Journal of Advanced Research in Instrumentation and Control Engineering
Volume 8, Issue 3&4 - 2021, Pg. No. 6-15
Peer Reviewed Journal

Case Study

A Comprehensive Study of Secrets Sharing Schemes of Visual Cryptography and its Applications

DR Somwanshi[1], Vikas T Humbe[2]

[1]Department of Computer Science, College of Computer Science and Information Technology (COCSIT) Latur, Maharashtra, India.
[2]School of Technology, Swami Ramanand Teerth Marathwada University Nanded, Sub-Center, Latur, Maharashtra, India.

I N F O

Corresponding Author:
DR Somwanshi, Department of Computer Science, College of Computer Science and Information Technology (COCSIT) Latur, Maharashtra, India.
E-mail Id:
somwanshi1234@gmail.com
How to cite this article:
Somwanshi DR, Humbe VT. A Comprehensive Study of Secrets Sharing Schemes of Visual Cryptography and its Applications. *J Adv Res Instru Control Engg* 2021; 8(3&4): 6-15.

Date of Submission: 2021-11-30
Date of Acceptance: 2021-12-20

A B S T R A C T

Visual Cryptography is a special cryptographic technique in which encryption of visual information such as pictures, drawing, graphs, written materials etc. is performed in such a way that the decryption can be performed by the human visual system. Visual cryptography is specially designed for data security or providing a more secure method for allowing access to more sensitive data. It is simply used for user authentication for providing access to data. Recently many methods and techniques have been developed for the visual cryptography schemes. This paper aims to explore the extensive review and to study the various visual cryptography schemes and also to analyze the performance of different visual cryptographic schemes. Different secret sharing schemes of visual cryptography such as Halftone Visual cryptography, Color Visual Cryptography, Visual Cryptography with Perfect Restoration, Multi-resolution Visual Cryptography and Progressive Multi-resolution Visual Cryptography etc. are elaborated and presented the merits and demerits of each type of cryptography schemes. With this number of secret share images, image format and type of share generated using each type of cryptography is discussed. Different problems of visual cryptography schemes such as pixel expansion, contrast mapping flipping issue, cheating prevention etc. are also discussed. Finally different applications of visual cryptography are illustrated and presented as the guidelines for future research.

Keywords: Visual Cryptography Scheme (VCS), Halftone Visual Cryptography, Color Visual Cryptography, Pixel Expansion, Contrast, Secret Sharing, Cheating Prevention

Introduction

Visual Cryptography (VC) is a technique of encrypting the visual information, written material such as printed text, handwritten notes, images etc. in a perfectly secure way and which can be decoded directly by human visual system.[1] It means decryption is not required or huge amounts of calculation are not required to decrypt the text. This allows everybody to make use of the system, even if they don't have sufficient knowledge about encryption or decryption of cryptography and fail to carry out any computations.

Initially this technique was first pioneered by Naor et al.[1] in 1994. In this technique the message or image data to be

protected or encrypted is divided into n different parts or shares. Each part or share is circulated among the n different users and then we can specify at least k shares from the n shares are required to get the original information. The k-1 shares cannot be used to produce the original message. For example suppose there are six thieves, who wanted to share a bank account, but they don't trust one another, and they divided up the password for the account in such a way that any three or more thieves working together can have access to the account, but not less than three thieves can access the account.

In Visual Cryptography each and every pixel of the original images is distributed into minor parts. There must be the same number white and black parts or blocks. If the pixel in the original image is divided into two parts then there will be one black and one white block. If the pixel in the original image is divided into four equal parts, then there will be two black and two white blocks.[1-4] In example Figure 1, each pixel in the original image is divided into two parts called share 1 and share 2. Combining or staking the two shares share 1 and share 2 reveals or generates the original image.

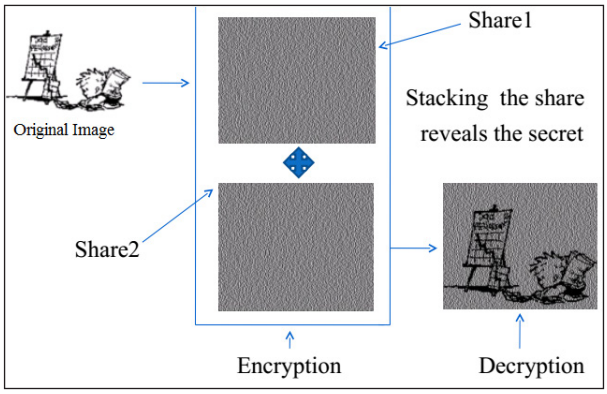

Figure 1.Visual Cryptography Scheme

Visual Cryptography Schemes

There are a number of visual cryptography schemes that are already developed for specific types of applications. Numbers of schemes can be developed in future to overcome some of the problems of visual cryptography. The visual cryptography schemes can also be called secret sharing schemes. This section discusses different types of schemes of visual cryptography.

