International Journal of Engineering &Technology, 7 (3.12) (2018) 374-379

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Emerging Trends in Visual Secret Sharing

Mainejar Yadav[1], Ranvijay[2]

[1,2]Computer science and engineering department
Motilal Nehru national institute of technology ALLAHABAD, INDIA
**Corresponding Author Email: [1]rahulit1210@gmail.com, [2]ranvijay@mnnit.ac.in*

Abstract

Visual Secret Sharing (VSS) is an increased applicability of traditional secret sharing. In VSS, the secret information is recovered by human visual system or lightweight computational device. There are two models available in VSS, one is Visual Cryptography (VC) which is introduced by Naor's in 1994 and other is a Random Grid (RG) based VSS which is proposed by Keren and Kafri. This state of the art covers both the models of VSS along with its application. The various application areas of VSS are visual authentication and identification, image encryption, access control, data hiding etc. The chapter has also covered various future enhancements in VC based on cryptanalysis, optimal pixel expansion, multiple secret encoding, progressive VC etc. Random Grid based VSS have some advantages over VC, which eliminates the need of Pixel expansion and codebook. But still, there is scope for the improvements in the contrast and the complexity of exiting algorithms. So there are various challenges and opportunities which make it an exciting research area to work upon.

Keywords: *Cheating, Essential participants, General access structure, Meaningful share, Pixel expansion, Progressive VSS, Random grids, Visual secret sharing.*

1. Introduction

In In today's life digital contents are widely used which is eavesdrop by intruders by communication channels. To protect digital contents from eavesdropping is a critical demand in information security. Many of the traditional cryptographic techniques are used to resolve this problem. The measurement of security in tradition cryptography is based on computational cost of encryption and decryption algorithm. It means that if we want a stronger security, the decryption computation cost is very high. The secret sharing approach follows the traditional cryptography, which divides the secret information. into n number of shadows (shares).This shares distributed among n participants. This secret information can be recovered by the cooperation of these participants. In traditional cryptography or secret sharing required a computing device at the time of decryption. Some time at the some places computing device are not available, so the above cryptographic technique is not working for this scenario. The solution of this type of situation is handled by a new cryptographic technique known as Visual Secret Sharing (VSS). VSS is an image encryption method. In this method, an image is divided into shadows which can be overlapped together to reconstruct the original secret image. The state of the art provides the survey of VSS from last two decades to till date. The Visual Secret Sharing technique is used for the secure secret sharing, which another desirable application area is related to distributed information storage such as secure cloud storage. It protects cloud storage from active as well as passive attack. Moreover, Secure Massage Transmission (SMT) is also an applied area of VSS. It can be also used for hiding military maps, commercial document and personal information.

Intruder cannot extract any information from an individual share. The secret information can be revealed iff the threshold condition is satisfied. It is perfectly secure under the condition.
During the survey journey, chapter found the different challenges in the VSS such as pixel expansion, codebook, contrast, distortion, line alignment and cheating activity etc. many researchers are accepted this challenges and try to rectify it, but still there is a need of improvement. Some of the researchers worked on pixel expansion issue, some of worked on contrast and security issues. Many authors worked on extended VSS such as multiple secret VSS and meaningful VSS. Some researchers also worked on crypt analysis. In VSS with meaningful shares, the generated shares are shown as natural images which are reducing the possibility of deceiving from the intruders. Cheating in visual cryptography is another issue, which could be done by malicious participant or malicious outsider cheater. Cheater cheats successfully if it finds fake shares which are indistinguishable to original shares, and if stacking with original shares it reveals the fake secret image. Secret sharing schemes affected by cheating from a decade, now most of the visual cryptography schemes also suffer with this problem. Due to cheating in VSS, only cheater is able to reconstruct the original secret. To protect from the cheating in VSS, different cheating prevention VSS schemes are available. There are two models are available in VSS, one is Visual Cryptography (VC) which is introduced by Naor's [1] in 1994 and other model is introduced by Kafri [15]. This state of the art covers both the models of VSS with its application.
This paper is organized as follows. Section 2 described the different types of VSS models.

Possible attacks in VSS schemes are introduced in section 3 and section 4 provides the details of different types of application of VSS scheme. Future research direction and conclusion are given in section 5.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. Visual Secret Sharing Models

This state of the art covers two different models of VSS scheme.

