A QUALITATIVE ANALYSIS OF VISUAL CRYPTOGRAPHY APPLICATIONS

Ekta[*] and Ajit Singh
Bhagat Phool Singh Mahila Vishwavidyalaya, Haryana, India
[*]ektacs155@gmail.com

ABSTRACT

In this modern era of information and communication technology, there is a great exchange of information over the internet and thus everyone needs secure communication. Keeping in view the same, a modern approach for information security which uses the concept of visual cryptography has been critically examined. Firstly, the focus has been made on the basis of visual cryptography and its need. Secondly, different techniques which have been used in information security based on visual cryptography along with their merits and demerits have been discussed. Comparisons have been made among the different visual cryptography techniques on the basis of pixel expansion and number of secret images as these are the factors by which performance of visual cryptography scheme can be measured including the parameters like contrast of image, accuracy, security, quality of image, computational algorithm complexity, meaningfulness of generated shares, number of secret images encrypted (single or multiple), type of secret image (binary, gray or colour). It is also intended to show which technique is used to solve what particular type of problem. Finally,a novel approach to prevent recent frauds in banking sector has been introduced.

Keywords: Visual Cryptography (VC), Shares, Human Visual System, pixel expansion, contrast and quality of image, computational algorithm complexity, Halftone, least significant bit.
Nomenclature: VC: Visual Cryptography, ⊗: XOR, GB: gigabyte

1.0 Introduction

In recent times, the increased penetration and availability of internet even to novice users has brought security of information to the helm of digital communication. Various personal and confidential data such as military and defence secrets, commercial secrets, scientific findings, banking details are transmitted over the internet. So, there is a need of great emphasis on information security than there have ever been [1][2]. Table 1, given belowprovides a brief history of attacks in different areas which underlines the need of information security. To handle all these security concerns, a lot of cryptographic algorithms have been developed out of which VC is a relatively newer technique which encrypts visual information (text, image etc.) such that it can easily be decrypted by human visual system i.e. eyes and brain without any computer based complex algorithm [3].

Table 1: History of Cyber-Attacks:
[Source: [4] and modified [1]]

Attack type	Attack name	Detail of attack	Year
Stolen credit cards / debit cards	Indian banks data breach	Estimated that data of 3.2 million debit cards were leaked affecting following banks SBI, HDFC, AXIS bank, YES, ICICI.	2016
	JP Morgan Chase breach	It was conducted by hackers from Russia.	2014
	Subway	Two Romanian men hacked into credit card payment terminals at more than 150 subway restaurant and data from more than 140 million accounts were stolen.	2012
	Stardust	Botnets were used to steal data from more than 2000 cards.	2013
	Goodwill Industries	Credit card data was stolen in more than 21 states.	2014
	Home Depot	More than 5million payment card data was stolen by installing malware on Home Depot's network.	2014

Compromised e-mail addresses and login credentials	Play station network outage	Login credentials were stolen leading to network outage.	2011
	Gawker	Anonymous hackers remotely rooted the servers and stole more than half GB private data.	2010
	IEEE	User names and passwords in plain text were exposed for more than hundred thousand members.	2012
	Yahoo	Login parameters for more than 450 thousand users were exposed.	2012 2013 2014
Government espionage	Cyber-attack on United States	Computers at Pentagon were targeted.	2008
	Cyber-attack during Paris G-20 summit	G-20 related documents were stolen.	2011
	Google	Top secret information about spies, agents and terrorist who are under observation by the U.S. government were stolen by Chinese hackers.	2009
Cyber warfare	Estonia	Both government and private entities were targeted.	2007
	Burma	Related to Burmese general elections	2010
	Singapore attack	Especially news outlets were attacked as a reaction to cyber censorship in Singapore.	2013

As compared to contemporary cryptosystems which involve computationally involved and highly complex algorithms for encryption as well as decryption, VC reduces the burden of complexity in decryption and no hardware is involved in decryption of VC messages [5].The simplest VC uses two transparent images called shares, out of which one image contains suitably selected actual dataand the other contains the random pixels. It is almost impossible to recover the secret information with only one of the shares. Allthe shares are stacked with each other to get the actual secret information [3][6]. The following figure 1 shows the basis of VC scheme.