The original secret image is divided into 2 parts or shares in (2,2) Visual Cryptography Scheme. A 2 or 4 subpixel non-overlapping blocks are used in each shared image to represent each pixel of the original image. Anyone, having only one share will not be able to extract secret information from the available share. Both the shares are required and which need to be used in superimposition to extract the original secret image.[1]

For encoding the pixel of the original image many different techniques have been developed so far. In one of the technique, for each pixel in original image, two sub-pixels are represented in each shares, while reading the pixels one after another from the original image, if a pixel encountered is white then, one of the first two rows in Table 1, is selected with probability of 0.5 and the shares are assigned 2 pixel blocks as shown in the third and fourth columns represented in Table 1. Similarly, if a pixel encountered is black then, one of the last two rows is selected with probability of 0.5, from which a sub-pixel block is assigned to each share. When two shares are superimposed, if two white pixels overlap, the resultant pixel will be white and if a black pixel in one share overlaps with either a white or black pixel in another share, the resultant pixel will be black. This suggests that the superimposition of the shares can be represented by the Boolean OR operation. When the sub-pixels of both the shares in the third and fourth columns in Table 1, are superimposed[1] then the last column shows the resulting sub-pixel.

Table 1.Visual Cryptography Scheme

Original Pixel	Probability	Share 1 Sub-Pixel	Share 2 Sub-Pixel	Share 1 || Share 2
	0.5			
	0.5			
	0.5			
	0.5			

In (2, 2) visual cryptography, both the shares are needed to extract the secret information. If one share gets lost due to some technical problem, secret information cannot be revealed. So there is a need to secure all the shares for revealing the secret information and users cannot bear the loss of a single share. To give some flexibility to users, the basic model of visual cryptography is proposed by Naor and Shamir and which can be generalized into a visual alternative of k out of n visual cryptography scheme.[1] In (k, n) visual cryptography schemes, n shares can be generated from the original image and distributed among users. Original image can only be revealed if k or more shares are stacked together, where the value of k is between 2 to n. If fewer than k shares are stacked together, the original image cannot be reconstructed.

It gives flexibility to the user that if a user loses some of the shares still secret information can be reconstructed, if at least k number of shares is available.

Visual Cryptography Scheme for General Access Structure

As we are familiar that all n shares have equal importance, in (k, n) visual cryptography scheme. Any k out of n shares can be used to reconstruct the secret information. It may affect the security of the system. To get control of this

problem, G Ateniese, C Blundo, A DeSantis and DR Stinson extended (k, n) model of visual cryptography to general access structure.[10] In the general access structure scheme, the created sets of n shares are divided into two sub parts called qualified and forbidden subparts of shares as per the importance of shares. Any k shares from a qualified subpart of shares can reconstruct the secret information, but less than k shares from a qualified subpart of shares cannot reconstruct any secret information. Even k or more shares from forbidden subparts cannot reconstruct the secret image. So, Visual cryptography, especially for general access structure, improves the security of the system.

Recursive Threshold Visual Cryptography Scheme

In (k, n) visual secret sharing scheme, a secret of "b" bits is shared among "n" shares of size at least "b" bits each. Then any k from n shares are needed to reconstruct the original a secret image, it means each and every bit of any shares carres at most 1/ k bits of secret. It produces inefficient results in terms of the number of bits of secret carried per bit of shares. To provide the solution to this problem, AbhishekParakh and SubhashKak proposed the "Recursive threshold visual cryptography".[11] The main idea behind this is, it recursively hides smaller secrets information into shares of larger secrets information with secret sizes becomes double in every step and therefore it increases the information, every bit of share carries to (n-1)/ n bit of secret which is nearly 100%.

Halftone Visual Cryptography Scheme

Halftone visual cryptography processes the halftone image, an image made up of a series of dots instead of continuous tone is called halftone image. Series of dots in the halftone image can be of different colors, different sizes, and different shapes. Larger dots in image are used to represent darker more dense areas of the image, whereas smaller dots are used for lighter areas in image.[4]

Halftone image, image Illustration, shares of image and final image after superimposing are illustrated in Figure 2, 3 and 4 respectively.

Figure 2.Halftone Image

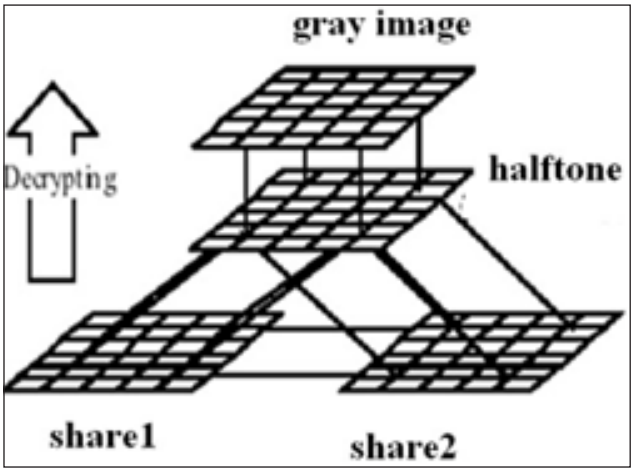

Figure 3.Halftone Image Illustration

Figure 4.Halftone Gray-Scale Image

Stacking or superimposing of shares can be performed using OR, XOR and many other operations.

