A REVIEW ON VISUAL CRYPTOGRAPHY BASED SECURE TRANSACTIONS IN E-BANKING

Shubham Sahai, M.Tech Scholar, Department of Computer Science & Engineering, Saraswati Higher Education & Technical College Of Engineering,Varanasi, India.
Arvind Kumar Singh, Assistant Professor , Department of Computer Science & Engineering, Saraswati Higher Education & Technical College Of Engineering,Varanasi, India

Abstract—**Image cryptography is a relatively new subject of study. Cryptography has been established using a variety of techniques. The visual information (pictures, text, etc.) in photographs has been hidden using a variety of encryption techniques. Visual cryptography is the core idea of encryption, which is the capability of decryption by human eye if the correct key image is utilised.**
Because banks are committed to providing secure core banking services to their consumers, security has become the most critical feature of today's banking transaction system. To reach this purpose, users must be authenticated, which means that only authorised users can participate in the transaction. Banks utilise biometrics-based authentication systems for this purpose, but the financial system's database is no longer safe owing to unavoidable malevolent activity. Smart hackers can extract biometric information from a bank's database and exploit it to make fraudulent transactions. To prevent all of this, a visual cryptography approach is employed. Banking transition security research for Visual Cryptography is covered in this paper.

Index Terms—Visual Cryptography,, Image Processing, Secret Sharing Scheme, Banking System.

I. INTRODUCTION

Digital data and information are currently sent via the Internet at a faster rate than ever before. The popularity of digital media has increased due to the availability and effectiveness of worldwide computer networks for the transfer of digital information and data. The way digital images, video, and audio are acquired, stored, transferred, and altered has been revolutionised, resulting in a wide range of applications in education, entertainment, media, and the military, among other disciplines. Computers and networking capabilities have grown more affordable and widely available. The digital multimedia area has benefited greatly from innovative techniques to storing, accessing, and sharing data, owing to qualities like as distortion-free transmission, compact storage, and easy editing [1].
Personal and sensitive information is increasingly being stored and communicated through computer systems and networks on a daily basis as our dependence on computers grows at all levels of our lives. However, as indicated by the rising incidence of computer intrusions and break-ins, this transformation has brought with it new risks and digital crimes. Intruders will have a better opportunity of accessing crucial information if it is duplicated. On the other side, having only one duplicate of this information implies there is no way to recover it if it is destroyed. As a result, there is a pressing need to handle data in a secure and dependable manner. Secret sharing becomes quite important in such scenarios.
Digitalization has the greatest potential to change our lifestyles. Security is a major worry in today's digitally connected world. When information is sent from one node to another through the network, security issues begin to emerge. Because the number of threats is expanding at a faster rate, effective security solutions are required. One of the most important strategies for ensuring information security is cryptography. Traditional cryptography methods require a lot of computer power and intricate algorithms to encode and decode a secret message, which takes a lot of time and money.
Biometrics-based authentication is commonly utilised in the banking industry. To authenticate the subject or verify claimed identity, a biometrics-based authentication system obtains raw biometric data (e.g., face image, fingerprints, etc.) from the subject, extracts feature set from the raw data, and compares the feature set to the blueprint recorded in the database. Any institute's or organization's security is based on the underlying design technology middleware and, to a large extent, the database design. Every transaction has an effect on the database, whether it be geographical or temporal. As a result, hackers are constantly

attempting to breach the database. The main concern with the banking system's web-enabled core services is user authentication. Password-based authentication, smart card-based authentication, and biometric-based authentication systems are all employed for this purpose. All of these strategies are required to keep a database up to date, making it vulnerable to hacking. Because the database contains private information, there is a risk of privacy breach. 1

Visual Cryptography [1-3] is a secret sharing scheme that takes a secret image as input (i.e. printed, handwritten) and encrypts it into a set of other images called shares in such a way that the original secret is revealed if the shares are printed on transparencies and superimposed or staked over one another. The simplest kind of visual cryptography, also known as visual secret sharing, takes a binary image as input and treats each pixel separately.

To encode a pixel of the secret image, we break it into n variants in such a way that the original secret pixel is exposed after all n versions are printed on transparencies and superimposed. This method must be used for the complete secret image. As a result, n copies of the original secret image are ready to be printed on transparencies and superimposed to disclose the secret. To assure authentication and security of the information contained in the bank database, a method employs XOR operation-based Visual Cryptography and image processing algorithms.

II. Literature Review

A literature survey analyses old data and generates a mix of new and old data. As a result, this part contains a brief explanation of numerous research papers as well as the presence of research paper summary and synthesis.