A. Visual Cryptography (VC)

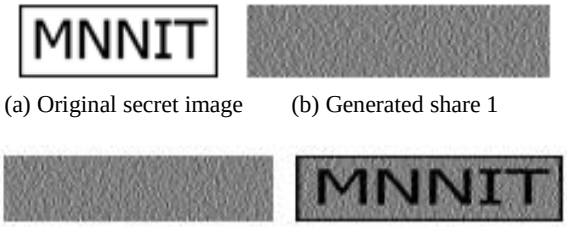
1) Basic Visual Cryptography

Visual Cryptography is a subset of secret sharing. In which secret information is encoded into n shares and distribute among the n number of participants. It requires simple logical OR (stacking) operation in decoding phase. Secret information can be visualized only when k or more participants overlap their shares (where 2≤ k≤ n). In which every pixel divided into some sub-pixels of the shares, which are shown in the table I.

Table 1: The various types of pixel patterns used in generation of shares in VC scheme

Pixel	White	Black
Probability	50%50%	50% 50%
Share1		
Share2		
StackShare1 & Share2		

This sub-pixel patterns are used in the encoding process of the VSS. Due to the random patterns of the sub-pixels, each shares does not have any clue about the original pixels of the shares. A (2, 2) VSS implemented result is shown in the figure 1, where figure 1 (a) is the original secret image, 1 (b) and 1 (c) are the generated shares, 1 (d) is the recovered secret image. The limitation of this method is that, it required pixel expansion and codebook. It is also suffering from share alignment. In this method the probability of recovery is 50% and 100% of the white and black pixels of the secret image respectively. So, the contrast of the recovered secret image is 50 %.



(a) Original secret image (b) Generated share 1

(c) Generated share 2 (d) Recovered secret image

Fig. 1: (2, 2) visual cryptography scheme

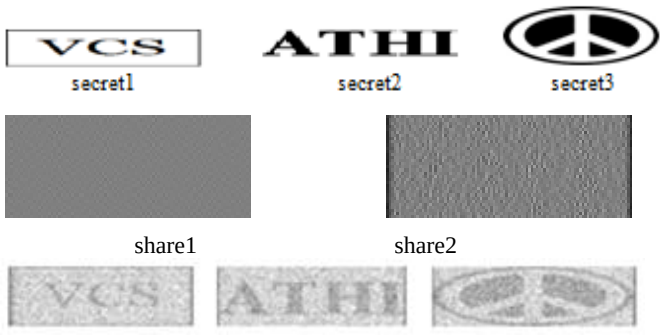
2) VC scheme with multiple secret image

The advantage of this type of technique is the more information encoded within the less amount of space. This research area was firstly opened by Wu and Chen [30] in 1998. In this method two secret images are encoded into two shares. The first secret image can be recovered by overlapping of both the shares, and rest secret images can be recovered by rotating first shares at 90˚ (anticlockwise) and overlapped with share 2. The limitation of the method is rotation angle, which are fixed. In which, the first share has only one forth part is random which cause the security issue. The angle restriction issue was handled by Hsu [31]. The contrast of the reconstructed secret image is better than Wu [30]. This approach is able to encode only two secret images. The limitation on number of secret images was increased by Feng [32] in 2008. This graph based approach recovered the secret images by

stacking the shares at aliquot angles. This method required the 3n time's pixel expansion, where the n is the number of secret images encoded. The visual quality of the recovered secret images will be degraded as the quantity of secret images will be increases. In cryptography, security is the main concern, in this approach the security is depends only on second share, which can be attacked by block attacking. The pixel expansion issue was handled by Chen [29], which is a Boolean based VSS. The advantage of this scheme is that the lossless reconstruction of the secret images.