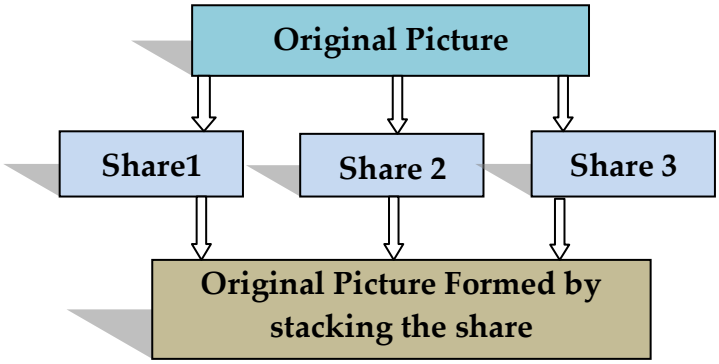

Figure 1: Block Diagram of typical VC scheme[Source: [7], [8]]

1.1. Basis VC

Naor& Shamirin 1994 developed the first basic VC scheme[9]. Two transparent images called shares were generated, one containedequally random black and whitepixels and the other was built according to the first share. Then the secret information could only be revealed by stacking of the two shares with each other [5]. Figure 2 shows the VC scheme applied for black and white image and figure 3 shows the VC scheme on colourful images.

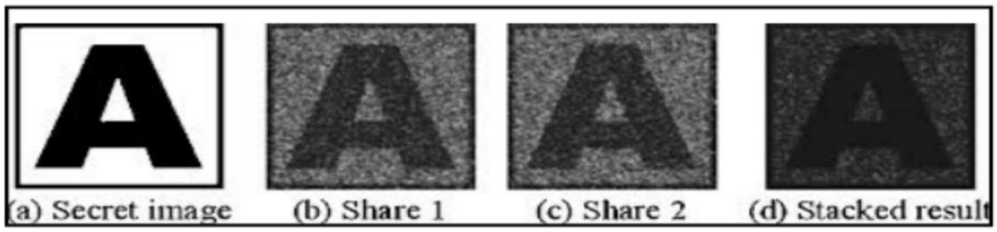

Figure 2: VC on Gray scale images [10]

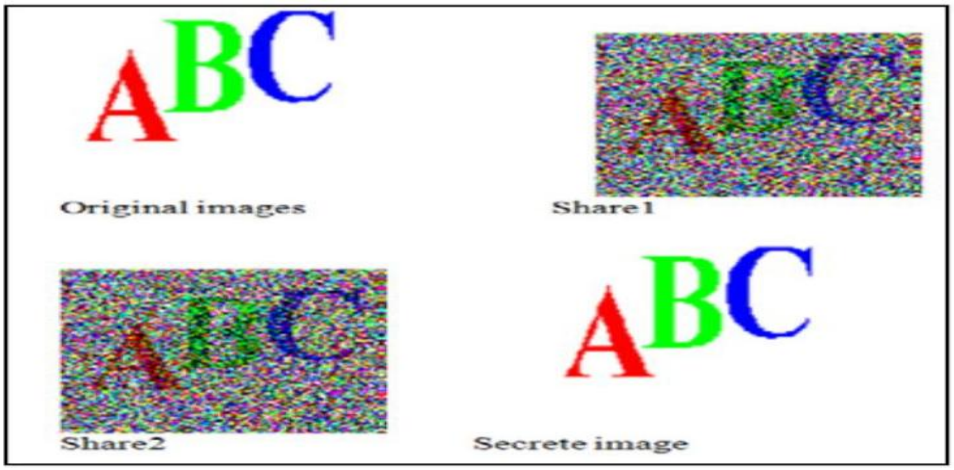

Figure 3: VC on colourful images [10]

1.2. Advantages of VC

VC scheme is easy to implement as it does not require any decryption algorithm, so the person who does not have any knowledge about cryptography can recover the message resulting in lower computational and training cost. The VC scheme can send the encrypted data through the email or fax easily [5][11].

