Volume 5, Issue 4, 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Road Map to Visual Cryptography

Sonam Soni
M.Tech Student, Computer Science, MPSTME,
NMIMS, Mumbai, India

Abstract*— The field of encryption is becoming very important in present days in which information security is greatest concern. Cryptography is a techniques related appearance of information security such as confidentiality, data security, authentication etc. Visual Cryptography is a new techniques used for securing the visual information like picture, text etc. the basic idea of Visual Cryptography is that images are divided into several parts that is called shares. Than these shares are distributed among concerned participants and to decrypt them arrange or stacked to get the image back. For security reason hackers cannot detect any clues about the secret image. At first Visual Cryptography techniques was developed for binary images only but later on it was advanced for colour images also. This paper summaries various methods of Visual Cryptography. Various methods on this topic have been discussed like Traditional Visual Cryptography, Halftoned Visual Cryptography, Hierarchical Visual Cryptography, Progressive Visual Cryptography, Extended Visual Cryptography and a comparison of all these methods is given.*

Keywords— Visual Cryptography, Extended Visual cryptography, Halftoned Visual Cryptography, Progressive Visual Cryptography, Hierarchical Visual cryptography

I. INTRODUCTION

Cryptography is a method of protecting confidential information. It encrypts the content of information using some mathematical computation and a secret key, and then decryption is done using the same secret key in symmetric key encryption. The basic Traditional Visual Cryptography algorithm [1] introduced by Adi and Shamir discussed about securing the digital images by dividing the image into two secret shares. Most of the existing methods on Visual Cryptography involve a variation on the Traditional Visual Cryptography approach. In this paper, most of the existing methods along with their advantages and limitations are been discussed. Visual Cryptography can be divided into three main phases, Image Acquisition, Encryption, and Decryption, in which only the encryption phase is varied based on the approach used.

Another approach to Visual Cryptography is Extended Visual Cryptography which allows the construction of visual secret sharing scheme within which shares are meaningful as opposed to having random noise on shares. This method can also be applied on colour images using error diffusion for High Visual Quality Shares [2]. A faster version of the algorithm is been discussed in [3] which reduces considerable amount of time for encryption and decryption process in a much easier way.

Visual Cryptography is applied on halftoned images as discussed by Zhou Z, Arce GR, Di Crescenzo G [4] to overcome the drawback of Traditional Visual Cryptography approach in which the shares consisting of random pixel patterns do not take any visual information and may lead to suspicion of secret information encryption. Halftone VC removes such disadvantage by generating shares taking meaningful visual information via halftoning methods

This method is used in performance of error filters in Halftone Visual Cryptography in improved shares have been developed by changing the error filters that were earlier used in Halftone Visual Cryptography via error diffusion and results were compared with the existing work for improvements on visual basis and on mathematical basis using mathematical parameters for index of quality of the image like PSNR and Universal quality index UQI [5]. Halftone Visual Cryptography via Error Diffusion [6] is also one of the methods which provides halftone images with good quality and has low complexity. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images and also used in a Novel Visual Secret Sharing Scheme for Multiple Secrets via Error Diffusion in Halftone Visual Cryptography [7].

A cluster of small dots can be used in visual cryptography to represent black and white pixels this approach is termed as dot size variant VC [8]. This would result in filtering out small dots if the share if the share is photocopied or scanned or even viewed with a mobile phone or digital camera.

A VC approach in which hidden information will appear only if more than two shares are stacked together is been discussed by Young-Chang Hou and Zen-Yu Quan [9] ,and is known as Progressive Visual Cryptography. The limitations of pixels expansion and poor visual quality problem of PVSS is overcome in [10]. This method is also used with water marking for meaningful share [11].Yet another friendly progressive visual secret sharing scheme is modification of previous one which suffers the problem of pixel expansion which is innate deficiency of conventional VC-based VSS. In this paper, a new friendly Progressive VSS scheme by random grids is proposed without pixel expansion this problem [12].