Table 2: Comparison of different types of multiple secret VC scheme

Authors	No. of secret images	Image format	Pixel expansion	Meaningful shares	Types of VSS
Wu. [30]	2	Color	4	No	(2, 2)
Hsu [31]	2	Gray	4	No	(2, 2)
Feng [32]	n≥2	Color	3n	No	(2, 2)
Chen [29]	n≥2	Binary ,gray, color	No	No	(n+1, n+1)
J.-S. Lee [33]	2	Binary ,gray	No	Yes	(2, 2)



Reconstructedsecret1 Reconstructedsecret2 Reconstructedsecret3

Fig. 2: (2, 2) multiple secret visual cryptography scheme

This method was not secured. Lee [33] in 2015, provides more secure VSS but the capability of encoding only two secret images. The scheme provides the lossless recovery of black pixels in the reconstructed secret image. It required the codebook for encoding and decoding. Figure 2 shows the experimental result of multiple secret VSS, and table II shows the comparison of different multiple secret VSS.

3) Visual cryptography with meaningful shares

In traditional VSS, the generated shares are meaningless (noise form) which is easily attacked by attackers either change in the shares or change genuine share with fake share. To handle this type of problem, researchers introduced the many VSS with meaningful shares (innocent images).



(a) Original secret image (b) Share1 and 2
(c) Recovered secret image
Fig. 3: (2, 2) VSS scheme with meaningful shares

Table 3: Comparison of different types of VC with meaningful share

Authors	No. of secret images	Image format	Pixel expansion	Types of VSS
Chang and Tsai [26]	1	Color	Yes	(2, 2)
C. C. Chang [27]	1	Gray scale	Yes	(n, n)
Gonzalo R. [25]	1	Binary, Gray scale	Yes	(3, 3)
Yasushi Yamaguchi [28]	n≥2	Gray scale	No	General access structure
Her Chang Chao [34]	1	Gray scale	No	(2, 2)

Chang [26] introduced (2, 2) a color VC with meaningful shares. This scheme was uses color index table as the codebook. When the secret image has many colors then, the size of generated shares will become larger. This limitation was tackle by Chang [27]. In which do not required the color coding table and the size of the generated shares are fixed. This scheme is work on gray scale image, whenever it is not suggestible for true color images. Gonzalo [25] was introduced another scheme based on halftone technique. In this scheme the pixel distribution is based on the homogeneous and isotropic manner, which creates the shares with good image quality. There is no interference in the reconstructed secret image. This scheme is work on binary and gray scale images. Yasushi [28] was introduced the generalized form of meaningful VC based on the optimum tone mapping and error diffusion technique. This scheme has the ability to encode more than one secret image without pixel expansion. The quality of reconstructed secret images is good. Her Chang Chao [34] was proposed the random grid based VSS with meaningful shares. This is XOR based technique. In which, does not required pixel expansion and code book. Table III shows the comparison among different types of VC with meaningful shares. Figure 3 shows the experimental result of VC with meaningful shares.

4) Progressive visual cryptography

The visual quality (contrast and clarity) of the reconstructed secret image will be increases as the number of shares increases in the decoding process. This technique can be used as access control at deferent levels. For example, it can be used in a banking system for joint account. Bank organization can control on the banking services like balance enquiry, mini statement, fund transfer and fund withdraw etc. As the number of participants increases at the time of accessing the joint account, the number of bank services increased. Fang [23] and Jin [21] were proposed a progressive nature of VSS. The limitation of Fang [23] method is that it required pixel expansion. Chen [22] proposed an RG-based PVSS scheme. In this scheme, during image coding, several x values are designed on the basis of the probability of the share having black or white pixels to ensure the secret image is recovered gradually. Note that the RG-based PVSS scheme generates shares using RGs; thus, each share is the same size as the original secret image. Hou [24] proposed a PVSS scheme, in which the size of generated shares is same as the original secret images. First, this scheme must create a codebook. On the basis of the pixel values of the secret image, pixel values in the codebook are assigned to their corresponding positions on the shares, thereby generating shares oriented toward progressive secret recovery.

5) Privilege based visual cryptography

In some applications, the participants required a special privilege due to their rank or position. In that case, the importance of shares is different, and distributes it into participants according to their privilege. In this type of VC, the shares are divided into two parts, one is essential shares which kept by high privilege participants and other is non-essential shares which are kept by low privilege participants.
Example: Suppose that a secret mission handle by five army man, where two officers and three general duty man. The secret information is divided into five parts and distributes it among five army man. To reveal the secret information required three positive votes (3 shares) which include both the officers' votes (share).
For this type of application, Li et al. [35] proposed an essential VSS scheme. This method is based on Lagrange Interpolation. The limitation of the scheme is that at the time of recovery the secret image required the known request of the shares. Also it required the high computational cost. This issue was handled by C-N Yang [36]. This technique reduced the computational cost by reducing the generated shares size. This scheme also based on Lagrange Interpolation.