1.3. Difficulties in VC

There are some disadvantages with the VC scheme and the researchers are trying to resolve them continuously. Reduction in loss of contrast in the image which is reconstructed by stacking the shares is actively being researched. The requirement of perfect alignment of shares to reveal original message is both boon and bane for the VC scheme. In addition, the pixel expansion causes the size of the decrypted image as twice of the original image which causes the loss of information because of change in aspect ratio [12]. Some of these difficulties and their resolution have also been discussed in this paper.

1.4. Paper Organisation

In section 2, various types of VC schemes are discussed along with their merits and demerits. In section 3, comparison between various VC schemes is made using various comparison parameters like number of secret images and pixel expansion. In section 4, various fields where VC scheme is beneficial are discussed andfinally summarising remarks are given in section 5.

2.0 Various VC Techniques (VCT):

The followingsubsections explain different types of VC schemes.

2.1. Traditional VC (VCT 01)

This refers to the sharing of a single binary secret between numbers of participants [7]. Itprovides security for binary images but does not generate meaningful share image [5][10].

2.2. Extended VC (VCT 02)

This was initially done by M Nakajima and Yamaguchi.It is a further advancement of traditional VC i.e. introducing share that have significant virtual meaning. The shares created using this scheme are meaningful to human visual system instead of random noise[11]. It has no pixel expansion but itsuffers from contrast loss occurrence.

2.3. Halftone VC (VCT 03)

This takes extended VC a step ahead[13]. Ituses error diffusion method. This technique can be used in greyscale and colour images.Halftone technique is used to convert an image into its binary form. Void and cluster algorithm is used to insert pixel from secret imageto the binary form of each share image [7]. Stacking of the shares retrieves original message. Though, it is a very good method and provides meaningful shares, but there is still a trade-off between pixel expansionand contrast of original image [6][11].

2.4. Dot Size Variant Technique (VCT 04)

Dot size variant means, we use a cluster of white and black dots to makes a share instead of using single white & black dots. So, if the original share is copied or scanned then the smallest dots in the share are altered. This adds more security in the original share and causes the loss of information into the copied shares preventing unauthorized copies [10], [11].

2.5. Recursive VC (VCT 05)

This was initially done by Wu and Chen.More than one secret message is inserted into shares. Rotation or shifting of the share to different locations on the corresponding share is required to recover the secret messages[14][11]. In this technique, one can encrypt two secret images between two shares. But size of the shares is fourfold the size of the main secret image due to extra overhead in the shares created by secret image bit insertion[6][7].

2.6. Colour VC (VCT 06)

VC schemes were initially applied to only grayscale, black and white images. Verheul and Van Tilborg, in 1997 appliedVC scheme for the first time to colour images.This opened a new gateway of research in VC since colour images are mostly used in communication and therefore will not make VC shares easily detectable by unintended users[7, 11 and 14].

2.7. Progressive VC (VCT 07)

It was proposed by Young-Chang Hou and Zen-Yu Quan[15].It takes into consideration the high quality secret reconstructions. When the quality of image is crucial, (as in case of colourful images) the progressive VC comes into consideration. This scheme solved the oversize problem of shares and the shares generated using this scheme have the same size as the secret message image. The output of the secret image pixel is constructed using 'OR' operation applied on the corresponding pixel in share images[11]. It has no pixel expansion.The message is recovery is probabilistic and there isno guaranteethat reconstruction of original pixel will be correct[3, 7].

3.0 Comparison of various VC schemes

The following Table2shows comparison between the various VC schemes. Various comparison parameters are pixel expansion, no. of secret images along with their merits and demerits in practical use of the various techniques.

Table 2: Comparison between Various VC Schemes: Source [[7][14],[16]]

Technique Used	Author	No. Of Classified Messages	Pixel Expansion	Merits	Demerits
Traditional VC	Naor and Shamir	1	1:2	Binary images are secured.	Shares have random noise.
Extended VC	M Nakajima& Yamaguchi	1	1:2	Shares are meaningful to human visual system.	Loss of contrast occurs in recovered image.
Multiple secret sharing VC	Wu & Chen	2	1:4	Multiple (two) classified messages can be encrypted. Rotating angle is $\pi/2$.	Message insertion overhead increases share size.