Next approach is Hierarchical Visual Cryptography the key idea behind Hierarchical Visual Cryptography is to encrypt the secret information in number of levels. As the number of levels in Hierarchical Visual Cryptography increases, the secrecy of data tends to increase [13]. This method is also used in as an Intelligent System for Secured Authentication using Hierarchical Visual Cryptography [14] and Hierarchical Implementation of RKO Technique for Visual Cryptography [15]. This is used in Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography [16].

II. COMPARATIVE STUDY OF VARIOUS METHODS

Traditional Visual Cryptography

General framework for visual cryptography:

Visual Cryptography was first introduced by Moni Naor and Adi Shamir in 1994. They come up with a visual secret sharing scheme, where an image is divided into n shares so that only someone with all n shares could decrypt the image, while someone with any n-1 shares can reveal no information about the secret image. Each share is printed on a separate transparency and decryption is performed by overlaying the shares when all n shares are overlaid, the original image gets appeared. This allows visual information like pictures to be encrypted in such a way that their decryption can be performed by human visual system without any complex computation or algorithms. This is known as (k,n) VCS model where k represents minimum no of shares needed to decrypt the secret image and n is the total number of shares generated by the visual cryptographic scheme.

Hence, the whole Visual cryptographic process can be summarized as given below in block diagram (Fig1) of visual cryptography. In first step we will acquire the image then we will apply an encryption by creating shares then we will transfer that share in channel and then the decryption is done by stacking all shares by human visual system.

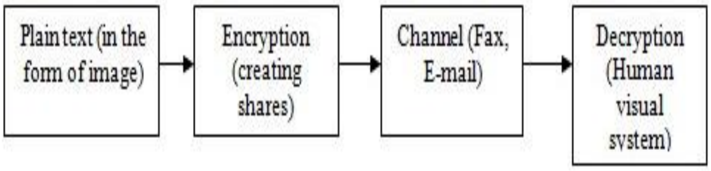

Plain text (in the form of image)
Encryption (creating shares)
Channel (Fax, E-mail)
Decryption (Human visual system)

Fig. 1 Block diagram of basic visual cryptography

1. Basic model

Visual Cryptography scheme was developed by Naor and Shamir in 1994 [17].It reduces complex computation problem in decryption process, and the secret image can be restored by overlapping share operation. In this scheme two transparent images called shares are developed. One of the shares is made of random pixels in which black and white pixels are of equal number. Second share is made according to first share. When these two shares are superimposed, information is revealed.

The basic approach of visual cryptography for Naor and Shamir method is depicted in fig. 2 below. If the pixel is white then it will be empty pixels and if the pixel is black then it will be information pixel. From the figure it can be seen that a white pixel can be divided into two different shares as 1 and 2 as shown in figure below. For white and black pixels there are six different states into which a pixel may be divided.

The disadvantage of this approach is the quality of image will be in degraded. So, this method is only suitable when the quality is not a biggest concern. The main concern is only the security of image.

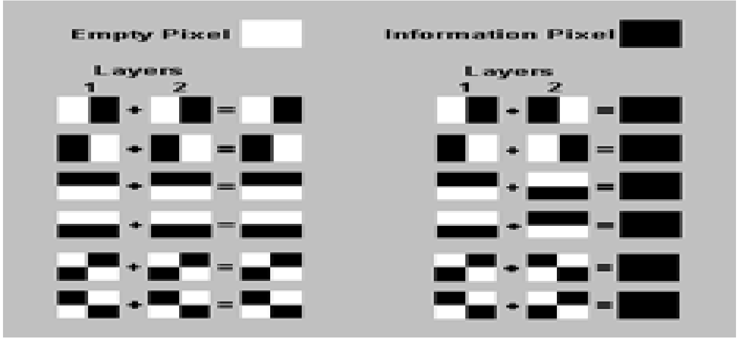


Fig.2 Six different states for black and white pixels [17]