B. Random grid (RG) based VSS

In 1987, Kafri [15] proposed Random Grid based Visual Secret Sharing (RGVSS) encoding secret image into two meaningless random grid's also called as share. This scheme doesn't require code book for the generation of shares as well as the shares generated were of same size as that of original secret image. The disadvantage of this scheme was that only two participants could participate and quality of recovered secret image was still low. In RGVSS, a secret binary image is encrypted into two RG's, R1 and R2, such that individual share reveals no information about the secret image. The secret image could only be revealed by stacking both the images. The functions used for the generation of pixels randomly can be defined as-

Definition 1: (Random pixel generator)
Through probability α, generate a black or white pixel and define it as b=g(α),where Prob(b=0)=α and Prob(b=1)=1-α. Here, 0 denotes a white pixel, and 1 denotes a black pixel.
There are three basic algorithms in RGVSS.

Algorithm 1:
Input: Black & White secret image I_{sec} of size p x q
Output: Random shares R_i, i=1, 2 of size p x q
1. for r=1:p
2. for c=1:q
3. R1(r, c)=g(1/2)
4. if(I_{sec}(r, c)==0) then R2(r, c)=R1(r, c)
5. else R2(r, c)= ⌐R1(r, c)

Algorithm 2:
Input: Black & White secret image I_{sec} of size p x q
Output: Random shares R_i, i=1, 2 of size p x q
1. for r=1:p
2. for c=1:q
3. R1(r, c)=g(1/2)
4. if(I_{sec} (r, c)==0) then R2(r, c)=R1(r, c)
5. else R2(r, c)= g(1/2)

Algorithm 3:
Input: Black & White secret image I_{sec} of size p x q
Output: Random shares R_i, i=1, 2 of size p x q
1. for r=1:p
2. for c=1:q
3. R1(r, c)=g(1/2)
4. if(I_{sec} (r, c)==0) then R2(r, c)= g(1/2)
5. else R2(r, c)= ⌐R1(r, c)

In 2009, Chen and Tsao [18] extended the applicability of Random Grid Based Visual Secret Sharing to generate n shares, among which each individual share reveals no information about the message in secret image, enabling n users to participate in the sharing process. During regeneration phase all the n shares were required to generate the secret image. Without the presence of all n shares, the secret image couldn't be generated. The disadvantage of this scheme was that as more and more shares were sacked the quality of secret image gets reduced. Later Chen and Tsao [19] adopted the kernel concept (n, n)-RGVSS to achieve (k, n)-RGVSS. In (k, n) scheme for n shares generated at least t shares were required where $k \leq t \leq n$. No information is revealed about the secret image if less than k shares are stacked.

Earlier the quality of the recovered secret image was low, to overcome this problem some XOR-based visual secret sharing scheme were presented. Wu and Sun [20] proposed a VSS scheme using a generalized random grid. In this scheme the pixels were not necessarily encoded as half black and half white. This scheme was more secure as well as the recovered image produced was of good quality as compared to previous secret sharing methods. As compared to traditional VSS schemes, here XOR -operator was used in decryption phase enabling complete recovery of the secret image. The shares in generalized RGVSS have adjustable average light transmission which do not compromise with the security of the image.

X. Yan [17] proposes Random Grid based VSS with multiple decryptions. In which the secret image could be recovered even if a computational system is not present with the help of human visual system (HVS). It has both the advantages of OR-VCS and XOR-VCS. In presence of a computational device original secret image could be recovered with better visual quality provided sufficient shares are made available. The limitation of this scheme was that for (k, n) threshold, the lossless construction of secret image is possible only if all the n shares are present, otherwise for all t, $k \leq t < n$ the constructed secret image is lossy.

In Generalized Random Grid Progressive Visual Secret Sharing [16] a secret image is encoded into multiple shares having the concept of average light transmission. During the decoding phase XOR operator is used and as more shares are being stacked clearer image is being recovered.