Zhi Zhou et al.[5] first proposed an inventive technique called halftone visual cryptography to achieve visual cryptography via half-toning. The method proposed by them is based on the principles called blue-noise dithering, this technique uses the cluster and void algorithm for encoding an original secret image which is in binary form, into halftone shares (images) which carries the remarkable visual information. The simulation proposed by them shows that the quality of the resultant halftone shares is remarkably better than that of any other available visual cryptography method.

Zhongmin Wang et al.[6] works on Halftone Visual Cryptography using error diffusion technique. In their method the secret image is concurrently embedded into binary valued shares while these shares are halftoned by error diffusion the workhorse standard of halftoning algorithms. Error diffusion of methods proposed have very little complexity and provide halftone shares with better

quality of the image. By the superimposition of qualified shares together, the original secret image is formed and which does not suffer from hybrid intervention of share images.

Halftone visual cryptography uses halftoning technique to create shares. Halftone is the reprographic technique. It replicates continuous tone images in the form of dots, those dots may differ in either shape, size, or in spacing. In halftone visual cryptography a secret binary pixels of the image is converted or represented in the form of an array of sub pixels, in each of the "n" shares, which is called a halftone cell. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. It keeps good contrast and security of the image shares and also increases the visual quality of the shares.

Visual Cryptography Scheme for Gray Images

This type of scheme is mainly designed to work with gray levels of image. All the schemes which were introduced before this scheme only work on or capable of processing the black and white image or binary images. These were not sufficient for solving real life problems. Chang-Chou Lin, WenHsiang Tsai initiated the visual cryptography scheme for gray level images.[12] This scheme mainly uses the dithering technique for conversion of gray level image into equivalent binary image. Once conversion of image is done the scheme uses existing visual cryptography schemes for binary images for creation of the shares.

Visual Cryptography Scheme for Color Images

Color Visual Cryptography

Visual Cryptography that processes the color images and works with color models and color channels for creating shares is called color visual cryptography. In this visual cryptography color decomposition of color channels in color image are performed and then the gray scale half toning for each channel is performed or the color halftoning first followed by the Color decomposition is performed.[4]

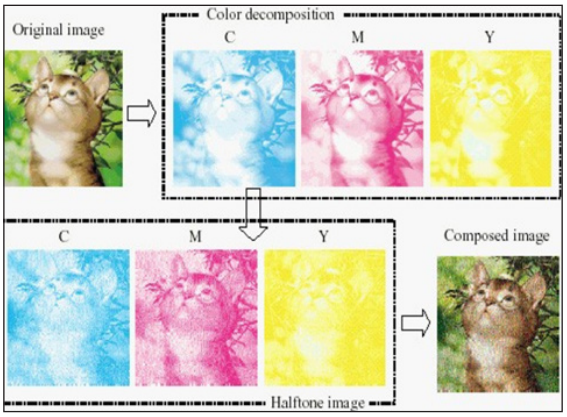

Figure 5.Color Decomposition in Color Visual Cryptography

Young-Chang Hou[2] works on Color visual cryptography and proposes three methods for visual cryptography of gray-level and color images these are: 1) black and white visual cryptography, 2) halftone technology, 3) the color decomposition method. Their method also preserves the benefits of black-and-white visual cryptography scheme, which make use of the human visual system to decrypt the original secret images without any computation and also provides the backward compatibility with the previous results in black-and-white visual cryptography scheme, such as the t out of n threshold scheme. Figure 5, Shows the Color decomposition in color visual cryptography.

Cyan(C), Magenta (M) and Yellow(Y) components can be extracted from color images if the image is made up of these three components. Each component can be used for creating shares, if shares and color components are stacked together then the final image will be extracted.

Visual cryptography schemes were applied to only black and white images till 1997. Verheul and Van Tilborg have developed the first color visual cryptography scheme for processing the color image.[13] In this visual cryptography scheme one pixel in the original image is represented intom sub pixels, and each sub pixel is divided or represented into c color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black.

F Liu, CK Wu, XJ Lin proposed a new approach for colored visual cryptography schemes.[14] They proposed three different approaches for color image representation:

In their first approach, colors in the secret image can be printed on the shares directly. It works similar to the basic visual cryptography model. Limitations of this approach are large pixel expansion and quality of decoded image is degraded.