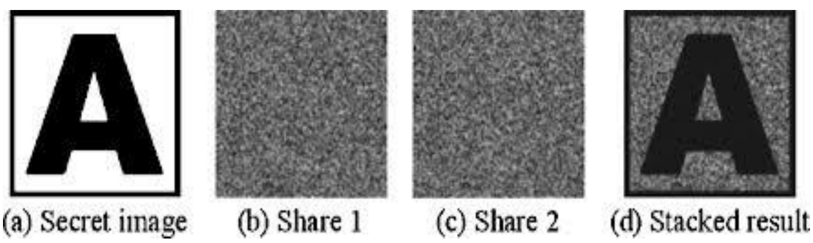


Fig. 3 Implementation of a (2, 2) VCS [24]

A. *Gray scale visual cryptography*-To encrypt a gray-scale image into two gray-scale shares, the original image is decomposed into eight bit planes. Each bit plane is encrypted using binary VC. All the encrypted shares of the bit planes are recomposed and two gray-scale shares are created. Superposing gray-scale shares reveals the secret [18].

The steps used for gray scale visual cryptography:

- In the first step transform the gray-level image into a black-and-white halftone image.
- The image will decomposed into 2x2 for each black and white pixel according to the rule in fig.2. If the pixel is white, then select one of the combinations from the content of blocks in share 1 and share 2. Same for black pixel select one combination from the two rows as the content of two transparencies.
- Repeat Step 2 until every pixel in the halftone image is decomposed into two share [19].

i) Sharing Single Secret Image: In this type of visual cryptography scheme, the secret image is divided into exactly two shares. This is the simplest kind of visual cryptography. The major application of this scheme is found with remote voting system that uses 2 out of 2 secret sharing schemes for authentication purpose. To reveal the original image, these two shares are required to be stacked together.

ii) Sharing multiple secret-In this approach hiding two secret binary images into two random shares, namely A and B, such that the first secret can be seen by overlapping the two shares, denoted by A XOR B, and the second secret can be obtained by first rotating A Ө anti-clockwise. It has been designed the rotation angle Ө to be 90. Further this method is modified because it is easy to obtain that Ө can be 180◦or 270◦. In this method there is a problem of angle restriction, Hsu proposed a scheme to hide two secret images in two rectangular share images to overcome the angle restriction of previous approach of Wu and Chen's scheme. Wu and Chang also refined the idea of Wu and Chen by encoding shares to be circles so that the restrictions to the rotating angles (Ө = 90◦, 180◦ or 270◦) can be removed [20].

B. *Colored based visual cryptography*- Previously, visual cryptography was only done for black and white image but further it was implemented for color image also. This technique generate noise like random pixels on share images to hide secret information which on overlay decrypt the information, this technique is known as conventional visual secret sharing scheme. In this. Visual Cryptography is applied on color image. The image is divided into three shares on the basis of color C (Cyan), M (Magenta) and Y (Yellow) [21]. This method first decomposes the original image into three primitive color images under the subtractive model, namely, C (Cyan), M (Magenta) and Y (Yellow) the three primitive color components of the image, where each image has 256 levels of the corresponding primitive color, and each pixel represented by three bytes. Converting to (C,M, Y), where C,M, Y {0- 255}. Example let's see in Fig. 4 the image is divided into three primitive color that is C (Cyan), M (Magenta) and Y (Yellow). And these will be considered as shares. Now we can apply same encryption algorithm for these three shares.

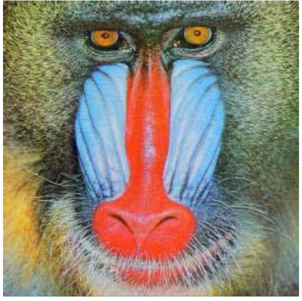


Fig. 4: Original secret image [21]