In n-GRGPVSS we generate n equal size shares R_i, $1 \leq i \leq n$ corresponding to the secret image I_{sec}. In this scheme we select two shares R_{p1} and R_{p2} such that $R_{p1} \neq R_{p2}$ The pixels of R_{p1} is determined by g(q/2n) where $1 \leq q \leq n$. The value of R_{p2} is calculated as follows-

1. if (I_{sec} (r, c)=0) then $R_{p2}(r, c)=R_{p1}(r, c)$
2. else if $R_{p1}(r, c)=0$ and I_{sec} (r, c)=1) then $R_{p2}(r, c)=1$
3. else $R_{p2}(r, c)=g(q/2n-q)$
4. For all other shares, all their pixel values are set to 0.

This scheme is work only on XOR operator. The visual quality of the reconstructed image is also not good for small values of q and less number of shares.

3. Attacks on Shares in VSS Scheme

There are many possible attacks on the share in VSS. It is categorized on the basis of state of the shares. The shares are in the digital (during share generation or storing in computer) form or physical form (kept by participants during overlapping of shares).

A. Signal Based Attacks

This type of attack is possible when the shares are stored in computer. It could happen intentionally or unintentionally. It can perform by two ways-

1) Brute Force Attack

Attackers try all the possibility of the shares for revealing the secret image. The probability of the success of this attack is depends on the creation of basis matrices in visual cryptography or generation of shares in a random grid based VSS. This type of attack is infeasible which show by below example.

Example: suppose a secret image (black and white) of size 512 X 512 and the number of participants is 20. According to aforementioned analysis, the total number of unique combination of pixel patterns is $2^{512 \text{ X } 512 \text{ X } 20} = 2^{5242880}$. This large value shows the decoding of secret image infeasible in polynomial time.

2) Malicious Modification of Shares

Attackers modify the shares by using some noise; the purpose of this type of attack is misleading the honest participants. The best example of this type of attack is cheating.

Cheating:

Cheating is a type of attacking activity which is done by malicious persons; they can be either malicious participants or malicious outsider cheater. In which malicious persons tries to find out fake shares which are indistinguishable to the original shares.

Table 4: Example of cheating in 2-out-of-3 visual cryptography scheme

Case	Pixel in secret message	Subpixel in share1	Subpixel in share2	Subpixel in share3	Pixel in cheating message	Subpixel in share2	Subpixel in share3
1	white	{100}	{100}	{100}	white	{100}	{100}
2	white	{100}	{100}	{100}	black	{010}	{001}
3	black	{100}	{010}	{001}	white	{001}	{001}
4	black	{100}	{010}	{001}	black	{100}	{010}

These fake shares are developed on the basis of the original shares and fake secret image. When the fake shares are overlapping with other original shares, the result will come as fake secret image. The secret image pixels are the combination of sub-pixel into shares and the sub-pixels are combination of white and black pixel. If intruder intend to cheat someone, he should know the black and white pixels' position into shares. If the intruders succeed to find out the pixel position into shares, they will be able to create the fake shares. Table IV shows an example of cheating in 2-out-of-3 VC scheme. In this example, only one intruder can be done the cheating activity but the probability of success is very low. When two intruders are participating in the cheating activity, they can success with 100 % probability. Table 4 shows the example of cheating in VSS.

B. Physical Attack

The probability of this type of attack is very low because the modification of the shares which are printed on the transparency is difficult. In which shares are either theft by intruders or mishandle by participants (when shares are in noise form). This type of attack can be prevented by generating meaningful shares.

4. Application of Visual Secret Sharing

There are so many applications of the VSS, some of which are discuss here.

A. Print and Scan Applications

Several Applications of VSS would require the printing of shares on the paper, precise superposition of such shares is difficult and may lead to misalignment. Yan et Al. [2] introduced a scheme to address the problems arising due to misalignment of shares. For this authors introduced two schemes, in the first scheme a mark was put beside the share and then the shares were superimposed according to that mark. In the second scheme, he put the mark in

the share itself using VSS scheme. The above two methods are example of spatial domain. The pitfall of these schemes are vulnerable to cropping and editing. To overcome the problems Yan [2] developed a frequency domain alignment method, employing Walsh transformation to embed the marks in the shares of the secret image generated so as to properly align these shares. In decryption phase the marks are extracted and the shares are precisely aligned even in the presence of noise.