In their second approach they have used the separate three color channels. These are Red, green, blue for additive model and cyan, magenta, yellow for subtractive model. Then a regular visual cryptography scheme for black and white images is applied to each of the color channels that is used. This approach eliminates the pixel expansion problems but quality of image gets degraded due to the half toning process.

In their third approach, binary representation of color of a pixel is used and the secret image is encrypted at bit-level, this results in better quality of image.

Visual Cryptography with Perfect Restoration

The half toning method used in halftone visual cryptography reduces or degrades the original quality of the secret image. In Visual Cryptography with perfect restoration both gray level and color images are decoded or decrypted without degradation. It also keeps up the benefits of traditional

visual cryptography. Superimposition of all the shares is performed only by using XOR operation with this visual cryptography.[3,4] Figure 6, Illustrate the idea of Visual Cryptography with perfect restoration.

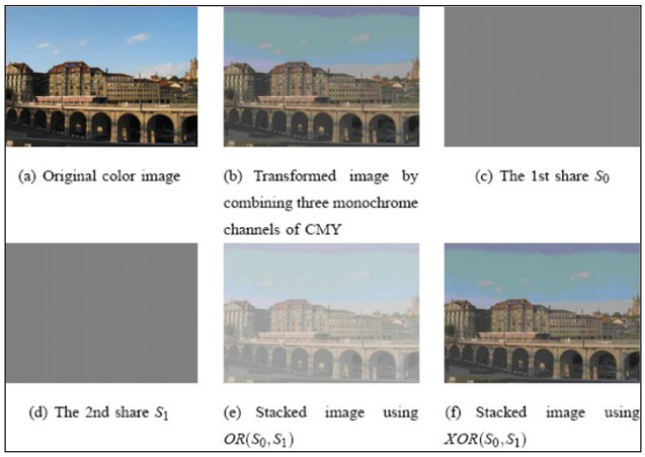

Figure 6.Visual Cryptography with Perfect Restoration

VandanaPurushothaman and SreelaSreedhar work on pixel expansion and poor image quality. They introduce the effective technique of share generation based on XOR-based visual cryptography for General Access Structures and succeed in Perfect restoration of the secret, no pixel expansion and no code book requirement is needed and they finally use generated shares to cover in an image using steganography which provides additional security.[7]

Multi-resolution Visual Cryptography

Multi-resolution Visual Cryptography allows improving the resolution of superimposed image and can superimpose images of unpredictable quality or of variable three-dimensional resolutions. In regular (k;n) visual cryptography, if the k number of shares are available and that are used then the image of single resolution is formed. In Multi-resolution Visual Cryptography superimposing the threshold number of shares together, a reconstructed image is formed and final image resolution is enhanced using other shares.[4] Figure 7, shows the multi-resolution visual cryptography.

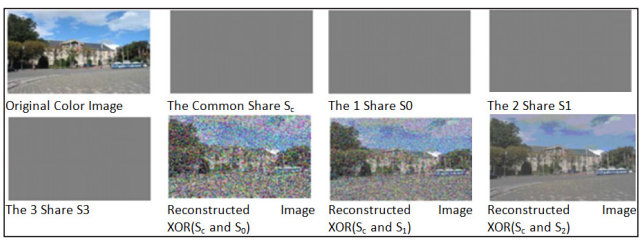

Figure 7.Multi-resolution Visual Cryptography

Jin et al., proposed a multi-resolution approach to share secret images that can be applied. They expand pixels to 3×3 blocks in which eight of them are used to represent the gray value of each pixel and the remaining one is used to store the halftone value of the secret image. In order to take advantage of visual effects, Jin et al., uses a "lookup table" to adjust the pixel value so that pixels with a larger gray value in the secret image own more "1"s (1 represents black) in its eight bit-planes. The adjusted eight binary digits are handled by conventional VC, therefore, an obscure secret image can be directly obtained from stacking shares. Their method expands every secret pixel to a 3×3 block, and by using the pixel-expansion scheme, their shares will be further expanded to 6×6 times larger, which causes a severe waste of storage and transmission time.[8]

Multiple Secret Sharing Scheme

All the previous research in visual cryptography was focused on securing only one image at a time. Wu and Chen[15] were first researchers, who developed a visual cryptography scheme to share two secret images in two shares. In this scheme, two secret binary images can be hidden into two random shares, namely A and B, such that the first secret can be seen by stacking the two shares, denoted by A, B, and the second secret can be obtained by rotating A by 90 degree anti-clockwise. Shyu, Tzung-Her Chen and Chang-Sian Wu[16,17] proposed a scheme for multiple secrets sharing in visual cryptography, where more than two secret images can be secured at a time in two shares.

Extended Visual Cryptography Scheme

In traditional visual cryptography schemes, shares are created as random patterns of pixels. These shares look like a noise. Noise-like shares arouse the attention of hackers, as hackers may suspect that some data is encrypted in these noise-like images. So it becomes prone to security related issues. It also becomes difficult to manage noise-like shares, as all shares look alike. Nakajima, M. and Yamaguchi, Y, developed Extended visual cryptography scheme (EVCS)[18] An Extended Visual Cryptography (EVC) provide techniques to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in traditional visual cryptography.