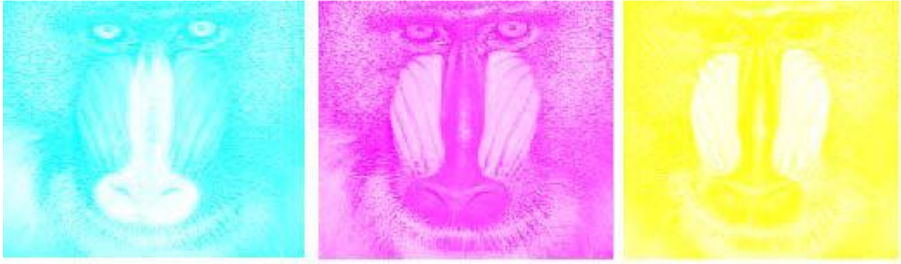


Fig. 5 Primitive Colour (C, M, Y) Components [21]

i) Sharing Single Secret Image- First colored visual cryptography scheme was developed by Verheul and Van Tilborg [21]. Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. In the c-colorful visual cryptography scheme one pixel is transformed into the m sub pixels, and each sub pixel is divided into the c color regions a colored image is seen as an array of pixels, each of which is of color $K_{0,}$ $K_{1,...,}K_{c-1}$. Here c is the number of colors and K_i is called the i-th color. In each and every sub pixel, there is exactly one color region is colored, and all the other color regions are black. The color of one pixel depends on the inter relationships between the stack sub pixels. In this colored visual cryptography scheme with c colors, the pixel expansion m is c× 3.

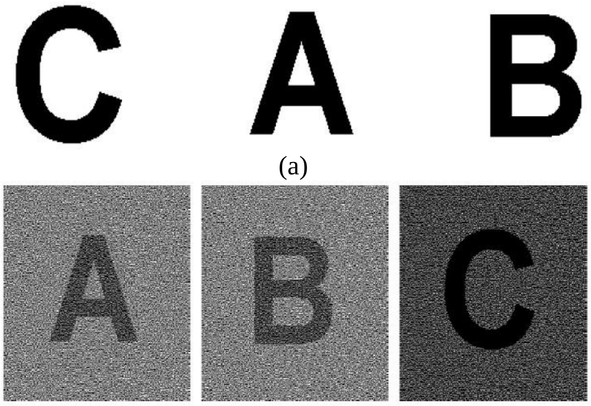
ii) Sharing multiple secret-Tzung-Her Chen anticipated a multi-secrets visual cryptography [22] which is extended from traditional visual secret sharing. The codebook of traditional visual secret sharing implemented to generate share images macro block by macro block in such a way that multiple secret images are turned into only two share images and decode all the secrets one by one by stacking two of share images in a way of shifting. This scheme can be used for multiple binary, gray and color secret images with pixel expansion of 4.

2. Extended visual cryptography:

Extended visual cryptography is an extended version of traditional visual cryptography in previous method the shares are in random form but in this extended visual cryptography the share are meaningful. After the set of shares are superimposed, the meaningful information disappears and the secret is recovered. This is the basis for the extended form of visual cryptography. Generally, a (k,n)-EVC scheme takes a secret image and n original images as input and produces n encrypted shares with approximation of original images that satisfy the following three conditions:

- In this any k no. of share out of n can recover the secret image;
- Secret cannot be obtain if any less than k share are obtained;
- All the shares are meaningful images; encrypted shares and the recovered secret image are colored.

Example [22] Fig. 4 provides an example of a (2, 2) EVCS. As can be seen from figure, two meaningful shares are generated from the base image. During this shares creation, the secret is encoded between each of the shares, after superimposing each share, the secret is completely recovered while the meaningful information on each share completely disappear.



(a)

(b)

Fig 6 . Result of (2,2) EVCS encryption process [22]

3. Halftone image visual cryptography

Halftone Visual Cryptography (HVC) is a type of extended Visual Cryptography which is a visual secret sharing scheme where image is encoded into meaningful Visual information taking Halftone shares. Halftone VC uses the density of the net dots to imitate the gray level is called “Halftone” [11] and transforms an image with gray level into a binary image before processing. In the gray-level image, every pixel of the image will be transformed into halftoned image that has only two possible colour levels (black or white). Because human eyes cannot identify too tiny printed dots and, when viewing tends to cover its nearby dots, we can simulate different gray levels through the density of printed dots, even though the transformed image actually has only two colours—black and white. Halftone visual cryptography is proposed to achieve visual cryptography via halftoning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares carrying significant visual information. The simulation shows that the visual quality of the obtained halftone shares is observably better than that attained by any available visual cryptography method known to date. In halftone visual cryptography a secret binary pixel ‘P’ is encoded into an array of Q1 x Q2 (‘m’ in basic model) sub pixels, referred to as halftone cell, in each of the ‘n’ shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. HVC also maintains contrast and security of the images.