B. Offline QR Code Authorization

QR (Quick Response) code is a matrix code. This code is read by Quick Response code reader. It consists of opaque modules arranged in square form on a white background. Fang et al. [7] introduced a method for the authentication of offline QR code. He used Visual Cryptography algorithm is reverse style. QR code can contain text based information, a web site URL, V-card information of a person or any other type of data. The main features of QR code are:

1) Small in Size
2) Damage Resistance
3) Readable from any direction, can work even if the scanner is not properly aligned
4) High capacity encoding of data
5) Structure appending feature
6) Chinese /Japanese capability (representation of Japanese characters)

A QR code must be surrounded by a quite zone and usually consists of encoding regions, function patterns like separator, finder, alignment patterns etc.

C. CAPTCHA Based Authentication

Vinodhini et al. [8] proposed a CAPTCHA based authentication. In this scheme shares for captcha image are being generated using the information provided by the user (unique PIN number of user). (2, 2) VSS scheme is used to generate the shares, one share is stored into the database and other is kept by the user. When these shares are superimposed, they reveal the original CAPTCHA thus verifying the identity of the user.

The various phased involved are:

1) Share generation: User provides its information such as name, age, Date of birth, Address, identifying marks, occupation and the pin number. The pin number is used to generate Unique CAPTCHA image.

2) Hash Code Generation: Hash code is generated corresponding to the shares using MD5. This code is stored into the database, which is used at the time of authentication.

3) Authentication: Whenever the customer presents its share for authentication, hash code is generated for the given share and is compared with the value stored in the database. If it matches with the stored value, then both the CAPTCHA's are superimposed to regenerate the original image followed by post processing for removal of noise.

D. Fingerprint based Authentication

Another application of VSS is fingerprint based authentication which is introduced by Rao [9]. It aims at developing an algorithm for the precise identification of individual using its fingerprint.

The Steps involved were as follows;

1) Registration phase: In this phase (2, 2) Visual Cryptography scheme is used to generate two shares of the secret image (finger print pattern). The first generated share is kept by user in the photo identity card and another share is stored into the database.

2) Authentication phase: At the time of authentication, extract the first share from the photo id card, this extracted share superimpose the stored share in the database to show the authentication image. The secret image is then compared with the newly provided fingerprint for authentication purposes.

E. Full Proof Lock and Key

Using visual secret sharing a safety method is introduced by Tunga et al. [13]. This method consists of lock and key in pair, each containing its share of image. This share is even unknown to the owner of the lock and key. The secret image is dividing into two parts; one part is stored in the internal memory of the lock and other in the key. When the key is inserted inside the lock, exchange of shares takes place and thus the two shares can be stacked on each other to generate the original secret image. The lock is usually attached to the door and connects to some power source. The key gets powered up from the lock when inserted. Usually a second secret image is also used for the security of safe; the second secret image is also break into two parts and stored in a similar fashion. Thus the overall security of the safe depends upon the two secret images.

F. Tongue Based Security Improvisation

Suryadeva etal. [12] introduced a tongue based biometric authentication in banking system. In this approach, human tongue is used as an identifying element. They used 3 dimensional image capturing method to capture the image of tongue from various angles using high resolution cameras, i.e. image of human tongue is captured front the front, side and laterally. The use of tongue in biometric system lies in the fact that other biometric systems like retinal, fingerprint, voice are susceptible to attacks. Fingerprints can be erased, changed due to continuous work, changed by surgery, and subjected to injuries and burns, so they are unstable. When voice is considered, it is affected by sicknesses such as cold and cough. While taking Retinal scan several factors such as amount of light falling on eye which can change the state of iris must also be considered while designing such systems. Whereas tongue is unique to everyone considering the shape size and the texture, its physiological texture and shape also remain constant. It is well protected from the external environment, and so it is not affected by external factors. Digital image of the tongue can be captured and compared with the already present in the database for authentication purposes.