Progressive VC	Young-Chang Hou and Zen-Yu Quan	1	1:1	Absence of pixel expansion.	Recovery of message is not certain.
Random grid VC	Kafri and Keren	1	1:1	Absence of pixel expansion.	Visual quality of recovered message reduces.
Halftone VC	Zhongmin Wang, Gonzalo R.	1	1:4	Shares are meaningful to human visual system.	Trade-off between pixel expansion and contrast of original image

4.0 Applications of VC

This is an era of technical advancement. More and more data is being digitized and most of the restricted data related to various fields like military, commercial, banking etc. is transferred via internet[5]. Therefore, there is a vital need of security of information today than there has ever been. VC enables to transfer the secret sharing among the number of trusted parties. Many VC scheme based applications for secure transfer of data have been developed which include copy write protection [17], biometric security, secure watermarking applications,steganography, remote electronic voting, various banking applications like online transaction etc. [3][11]. Therefore, VC is boon for present scenario where most of the data is digitized and information needs to be exchanged in a secure and quality ensuring way. VC can be applied easily in banking sector especially in India where users areunaware of safe internet banking practices, let alone complex encryption and decryption methods. VC doesn't require any technical sophistication for the user part other than human visual system.

5.1 Watermarking Applications [18]

5.1.1Watermarking: Intellectual and art property rights are increasingly becoming difficult to be protected in this digital era.Identification of original work from a plagiarised work is a challenge. If a secret watermark is embedded inside the art / intellectual property such that it becomes an integral part of the original work making it difficult to remove from the original work, the copyright holder of the original work can prove his right by pulling out the embedded secret image from the VC generated image. Agood watermarking scheme should possess the following criteria such as subtlety;withstand rigorous testing and attack and security.Subtlety deals with the fact that the difference between the cover image and watermarked image is too subtle to be observed. Security refers to the feature that only the owner of the watermarked image can identify the watermark from to claim his copyright and no one else [19]. Further, it should not require original cover image for extraction of secret watermark.

Discrete Fourier Transform (DFT) is one of the most commonly used mathematical techniques along with Discrete Wavelet Transform (DWT) [18, 19 and 20]. One such watermarking scheme [19] is described in the following paragraph which based on DWT with error-detecting code along with VC providing the benefits of all these techniques viz. embedding capacity, security of VC, randomness of DWT, error minimization and detection of error-detection codes.

The scheme consists of two algorithms viz. embedding algorithm for hiding watermark (using VC, DWTand error detecting code) and the extracting algorithm for extracting watermark from the modified / cheated image and finally comparing the two watermarks to determine the legitimacy of the attacked / modified image.

Encryption Algorithm:

Input: "*n*"number of original art / IP say,P_1, . . . , *Pn*and an image W as watermark (secret image).

Output: The encryptedwork, a secret share *S* that is registered to an Copyright Authority (TA) and "*t*" number ofkey images *K*1, . . . ,*Kt* given to the owners.

Step 1: Two level Discrete Wavelet Transform is applied to generate the wavelet transformed images from the *to be published original work* say P1, . . . , *Pn*, where *P*1, . . . , *Pn*are the low

sub-band of the cover images *I*1, . . . , *In*, respectively after Discrete Wavelet Transform.

Step 2: Wavelet transformed images*FP*1, . . . , *FPn*are converted into binary images *BP*1, . . . , *BPn* hexadecimal form may also be used.

Step 3: Torus automorphism is applied to convert*W* into a disordered image *WT* with parameter *k* for *i*rounds.

Step 4: Encode the disordered image*WT* into *WE* by using the error- detecting code.

Step 5: Generate *t* random images as key images *K*1, . . . ,*Kt* forowners.