Progressive Visual Cryptography Scheme

In (k, n) visual secret sharing scheme, it is not possible to recover the secret image though one less than k shares are available. This problem is solved in progressive visual cryptography scheme developed by D Jin, WQ Yan and MS Kankanhalli.[8] In progressive visual cryptography scheme, it is not necessary to have at least k shares out of n, as in (k, n) secret sharing scheme. If more than one share is obtained, it starts recovering the secret image gradually. The quality of recovered images improves, as the number of shares received increases.

Progressive Multi-resolution Visual Cryptography

In Progressive Multi-resolution Visual Cryptography

(PMRVC), the shares are ordered and merged in such a way that if more shares are used, then the spatial resolution of the reconstructed image will be bigger. A (n, n) - PMRVCS is defined as: Let I be the original image, S_0, S_1...S_n are the shares created. For k =1, 2..., n-1, image I^k can be reconstructed by merging S_0, S_1.....S_k.[3,4]

Young-Chang Hou and Zen-Yu Quan work on Progressive Visual Cryptography and proposed a brand new sharing scheme of progressive VC to produce pixel unexpanded shares. In their research, the possibility for either black or white pixels of the secret image to appear as black pixels on the shares is the same, which approximates to 1/ n. Therefore, no one can obtain any hidden information from a single share, hence they ensure security. When superimposing k (sheets of share), the possibility for the white pixels being stacked into black pixels remains 1/ n, while the possibility rises to k/ n for the black pixels, which sharpens the contrast of the stacked image and the hidden information, therefore, becomes more and more obvious. After superimposing all of the shares, the contrast rises to (n - 1)/n which is apparently better than the traditional ways that can only obtain 50% of contrast, consequently, a clearer recovered image can be achieved.[9]

Region Incrementing Visual Cryptography Scheme

In traditional visual cryptography schemes, one whole image is considered as a single secret and the same encoding rule is applied for all pixels of one image. So it reveals either the entire image or nothing. It may be the situation that different regions in one image can have different secrecy levels, so we can't apply the same encoding rule to all pixels. Ran-Zan Wang[19] developed a scheme "Region Incrementing Visual Cryptography" for sharing visual secrets of multiple secrecy levels in a single image. In this scheme, different regions are made of a single image, based on secrecy level and different encoding rules are applied to these regions.

Segment based Visual Cryptography Scheme

Traditional visual cryptography schemes were designed to work on pixels in an input image. The problems occurring in this type of visual cryptography scheme is that there is a loss in contrast to the reconstructed image. Loss in contrast leads to pixel expansion. To overcome this problem Bernd Borchert[20] proposed the new scheme called segment based visual cryptography scheme. They suggested that it is useful to encrypt messages consisting of symbols represented by a segment display. For example, the decimal digits 0, 1, ..9 can be represented by a seven-segment display. The advantage of the segment-based encryption is that, it may be easier to adjust the secret images and the symbols are potentially easier to recognize for the human eye and it may be easier for a non-expert human user of an encryption system to understand the working.

Various Problems in Visual Cryptography

Alignment Problems

Pixel expansion is a crucial parameter for Visual Cryptography Schemes (VCS).[1] However, most research in literature is based on reducing pixel expansion in an image at pixel level[2], i.e., to reduce the number of sub pixels that are used to represent a pixel in the original secret image. It is quite insufficient since the final size of the transparencies of the VCS is affected not only by the number of the subpixels, but also by size of the subpixels in the transparencies. However, reducing the size of the subpixels in transparencies is due to difficulties of the transparencies alignment.[1,21] Final goal of reducing the pixel expansion is to shorten the size of the transparencies that are distributed to the participants,[21] because smaller transparencies are easier to be transported. However, the sub pixels that are printed on the transparencies affect the final size of the transparencies; in fact, size of the transparencies is the product of size of the subpixels and number of the subpixels in each transparency. When the sub pixel size is large, it is easy to align the shares, but large sub pixel size will lead to large transparencies. On the other hand, when the sub pixel size is small, it is relatively hard to align the shares. From the viewpoint of VCS participants, the goal is to align the shares easily and have small transparencies as well.[21]

Visual Cryptography Scheme Cheating Prevention

While superimposing the shares to recover the original image we need to verify the authenticity of the shares presented for superimposition. there may be the difference between the presented shares and the actual shares that are distributed. the shares may be tempered malformed or changed by a cheater or participants themselves and we may not be aware about this.