4. Dot-size variant visual cryptography-

In Dot-size variant Visual Cryptography two extended style VC is generated, it seems like a normal random visual cryptography share, when the share is viewed. However, this scheme is designed with spatial filtering in mind; this is the dot size variant part of the scheme. Dot size variant means that instant of having single dot. This means that after printing, if the share is scanned or photocopied or even viewed with a mobile phone or digital black and white dots which makes up a VC share, we use a clustered of smaller dots to represent these black and white pixels. camera, the smaller dots in the scheme are altered.

5. Progressive visual cryptography

A technique that enables visual cryptography to be used on colour and greyscale images is developed in progressive colour Visual Cryptography [23]. Many techniques of visual cryptography degrade the quality of decoded image, which makes it unsuitable for digital media. The meaning of the progressive term refers to how the image is build. Example, downloading or viewing an image on a web page, the image is loaded in stage. The full dimension of the image is visible but it is very blurry. As more of the image is downloaded, the clearer the resulting image becomes, until it is fully loaded. Progressive visual cryptography (PVC) can be utilized to recover the secret image gradually by superimposing more and more shares. If we have a few pieces of shares, we could only get an outline of the secret image. The details of the hidden information can be revealed progressively, by increasing the number of the shares being stacked.

A progressive secret image sharing scheme that demonstrated when mores hares are stacked progressively, the recovery of the secret image will be clearer and clearer. They input a secret image which has been halftoned in advance, and then expand every pixel into a 2×2 block. If the pixel is black, it is expanded into a four fully black block; on the contrary, if the pixel is white, it is expanded into a two white and two black blocks arbitrarily. From the example given below as more shares are overlapped the image becomes clearer in a progressive manner.

Example

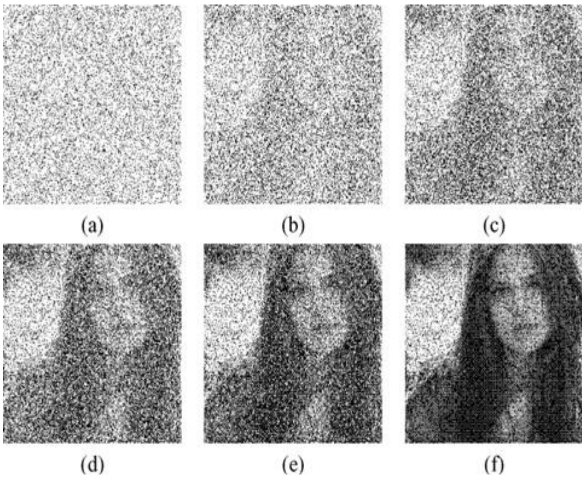


Fig. 7. Menais reconstructed by stacking different numbers of share Images.
(a)– (f) any 1–6 share images stacked [23].

6. Hierarchical visual cryptography.

Hierarchical visual cryptography encrypts the secret image in various levels. As the numbers of levels in hierarchical visual cryptography increases, its secrecy tends to increase. All shares generated are meaningless gives no information about secret image. The expansion ratio also reduced to 1:2 from 1:4. , hierarchical visual cryptography is a method it encrypt the image in no. of shares. Initially the secret is divided into two shares after that these two shares further divided into each two shares. 2. Further, among these four shares, any three shares are chosen to generate the key share. The superimposition of key share with the remaining share reveals the secret information. The superimposition is performed by X-OR operation. As the level of hierarchical visual cryptography increases the secrecy tends to increases.

- With the help of following formula we can find key share pixel value.