Step 6: Generate the secret share *S* by applying the *(n + t + 1, n + t + 1)*-VCS based on XOR operation, where *WE = S* ⊗*BP*1 ⊗ · · · ⊗*BPn*⊗K1 ⊗ · · · ⊗*Kt*, i.e., *S = WE* ⊗*BP*1 ⊗ · · · ⊗*BPn*⊗K1 ⊗ · · · ⊗*Kt*.

Step 7: Publish *P*1, . . . , *Pn*⊗*W* as the encrypted images , register *S* to Copyright Authority discretely and distribute *K*1, . . . ,*Kt* to the IPR holders discretely.

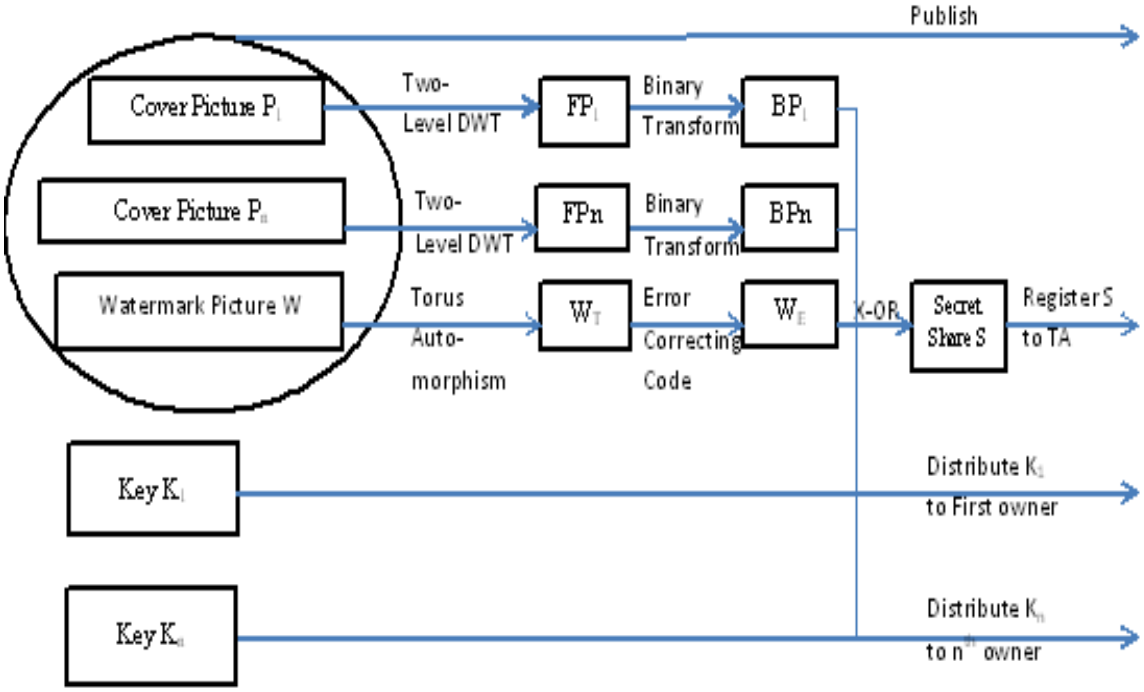

Figure 4: Encryption Algorithm [19, 20]

Decryption Algorithm

Input The attacked images *P*1*'*, . . . , *Pn'* , the secret share *S* and *K*1, . . . ,*K* involved in encryption part.

Output An extracted image *W'* similar to inserted secret image and compare it with the original secret image*W*.

Step 1. Two level Discrete Wavelet Transform is applied to get the wavelet transformed images of the attacked images *FP*1*'*, . . . , *FPn'*,

Step 2. Convert the wavelet transformed images images*FP*1', . . . , *FPn'*into binary images *BP*1*'*, . . . , *BPn'* .The step is same as encryption step.

Step 3. Obtain the secret share *S* from copyright authority, and obtain *K*1, . . . ,*Kt* from the owners.

Step 4. Get the *Ws'* by the following equation *Ws'= S* ⊗*BP*$_1$*'*⊗ · · · ⊗*BPn*⊗K1 ⊗ · · · ⊗*Kt*.