Cheating Intensive Visual Cryptography Scheme (CIVCS) are designed to avoid cheating problems when the secret image from the shares are to be recovered. However, the scheme CIVCS have some drawbacks such as: the scheme needs an online trusted authority or it requires additional shares for the purpose of verification, or it has to sacrifice the properties by means of pixel expansion and contrast reduction of the original scheme[21] or it may only be based on such type f schemes with specific access structures. For cheating or breaking the schems developed, the cheaters present some duplicate, tampered or fake shares so that the stacking of fake and original shares together reconstructs the a fake image and the victims who cannot detect the cheating activities will be fooled to believe that the recovered fake image is the genuine secret image. This is terrible because the secret image is usually important to the victims. Many studies focused

on the cheating problems in VCS and consequently many Cheating Immune Visual Cryptography Schemes (CIVCS) have been proposed. We classify the techniques in these CIVCSs as follows:[21]

- Make use of an online trusted authority who can verify the authenticity of the shares presented for superimpositions
- Extra verification shares can be generated to verify the genuineness of the stacked shares
- Expand the shared image pixel expansion to add the extra authentication information about the shares
- More than n shares need to be generated to reduce the possibility that the cheaters can correctly guess the distribution of the victims' shares
- Make use of the genetic algorithm to encrypt homogeneous secret images

Flipping Issues in VCS

When superimposing or reconstructing the original image from created shares, direction and placement of the shares is important. If this is not maintained properly, the original image will not recover properly so the flipping issue may arreges. Most of the schemes developed so far are dependent on the direction and placement of the shares, so there is a need of maining the proper direction and placement of the shares while superimposing the shares.[21]

Distortion Problems

For Visual Cryptography Scheme (VCS),[1,21] normally, the size of the recovered secret image is increased by m (≥ 1) times of the original secret image.

In most of the cases, m is not a square number, therefore the recovered secret image is distorted. Sometimes, m is too large that will be inconvenient for the participants to carry the shared images.

Zheng D et al.,[22] introduces a new visual cryptography scheme which imitates the principle of fountains. The two important advantages of the scheme are: non-distortion and flexibility (with respect to the pixel expansion). Furthermore, the presented scheme can be applied to any VCS that is under the pixel by pixel encryption model,[22] such as VCS for general access structure, color VCS and extended VCS. In general, the recovered secret image of VCS will be expanded by (≥ 1) times over the size of the original secret image i.e., the size is m. However in most cases, m is not a square number, therefore the image recovered will be distorted.[22]

Thin Line Problems (TLP)

Traditionally, the size invariant visual cryptography schemes (SIVCS's) are only suitable to encrypt coarse secret images that do not contain much detailed information. The reason is that, SIVCS can only recover the secret image from an overall view point; each secret pixel can only be correctly represented with a certain probability in the recovered secret image. In such a case the thin lines, in the secret image, are usually unclear and misrepresented in the recovered secret image of SIVCS, where we call such phenomena the Thin Line Problem (TLP).[21]

Feng Liu et al.,[23] proposed two multi-pixel encryption size invariant visual cryptography schemes (ME-SIVCS's) which improve the visual quality of the recovered secret image by reducing the variance of the darkness levels.

In addition to the proposed ME-SIVCS's, they also introduced a scheme for encrypting fine secret images and this scheme elimited the thin line problems.[23]

Applications of Visual Cryptography

Biometric Security

For providing security to the biometric system such as figure print recognition, face recognition etc. visual cryptography secret sharing schemes are now widely used. For providing security to figure print recognition, the original figure print image is divided into two or more shares and when two shares are combined together the resultant image is formed and then the user is recognized.

Arun Ross, Asem Othman[24] works on Visual Cryptography for Biometric Privacy and the suggested a technique for using visual cryptography for providing privacy to biometric models. They work on the fingerprints and iris, in that the templates are divided into two noise-like images using (2, 2) VCS and since the spatial arrangement of the pixels in these images varies from block to block, it is impossible to recover the original image template without using both the two shares. The XOR operation is used to reconstruct and recover the original image from two noisy images.[24]

Watermarking

Visual Cryptography scheme is also used for digital watermarking, this process involves two phases: watermarks embedding in documents and watermarks retrieving from documents. In watermark embedding, watermark is split into two shares, one share is kept with the owner and another share and host image is kept together. To authorize the original image, one share is extracted from the image, and this share is combined with the owner's share and the original image is formed.[25]

Yuh-rauwang et al.,[26] works on lossless watermarking using visual cryptography, and presented that watermark can be recognized visually by overlapping the printout transparencies of share I and share 2 images. They used public image to get share I image and generate the secret (i.e., watermark) image using owner (i.e., share 2) image.

Steganography

Hiding one message inside another, so the hidden

message will not be detected by the causal eye, is the art of steganography. Text, image, video and audio are used to protect media for hiding actual data in steganography.[27]

In the method proposed by Souvik Roy and P Venkateswaran,[28] a customer password for unique authentication provided by a bank application is hidden inside a cover text using the text based steganography method. Customer authentication information such as account number in connection with the merchant is placed over the cover text in its original form then a snapshot of two texts is taken. From the snapshot image, two shares are generated using visual cryptography and then authentication is performed using text steganography and visual cryptography.