Key Shares pixels values 0 If sum of Si <=1
1 If sum of Si >1

Now, according to above two rules we can find all key share pixels values.

Table I. Truth Table Indicating Key Share Pixel Value [13]

S12	**S21**	**S22**	**Key share pixel values**
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Hierarchical visual cryptography encrypts the secret in number of levels. Initially the secret is divided into exactly two share called share 1 and share 2 as shown in fig 6. Each share is then encrypted independently resulting in four shares: share 11, share 12, share 21 and share 22. Later, among these four shares, any three shares are chosen to generate the key share. The superimposition of key share with the remaining share reveals the secret information. The superimposition is logically performed by the X-OR operation. As the level of encryption in hierarchical visual cryptography increases, the secrecy tends to increase. Figure 6 indicates the concept of hierarchical visual cryptography.

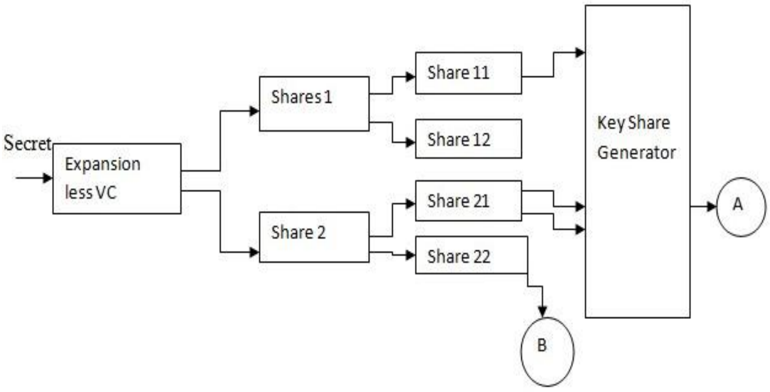


Fig. 8 Concept of hierarchical visual cryptography

Table II. Comparative Study Of Methods

S. NO.	METHOD NAME	GRAY/ COLOUR IMAGE	PIXELS EXPANSION	QUALITY
1.	TRADITIONAL VC	BINARY IMAGE	1:4	DEGRADED
2	EXTENDED VC	GRAY SCALE/COLOUR IMAGE	1:4	DEGRADED
3	HALFTONED VC	GRAY SCALE/COLOUR IMAGE	1:4	DEGRADED
4	PROGRESSIVE VC	GRAY SCALE/COLOUR IMAGE	1:1	SAME
5	HIERARCHICAL VC	GRAY SCALE/COLOUR IMAGE	1:2	DEGRADED

III. CONCLUSIONS

Visual Cryptography provides one of the secure method or ways to transfer images on the internet. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. This paper exploits various techniques of visual cryptography. The first approach is traditional visual cryptography which has been used in binary images only, but in this method the quality of image degrades. The extended visual cryptography provided meaningful shares hacker will not get any clue from these shares that there is any secret hidden behind the shares. Halftoned visual cryptography, this maintains the contrast and security of image. In progressive visual cryptography the image is obtained by increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively, but this method is not secure because if the hacker gets some shares than, the outline of image can be revealed . Last approach is hierarchical visual cryptography in this approach the image is divided into no. of levels as the no. of level increases secrecy tends to increase. This method can be used for authentication such as in biometrics, signature of user is scanned and applied as an input to the hierarchical visual cryptography. And can be combined with stenography for more robustness of image.

ACKNOWLEDGMENT

This research was supported by my faculty guide **Dr. Dhirendra Mishra** and by my mentor **Pallavi Halarnakar**. I am grateful to them for sharing their pearls of wisdom with me during the course of this research.

REFERENCES

[1] Revenkar, Pravin S., AnisaAnjum, and W. Z. Gandhare. "Survey of visual cryptography schemes." International Journal of Security and Its Applications4, no. 2 (2010): 49-56.

[2] Bandamneni, Lavanya, and V. Venkatra Rao. "Color Extended Visual cryptography Using Error Diffusion for High Visual Quality Shares."Internatisonal Journal of Electronics and Computer Science Engineering 1.3 (2012): 1176-1182.