Step 5. Decode the *Ws'* into W_E*'* by using the error detecting code.

Step 6 Inverse torus automorphism is applied to generate *W'*.

Step 7. Compare the secret images*W* and *W'*

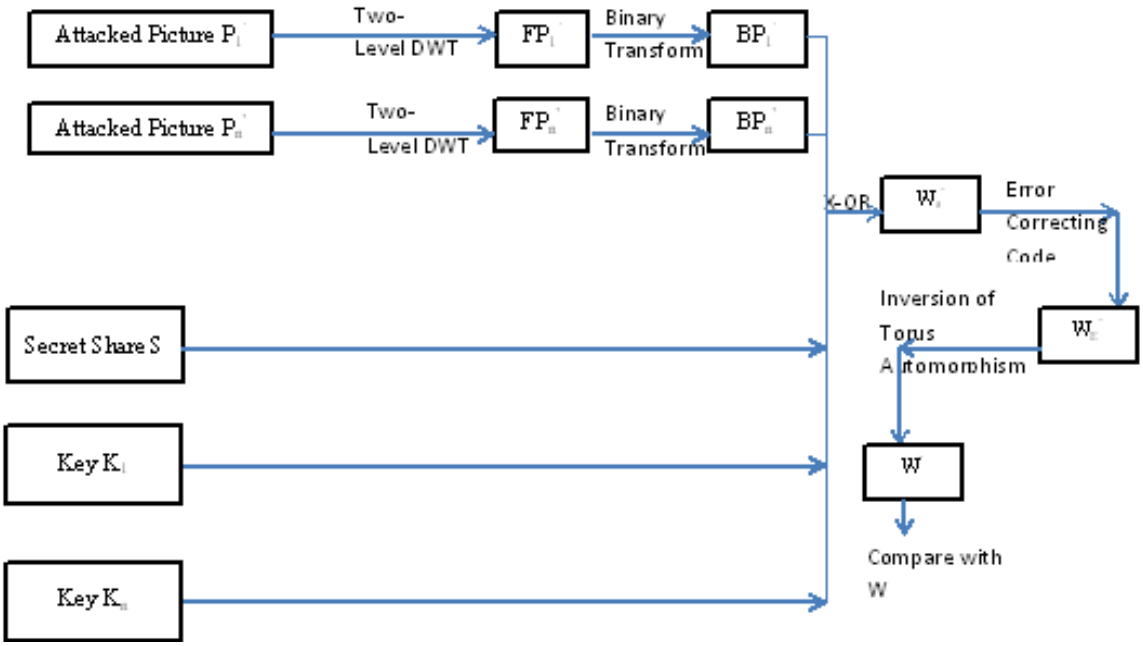

Figure 5: Decryption Process [19, 20]

5.2 Multiple Secret Open Transmissions (Broadcasting):

The VC Scheme provided by Naor& Shamir [9] deals with sharing of secret message among k participants in which qualified subset (say t) of participants ($t \leq k$) can easily rebuild the secret message using normal human vision. However, one of the most important& difficult to break application which does not require even a secure medium of communication to send a secret message can be developed using VC. VC can be further modified to share n secret messages to i different receivers (requiring individually different secret messages) [21]. Beautiful algorithm for the above is described below:

1. Two types of shares need to be generated say A_i's & B_i's.
2. A_i's can be generated from any random image & thus can be distributed to individuals without any security threat.
3. B_i's can be generated using various like linear feedback shift register (LFSR eg. X-OR) with A_i's & n secret messages as inputs (which can further randomised using a different LFSR technique).
4. These B_i's can be published anywhere (in newspaper, internet etc.) so as to reach the intended I receivers at any location.

.

5. The k^{th} receiver will get its individual secret message just by superimposing A_k^{th} share which was generated using a random image.