G. Signature Based Authentication

An authentication method for banking application based on Signature was proposed by Hegde et al. [10]. Earlier pin and passwords were used for authentication mechanism, user used to create password and these passwords were stored in the database. Whenever used wants to authenticate, it enters the password and the entered password is matched with the password present in the database. But the problem was that what if the password got stolen by someone else or if the password is forgotten.

To overcome these problems several biometric solutions like retinal scan systems, voice recognition, finger print recognition systems were introduced but the cost of implementation of such systems was too high.

To overcome the disadvantages of both the systems, i.e. biometric system (expensive, intrusive, and disastrous if compromised) and password based authentication (relatively easy to compromise, easy to forget) signature based authentication was proposed. It consists of verifying the user share of signature given as input with the share already present in the database, thus verifying the authenticity of the end user.

H. Sheltered Iris Attestation

Sindhuja et al. [11] proposed a method for sheltered iris attestation using visual secret sharing. In this scheme, capture eye image of the user, the iris part of the image is extracted and preprocessed.

After preprocessing two shares are being generated, one share is stored in the database and other share is giver to the user. For authentication both the shares are being overlapped to reveal the original image.
Apart from the above application, some more application are available such as computer generated Hologram, Human machine identification using visual secret sharing etc.

5. Future Research Directions and Conclusion

The VSS is a popular research area due to its applications. From last two decades, the researcher is continuously doing research in different paradigm of VSS. During this journey, they found out many challenges present in VSS, due to which the real implementation of this technology is still suffered. The major challenges are pixel expansion, cryptanalysis, cheating activity and visual quality of recovered secret image etc., which provides an exciting research area to work upon.
Various application areas of VSS are visual authentication and identification, image encryption, access control, data hiding etc. Visual secret sharing based watermarking provides some interesting applications, which are related to digital right management. The state-of-the–art covered various future enhancements in VSS based on cryptanalysis, optimal pixel expansion, multiple secret encoding, progressive VSS and cheating prevention etc. So there are various challenges and opportunities which make it an exciting research area to work upon.

