must be enrolled in the system, the signature of the employee is scanned and entered in the (HVC) system to get its key share and it's simple share as discussed in[5] this key is printed on a card and given to the employee and the simple share is entered to the system database. During authentication, the employee inserts his own card in the card reader mounted in the entrance to read the key share from the card and superimposes over the corresponding simple share available in the database. Figure23 illustrate the process of creating the shares by (HVC).

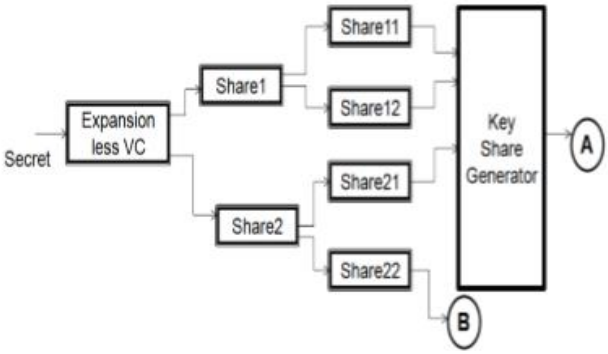


Fig 24 Hierarchical Visual Cryptography Encoder

V. CONCLUSION AND FUTURE WORK:

The importance of encrypting and decrypting secret images was the motive behind reviewing a variety of visual cryptography techniques in this paper. Many factors decide on which technique to use. Among the factors are number of shares, image format, encrypted shares' size, and the type of share to be generated. A comparison table is presented to summarize the different features of each technique reviewed. It has been concluded that the work done in visual cryptography using universal share is minimal. The universal share, or the public key, solves the problem of having to deal with many keys to decrypt several images. Our future work will focus on this area; to use a public key in order to decrypt multiple images with utmost security.

REFRENCES

[1] Moni Naor and Adi Shamir, *Visual Cryptography*, Advances in cryptology– Eurocrypt, pp 1-12, 1995.

[2] C.C. Wu, L.H. Chen, *A Study On Visual Cryptography*, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[3] Hwa-Chiug Hsu , Tung-Shou Chen, Yu-Hsuan Lm, *The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing*, in Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001, March 2004.

[4] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, *New Visual Cryptograpgy System on Circular Shadow Image and Fixed Angle Segmentation*, Journal of Electronic Imaging 14(3), 033018 (Jul–Sep 2005).

[5] Pallavi Vijay Chavan1, Dr. Mohammad Atique2 and Dr. Latesh Malik3, *Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares*, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[6] Chin-Chen Chang and Tai-Xing Yu, *Secret Sharing for image encryption*, Pattern Recognition, vol. 38, no. 5, pp. 767-772, 2005.

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

[8] E.R. Verheul and. van Tilborg, *Constructions and Properties of k out of n Visual Secret Sharing Schemes*, Designs, Codes and Cryptography, Vol. 22(No. 2, pp. 179- 196, 1997.
[9] Tzung-Her Chen, Kai-Hsiang Tsao, Kuo-Chen Wei, *Sharing A Secret Two-Tone Image In Two Gray-Level Images*, Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2008.
[10] C. N. Yang and C. S. Laih, *New colored visual secret sharing schemes*, Designs, Codes and Cryptography, Vol. 20, No. 3, pp. 325-335, 2000.
[11] Young-Chang Hou, *Visual cryptography for color images*, Pattern Recognition, Vol. 36, pp. 16 19- 1629, 2003.
[12] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, *Sharing A Secret Two-Tone Image In Two Gray-Level Images*, Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.
[13] Xiaotian Wu and Wei Sun, *A Novel Extended Visual Cryptography Scheme Using One Shared Image* ©2010 IEEE.
[14] Qin Chen, Xiaorong Lv, Min Zhang, Yiping Chu, *An Extended Color Visual Cryptography Scheme with Multiple Secrets Hidden*, Processing of the International Conference on Computational and Information Sciences 2010.
[15] Xiaotian Wu,Wei Sun, *A Novel Bit Plane based Image Sharing Scheme using EVCS*, International Conference on Information, Networking and Automation (ICINA). IEEE, 978-1-4244-8106-4, 2010
[16] W. P. Fang and J. C. in, *Universal share for the sharing of multiple images*, Journal of the Chinese Institute of Engineers, Vol. 30, 2007, pp. 753-757.
[17] Hsien- Chu Wu, Hao- Cheng Wang, and Rui-Wen Yu, *Color Visual Cryptography Scheme Using Meaningful Shares, achieves a high security level*, Proceedings of the Eighth international Conference on Intelligent Systems Design and Applications, pp. 173-178, 2008.
[18] W. P. Fang and J. C. in, *Universal share for the sharing of multiple image*, Journal of the Chinese Institute of Engineers, Vol. 30, 2007, pp. 753-757.
[19] Hirdesh Kumar , Awadhesh srivastava, A *Secret Sharing Scheme for Secure Transmission of Color Images*, International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) 2014.
[20] Souvik Roy1 and P. Venkateswaran, *Online Payment System using Steganography and Visual Cryptography*, 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science.
[21] Introduction to CRYPTOGRAPHY and NETWORK SECURITY, Behrouz A.Forouzan , McGraw-Hill International Edition.
[22] Mr. K. A. Aravind1, Mr. R .Muthu Venkata Krishnan, *Anti-Phishing Framework for Banking Based on Visual Cryptography*, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January- 2014.
[23] Pallavi Vijay Chavan, Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography, 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science