In above steps only LFSR's [21]are the crucial link for encryption & decryption which need not be shared with any other individual & thus ensures the security of the algorithm

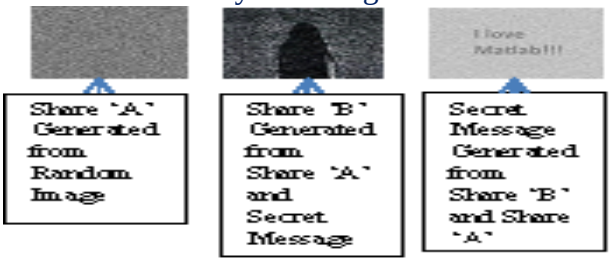

Figure 6: Process of Multiple Broadcasting

5.3 Signature Authorisation in banking

5.3.1 All banking applications require user's signature authentication before any further processing. To perform this activity, bank employees usually compare the signature of the user which is stored in their database. This can be a security threat [1, 4] for the user's financial activities if the banks database is leaked. VC can be used to avoid such information hazards using following technique given in figure 7.

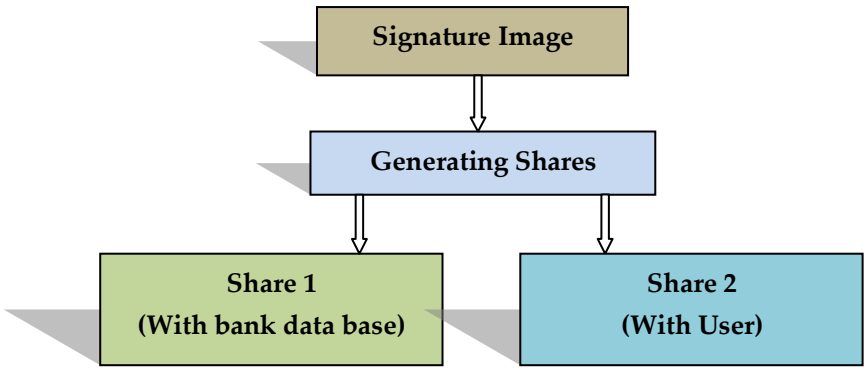

Figure 7: VC in Banking Signature Authorisation

In above process, the privacy and financial secrecy has been given in the hands of user. Whenever, a signature authorisation is required by bank, the user's assent will be required along with his share. This will ensure no fraud transaction be carried out in the name of the user even if bank employee corruptly collude for such fraud transactions.

5.3.2 Recent PNB (Punjab National Bank) scam[22] could have been prevented if necessary integration between SWIFT system[23] and Indian IFSC systems was available. This integration of two systems could have been done by using proper signature authorisation of appropriate level authorities. VC can play a crucial role in signature authorization as well as document authorisation if proper shares of the secrets are distributed to different authorisation levels.

Any transaction will then require availability of shares from all such appropriate authorities along with their consent and thus avoiding any fraud transactions.

6.0 Conclusion

VC can be used in different area to ensure security. This paper represents the techniques developed by various authors for solving the popular problems associated with shares in VC like pixel expansion, contrast loss, quality of reconstructed fact, which mayreducethe benefits of VC. Some of the major applicable areas of Visual Cryptography have been introduced. A novel approach to prevent scams like recent PNB scam and frauds in which users are cheated by copying signs etc. have been provided after analysing other present applications like watermarking, broadcasting. This paper opens up era to use different VC techniques according to application area sensitivity. There are still many areas which have not been coupled with Visual Cryptography which otherwise would prove beneficial.

Funding

No external grant was provided for this work.

References

1. Chaudhary, Deepti, Rashmi, Welekar (2015). A Secure Authentication Using Visual Cryptography & Steganography. International Journal of Engineering Trends and Technology, 21(6), 324–327. https://doi.org/10.14445/22315381/ijett-v21p260.
2. Lin, Chang-Chou, Tsai, Wen-Hsiang (2003). Visual Cryptography for Gray Level Images by Dithering Techniques. Pattern Recognition Letters 24, 349-358. https://doi.org/10.1016/S0167-8655(02)00259-3
3. Pandey, A., Som, S. (2016). Applications and Usage of Visual Cryptography: A Review. 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 375-381. https://doi.org/10.1109/ICRITO.2016.7784984.
4. https://en.wikipedia.org/wiki/List_of_cyber-attacks, Date: 25 March 2017