References

[1] M. Naor and A. Shamir,"Visual Cryptography", Eurocrypt', vol. 950, Springer,1994.
[2] Wei-Qi Yan, D. Jin, Kankanhalli, M.S., "Visual cryptography for Print and Scan applications", Proceedings of the International Symposium on Circuits and Systems,2004.
[3] K. Kim, J. Park and Y. Zheng , "Human-machine Identification using visual cryptography", In Proceedings of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems, pp. 178–182, 1998.
[4] T.Katoh and H.Imai , "An Application of Visual Secret Sharing Scheme Concealing Plural Secret Images to Human Identification Scheme", Proc. of SITA'96, pp. 661-664, 1996.
[5] S.Droste , "New Results on Visual Cryptography", Advanced in Cryptology-CRYPT'96, pp. 401-415, 1996.
[6] M. Agnihotra Sharma and M. Chinna Rao , "Visual Cryptography Authentication for Data Matrix Code", International Journal of Computer Science and Telecommunications, pp. 58-62, 2011.
[7] Wen-Pinn Fang , "Offline QR Code Authorization Based on Visual Cryptography", Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 89-92, 2011.
[8] A.Vinodhini and L. J. Ambarasi , "Visual Cryptography for Authentication Using CAPTCHA", International Journal of Computer and Internet Security, pp. 67-76, 2010.
[9] Y.V. Subba Rao, Y. Sukonkina, B. Chakravarty and U. K. Singh, "Fingerprint Based Authentication Application using Visual Cryptography Methods", TENCONIEEE, pp. 1-5, 2008.
[10] Hegde, Manu S, P D. Shenoy, Venugopal K R, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications", ADCOM, pp. 65-72, 2008.
[11] R. Sindhuja, R. D. Sathiya and V. Vaiythiyanathan, "Sheltered Iris Attestation by means of Visual Cryptography (SIA-VC)", ICAESM -2012, pp. 650-655, 2012.
[12] S. Suryadevara, R. Naaz, Shweta, S. Kapoor, A. Sharma, "Visual Cryptography Improvises the Security of Tongue as a Biometric in Banking System", ICCCT, pp. 412-415, 2011.
[13] Tunga and S. Mukherjee, "Design and Implementation of a Novel Authentication Algorithm for Fool-Proof Lock-Key System Based On Visual Secret Sharing Scheme", IJCSI, pp. 182-186, 2012.
[14] Yi, S. Y., Chung, K. L., Ryu, C. S., Cha, K. H., Lee, S. H., and Kim, E. S.,. "Encryption of Cell-oriented Computer Generated Hologram by using visual cryptography", CLEO/Pacific Rim, Vol. 3, pp. 817-818, 1999.
[15] O. Kafri, E. Keren , "Encryption of pictures and shapes by random grids", Opt. Lett. 12, pp. 377–379, 1987.
[16] H.-C. Chao, T.-Y. Fan, "XOR-based progressive visual secret sharing using generalized random grids", Displays 49, pp. 6-15, 2017.
[17] X. Yan, S. Wang ,X. Niu , C.-N. Yang, "Random grid-based visual secret sharing with multiple decryptions", J.Vis. Commun. Image. R.26, pp. 94-104, 2015.
[18] T.H. Chen, K.H. Tsao, "Visual secret sharing by random grids revisited", Pattern Recogn. 42, pp. 2203–2217, 2009.
[19] T.H. Chen, K.H. Tsao,"Threshold visual secret sharing by random grids", J. Syst. Softw. 84, pp. 1197–1208, 2011.
[20] X. Wu, W. Sun, "generalized random grid and its applications in visual cryptography", IEEE Trans. Inf. Forensics Security 8, pp. 1541–1553, 2013.
[21] Jin, W.Q. Yan, M.S. Kankanhalli, "Progressive color visual cryptography", J. Electron. Imaging 14 (3), 2005.
[22] S.K. Chen, "Friendly progressive visual secret sharing using generalized random grids", Opt. Eng. 48, 2009.
[23] W.P. Fang, J.C. Lin, "Progressive viewing and sharing of sensitive images", Pattern Recognition Image Anal. 16, pp. 638–642, 2006.
[24] Y.C. Hou, Z.Y. Quan, "Progressive visual cryptography with unexpanded shares",IEEE Trans. Circ. Sys. Video Tech. 21, pp. 1760–1764, 2011.
[25] Gonzalo R. Arce, "Halftone Visual Cryptography via error diffusion", IEEE Trans. Inf. Forensics Security, vol. 4, 2009.
[26] Chang, C. Tsai, and T. Chen, "A New Scheme for Sharing Secret Color Images in Computer Network", Proc. of International Conference on Parallel and Distributed Systems, pp. 21-27, 2000.
[27] Chin-Chen Chang and Tai-Xing Yu., "Sharing a secret gray image in multiple images", International Symposium on Cyber Worlds, 2002.
[28] Y. Yamaguchi, "Extended Visual Cryptography scheme for multiple-secrets continuous-tone images", Trans. on DHMS IX, Springer, pp. 25-41, 2014.
[29] T. H. Chen, and C. S. Wu., "Efficient multi-secret image sharing based on Boolean operations", Journal of Signal Proc., pp. 90-97, 2011.
[30] Wu, C. and C. , "A study on visual cryptography, Masters thesis", Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C, 1998.
[31] Hsu, H.C., Chen, T.S., Lin and Y.H., "The ringed shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing", Networking, Sensing and Control 2, 2004.
[32] Tsai, C.S., Chang, Y.F., Feng, J.B., Wu, H.C., Chu, and Y.P. , "Visual secret sharing for multiple secrets", Pattern Recognition, 2008
[33] J.-S. Lee, C.-C. Chang, N.Tu Huynh and H.-Yi Tsai, "Preserving user-friendly and high-contrast quality for multiple secret sharing techniques", Digital Signal Proc., pp. 131-139, 2015.
[34] Her Chang Chao and T. Y. Fan, "Generating random grid-based visual secret sharing with multi-level encoding", Signal Processing: Image Communication 57, pp. 60-67, 2017.
[35] Li, P., Yang, C.N., Wu, C.C., Kong, Q., Ma, Y., "Essential secret image sharing scheme with different importance of shadows", Journal of Visual Communication and Image Representation, pp. 1106-1114, 2013.
[36] C.N. Yang, P. Li, C.C. Wu, S.R. Cai, "Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach", Signal Process. Image Communication 31, pp. 1-9, 2015.