Printing and Scanning Applications

In printing and scanning application of visual cryptography, the shares of visual cryptography are printed in paper on transparencies, after scanning the spare printed on paper it is superimposed with the owner's shares. However, it is not that easy to do an accurate superposition because of fine resolution and as well as printing noise. So there is a scope of improving the visual cryptography result. Wei-Qi Yan et al.,[29] works on Visual Cryptography for Print and Scan Applications, in that they considers the problem of exact alignment of printed and scanned visual cryptography shares.

Bank Customer Identification

Visual Cryptography can also be used for bank customer identification, for that signature of the customer such as password, fingerprint or photo is taken as input and is divided into different numbers of shares depending upon the bank's scheme. One share of the signature is preserved in the bank database and all other shares are given to the applicant. The customer needs to provide his shares for each transaction and those shares are superimposed with the share already existing in the bank and final authentication for the transactions is performed. Various techniques are used for this purpose. B Srikanth et al.,[30] works on Secured Bank Authentication using Image Processing and Visual Cryptography and uses the correlation for matching the share for transaction.

Anti-Phishing Systems

User authentication data such as security pins numbers, credit and debit card numbers and passwords are important information and can be theft by unauthorized users. Phishing is basically stealing secret credential from their owners. To provide the security for the phishing attacks Cryptographytechniques can be more useful. By superimposing the two shares, one received from the server site and second from his own share, the user can ensure the information on the website without phishing.[36]

Human Machine Identification

Human machine identification using visual cryptography can be performed. Kim M et al.,[36] works on Human-machine identification using visual cryptography and proposes desired property of decoding concealed images without any computationally expensive cryptographic operations

Defense System

To provide security to sensitive information in defense systems, visual cryptographic schemes can be used.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)

CAPTCHA is a technique for authentication, which can be supported by visual cryptography. It involves three steps: Share creation process, Hash Code generation and authentication process.

Offline QR Code Authorization

QR code (Quick Response Code) is the symbol for a type of matrix barcode. It is a machine-readable optical label that contains information about the item to which it is attached. It allows users to redirectto a particular page once the QR code is scanned. Visual cryptography based QR codes authentication mechanism can be used. It checks the identity accessing the QR codes and to control the permission to the protected data. Wen-Pinn Fang[37] works on Offline QR Code Authorization Based on Visual Cryptography and proposes an offline authentication mechanism for QR codes based on the technology of visual cryptography. They show that it is possible to check the identity accessing the QR codes and to control the permission to the protected data.

Electronic Voting System

Corporate companies conduct their elections for different posts such as the constitutional election, manager election etc. The branches of the companies may be situated in different parts of the country or the world the elections can be conducted easily and effectively in a proper manner by using Internet based voting system using visual cryptography. Voter can vote from anywhere using his share provided by a visual cryptography scheme.35 With this visual cryptography can be used for a variety of other applications also.

Conclusion

Information shared between the people over networks requires high security, providing security to the information that is shared is an important problem. From the inception of Visual Security in 1994 many types of visual cryptography ranging from Halftone visual cryptography, tp Progressive multi-resolution visual cryptography and different types of visual cryptographic scheme from (2, 2) to segment

based visual cryptography scheme have been developed. With this many types of visual cryptography models such as black and white to color images and random dot like shares to meaningful shares are being used to provide security over the network. Different researches are carried out for this, still there is much scope to do research in color visual cryptography and multiple secrets sharing schemes, progressive visual cryptography, Region Incrementing Visual Cryptography and Segment based Visual Cryptography Scheme and overcome the common limitations of these techniques like large pixel expansion and lower contrast. Comparative study of different cryptography techniques is carried out in this paper and finally different application areas of visual cryptography are presented.