5. Shrivas, Bhawna, Yadav, Shweta (2015).A Survey on Visual Cryptography Techniques and their Applications. International Journal of Computer Scienceand Information Technologies, 6 (2), 1076-1079.
6. Das, K., Bandyopadhyay, Samir Kumar (2016). A Review Paper on Various Visual Cryptography Schemes", International Journal of Current Research 8, 32445-32449.
7. Rani, Mamta, Kumar, Raj (2015). Various Visual Cryptography schemes for Database Security. International Journal of Enhanced Research in Management & Computer Applications 4
8. Abboud, G., Marean, J., Yampolskiy, R. V. (2010). Steganography and Visual Cryptography in Computer Forensics. 5th International Workshop on Systematic Approaches to Digital Forensic Engineering, (SADFE),25-32. https://doi.org/10.1109/SADFE.2010.1.
9. Naor, M., Shamir, A. (1994). Visual cryptography. In: De Santis A. (eds) Advances in Cryptology — EUROCRYPT'94. EUROCRYPT. Lecture Notes in Computer Science, 950. Springer, Berlin, Heidelberg (1995).
10. Kumar, M.S., Shilpa, A. and Vijayalakshm, J.R. (2015). A survey on Visual Cryptography Techniques. International Journal of Application or Innovation in Engineering & Management (IJAIEM) 5, 100-112.
11. Weir JP (2011). Visual cryptography and its applications. Bookboon.
12. Liu, F., Yan, W.Q. (2014). Visual Cryptography for Image Processing and Security. Springer. https://doi.org/10.1007/978-3-319-23473-1.
13. Wang, Z. M., Arce, G. R., Crescenzo, G. Di. (2009). Halftone Visual Cryptography via Error Diffusion. IEEE Trans. Inf. Forensics Security4, 383–396. https://doi.org/10.1109/TIFS.2009.2024721
14. Kiran, T. (2012). A Review on Visual Cryptography Schemes: Journal of Global Research in Computer Science 3, 96-100.
15. Hou, Young-Chang, Quan, Zen-Yu (2011). Progressive Visual Cryptography with Unexpanded Shares. IEEE Transactions On Circuits And Systems For Video Technology 21, 1760-1764. https://doi.org/ 10.1109/TCSVT.2011.2106291.
16. Ramya, J., Parvathavarthini, B. (2014). An extensive review on visual cryptography schemes. International Conference on Control, Instrumentation, Communication and Computational Technologies, pp. 223-228.https://doi.org/10.1109/ICCICCT.2014.6992960
17. Ying, Shen, Yinlan, Ye. (2010). Visual Cryptography based Multiparty Copyright Protect Scheme 223 - 226 https://doi.org/10.1109/ICACC.2010.5486685.
18. Tai GC., Chang LW. (2004). Visual Cryptography for Digital Watermarking in Still Images. In: Aizawa K., Nakamura Y., Satoh S. (eds) Advances in Multimedia Information Processing - PCM. Springer, Berlin, Heidelberg.
19. Liu F., Yan W. (2015). Various Applications of Visual Cryptography. In: Visual Cryptography for Image Processing and Security. Springer, Cham. https://doi.org/10.1007/978-3-319-23473-1_6
20. Lin, C.Y., Wu, M., Bloom, J. A., Cox, I. J., Miller, M. L., Lui, Y. M. (2001). Rotation, scale, and translation resilient watermarking for images. IEEE Transactions on Image Processing, 10, 767-782. https://doi.org/10.1109/83.918569.
21. Yengisetty, S. R. V., Roy, B. K. (2011). Applications of visual Cryptography. International Journal of Parallel, Emergent and Distributed Systems, 26, 429-442. https://doi.org/ 10.1080/17445760.2011.574628
22. https://en.wikipedia.org/wiki/Punjab_National_Bank_Scam, Accessed Nov 18, 2018
23. https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication, Accessed Nov 18, 2018