[3] Mande, Anuprita, and Manish Tibdewal. "A Fast Encryption Algorithm for Color Extended Visual Cryptography." International Journal of Emerging Technology and Advanced Engineering 3.4 (2013)

[4] Zhou, Zhi, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography." Image Processing, IEEE Transactions on 15.8 (2006): 2441-2453.

[5] Kang, InKoo, Gonzalo R. Arce, and Heung-Kyu Lee. "Color extended visual cryptography using error diffusion." Image Processing, IEEE Transactions on20.1(2011): 132-145.

[6] Wang, Zhongmin, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography via error diffusion." Information Forensics and Security, IEEE Transactions on 4.3 (2009): 383-396.

[7] Anbarasi, L. Jani, M. Jenila Vincent, and GS Anandha Mala. "A novel visual secret sharing scheme for multiple secrets via error diffusion in halftone visual cryptography." Recent Trends in Information Technology (ICRTIT), 2011 International Conference on. IEEE, 2011.

[8] Weir, Jonathan, and Wei-Qi Yan. "Dot-size variant visual cryptography." Digital Watermarking. Springer Berlin Heidelberg, 2009. 136-148.

[9] Hou, Young-Chang, and Zen-Yu Quan. "Progressive visual cryptography with unexpanded shares." Circuits and Systems for Video Technology, IEEE Transactions on 21.11 (2011): 1760-1764.

[10] Yan, Xuehu, Shen Wang, and XiamuNiu. "Equivalence proof of two (2, n) progressive visual secret sharing." Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on. IEEE, 2014.

[11] Yan, Xuehu, Shen Wang, and XiamuNiu. "Equivalence proof of two (2, n) progressive visual secret sharing." Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on. IEEE, 2014.

[12] Chen, Tzung-Her, and Yao-Sheng Lee. "Yet another friendly progressive visual secret sharing scheme." Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on. IEEE, 2009.

[13] Chavan, Pallavi V., and Mohammad Atique. "Design of hierarchical visual cryptography." Engineering (NUiCONE), 2012 Nirma University International Conference on. IEEE, 2012.

[14] Chavan, Pallavi V., Mohammad Atique, and Anjali R. Mahajan. "An intelligent System for secured Authentication using Hierarchical Visual cryptography-review." ACEEE International Journal on Network Security 2.04 (2011).

[15] Kuri, MsMoushmee, and TanujaSarode. "Hierarchical Implementation of RKO Technique for Visual Cryptography."

[16] Moses, Timothy, and Adrian O. Mancini. "Method and system for notarizing digital signature data in a system employing cryptography based security." U.S. Patent No. 6,314,517. 6 Nov. 2001.

[17] Naor, Moni, and Adi Shamir. "Visual cryptography." Advances in Cryptology—EUROCRYPT'94. Springer Berlin Heidelberg, 1995.

[18] Nakajima, Mizuko, and Yasushi Yamaguchi. "Extended visual cryptography for natural images." (2002).

[19] Hou, Young-Chang. "Visual cryptography for color images." Pattern Recognition36.7 (2003): 1619-1629.

[20] Shyu, ShyongJian, et al. "Sharing multiple secrets in visual cryptography."Pattern Recognition 40.12 (2007): 3633-3651.

[21] Hou, Young-Chang. "Visual cryptography for color images." Pattern Recognition36.7 (2003): 1619-1629.

[22] Chen, Tzung-Her, and Kuang-Che Li. "Multi-image encryption by circular random grids." Information Sciences 189 (2012): 255-265.

[23] Hou, Young-Chang, and Zen-Yu Quan. "Progressive visual cryptography with unexpanded shares." Circuits and Systems for Video Technology, IEEE Transactions on 21.11 (2011): 1760-1764.

[24] Hsu, Chig-Sheng, and Young-Chang Hou. "Goal-programming-assisted visual cryptography method with unexpanded shadow images for general access structures." *Optical Engineering* 45.9 (2006): 097001-097001.