References

1. Naor M, Shamir A. Visual Cryptography Eurocrypt, 1994.
2. Young-Chang H. Visual cryptography for color images Pattern Recognition. *Journal of the Pattern Recognition Society* 2002; 36: 1619-1629.
3. Weir J, Qi Y. Visual Cryptography and its Application. Ventus Publishing Aps, eBook. 2012; 1-144.
4. Moraru E. Visual Cryptography. Published in: Technology, Art & Photos on Slide share. 2008; 1-38.
5. Zhi Z, Arce GR, CrescenzoGD. Halftone Visual Cryptography. *Image Processing* 2006; 15(8): 2241-2453.
6. Wang Z. Student Member, IEEE, Gonzalo R Arce, Fellow, IEEE, and Giovanni Di Crescenzo. Halftone Visual Cryptography via Error Diffusion. *IEEE Transactions on Information Forensics and Security* 2009; 4(3): 383-396.
7. Purushothaman V, Sreedhar S. An improved secret sharing using XOR-based Visual Cryptography, Green Engineering and Technologies (IC-GET). Online International Conference, 2016.
8. Jin D, Yan WQ, Kankanhalli MS. Progressive color visual cryptography. *Journal of Electron Imaging* 2005; 14(3): 1-13.
9. Young-Chang H, Zen-Yu Q. Progressive Visual Cryptography with Unexpanded Shares. *IEEE Transactions on Circuits and Systems for Video Technology* 2011; 21(11): 1760-1764.
10. Chang-Chou L, Wen-Hsiang T. Visual cryptography for graylevel images by dithering techniques. *Pattern Recognition Letters* 2003; 24: 1-3.
11. Verheuland E, Tilborg HV. Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes. *Designs, Codes and Cryptography* 1997; 11(2): 179-196.
12. Liu F, Wu CK, Lin XJ. Colour Visual Cryptography Schemes. *IET Information Security* 2009; 2(4): 151-165.
13. Wu CC, Chen LH. A Study On Visual Cryptography. Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, ROC, 1998.
14. Shyu SJ, Huanga SY, Lee YK et al. Sharing multiple secrets in visual cryptography. *Pattern Recognition* 2007; 40(12): 3633-3651.
15. Tzung-Her CN, Chang-Sian W. Efficient multi-secret image sharing based on Boolean operations. *Signal Processing* 2011; 91(1): 90-97.
16. Nakajima M, Yamaguchi Y. Extended visual cryptography for natural images. *Journal of WSCG* 2002; 10: 303-310.
17. Wang RZ. Region Incrementing Visual Cryptography. *SP Letters* 2009; 16(8): 659-662.
18. Borchert B. Segment-based Visual Cryptography.
19. Feng L, Wei Q. Visual Cryptography for Image Processing and Security Theory, Methods and Applications Springer, eBooks, 2014; 1-154.
20. Zheng D, Zhao Y, Wang J. An efficient method of license plate location. *Pattern Recognition Letter* 2005; 26(15): 2431-2438.
21. Feng L, Tengguo, Kun Wu C et al. Improving the visual quality of size invariant visual cryptography scheme. *Elsevier Journal of Visual communication Image* 2012; 23: 331-342.
22. Ross A, Othman A. Visual Cryptography for Biometric Privacy. *IEEE Transactions on Information Forensics and Security* 2011; 6(1): 70-82.
23. Yuh-Rau W, Wei-Hung L, Ling Y. Lossless Watermarking Using Visual Cryptography Authentication. Proceedings of the International Conference on Machine Learning and Cyberetics, Tianjin, IEEE. 2013; 1109-1113.
24. Brassil J, Steven L, Nicholas M et al. Hiding Information in Document Images. Proceedings of the Conference on Information Sciences and Systems, Johns Hopkins University. 1995; 482-489.
25. Wei-Qi Y, Duo J, Kankanhalli MS. Visual Cryptography For Print And Scan Applications. *ISCAS* 2004; 572-575.
26. Srikanth B, Padmaja G, Khasim S et al. Secured Bank Authentication using Image Processing and Visual Cryptography. *International Journal of Computer Science and Information Technologies* 2014; 5(2): 2432-2437.
27. Rose A, Thampi SM. A Secure Verifiable Scheme for Secret Image Sharing. *Procedia Computer Science* 2015; 58: 140-150.
28. Hodeish ME, Humbe VT. An Optimal (k,n)Visual Secret Sharing Scheme for Information Security. *Elsevier-Procedia Computer Science* 2016; 93: 760-767.
29. Dahata AV, Chavan PV. Secret Sharing Based Visual Cryptography Scheme Using CMY Color Space. *Elsevier, Procedia Computer Science* 2016; 78: 563-570.
30. Rajendra AB, Sheshadri HS. Visual Cryptography in Internet Voting System. *IEEE* 2013; 60-64.
31. Kim M, Park J, Zheng Y. Human-machine identification using visual cryptography. Proceedings of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems. 1998; 178-182.

32. Wen-Pinn F. Offline QR Code Authorization Based on Visual Cryptography. IEEE Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Seventh International Conference. 2011; 89-92.
33. Shivendra S, Agarwal S. VPVC: verifiable progressive visual cryptography. *Springer-Pattern Anal Application* 2016; 1-28. https://doi.org/10.1007/s10044-016-0571-x
34. Shivendra S. VMVC: Verifiable multi-tone visual cryptography. Springer, Multimed Tools Application. https://doi.org/10.1007/s11042-017-4422-6
35. Hodeish ME, Humbe VT. An Optimized Halftone Visual Cryptography Scheme using Error Diffusion. *Springer, Multimed Tools Application* 2018; 1-17.
36. Hodeish ME, Humbe VT. State-of-the-Art Visual Cryptography Schemes. *International Journal of Electronics Communication and Computer Engineering* 2014; 5(2): 412-420.