This section provides a brief overview of Visual Cryptography and its applications in the banking system. Keys to cryptographic systems must be kept safe. In 1979, G. Blakely [11] and A. Shamir [12] independently devised the (t, n)-secret sharing scheme, which states that the secret can be revealed if at least t out of n shares are combined in a specific way. If there are fewer than t shares available, the secret will not be divulged. The secret sharing schemes of G. Blakely and A. Shamir are based on vector space and polynomial interpolation, respectively.

Visual cryptography is a safe method of detecting phoney websites and the phishing assaults that result from them. It is a way of delivering and receiving communications that only the sender and receiver can decrypt. This concept was introduced by Naor and Shamir [1] as a simple and secure way of distributing a secret image as a password.

This approach has two parts: encryption decryption and image sharing creation. A simple mathematical procedure is used to encrypt and decrypt messages. The image's share generation is the scheme's second crucial component. VCS is a cryptography technique for encrypting visual information so that it can only be decrypted by humans.

The visual cryptography system for secret sharing was explicitly developed and proposed by Naor and Shamir [1]. Since then, VC research has grown in popularity, becoming a focus for a variety of studies. There are several different forms of VC, each with its unique emphasis on practical application. The operation of dividing a VC secret image into shares has been concentrated on the areas of being applied to various types of secret images, such as grayscale and colour images. To address the prior successes, this chapter first introduces basic knowledge of secret sharing and VC. Several contributions to the literature have been reviewed in light of various VC schemes that have been proposed in the literature.

The reconstructed image of the OR-based VCS is of poor quality. In most of the schemes, it cannot be enhanced beyond a certain point. Tuyls et al.[13] proposed a VCS system that uses the Boolean XOR as the fundamental mathematical operation and is based on light polarisation.

A liquid crystal layer is inserted into a liquid crystal display to do this (LCD). In contrast to OR-based schemes, where participants must carry a number of transcripts in order to update their shares, an XOR-based VCS requires only a device with a display.

The liquid crystal layers must be layered together in order to recover the secret image. Furthermore, thanks to rapid technological advancements, these devices are becoming more affordable. The authors of the suggested XOR technique [13] built an XOR based (n,n) -VCS and established that an XOR based VCS is comparable to a binary code.

In general, XOR-based VCS are non-monotone, which means that just because a qualified set of parties can recover the secret picture does not mean that every superset can. The key difference between these two visual cryptography models is that the OR model captures robust access structures, whereas the XOR model cannot satisfy monotone criteria due to the unpredictability of the XOR operation. However, by making a minor change to the definition of the XOR scheme, we can fix this problem.

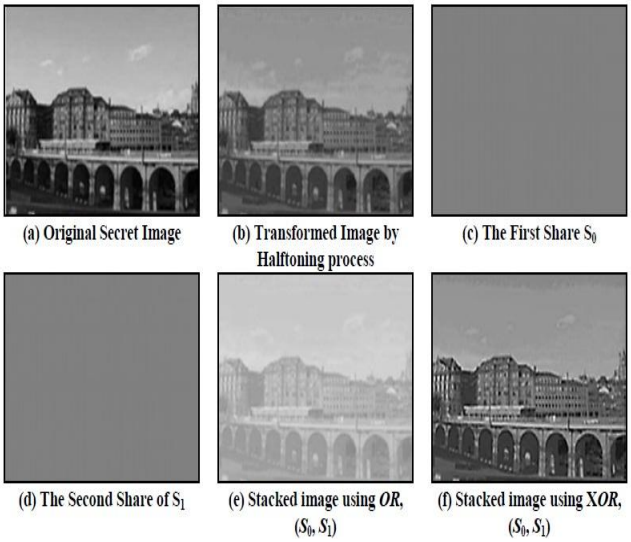

Figure 1: Process of XORing operation on VCS

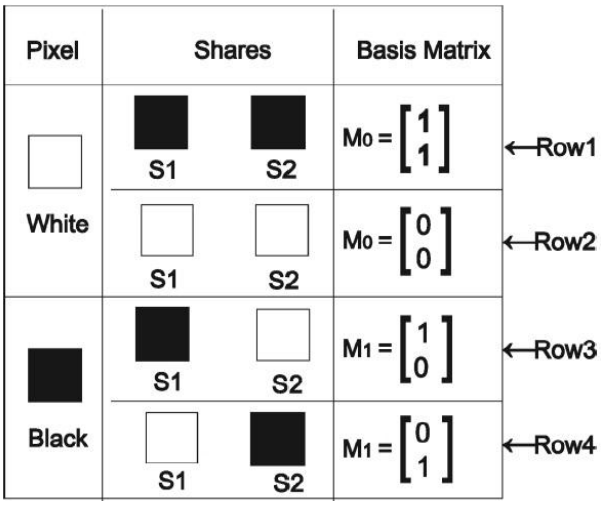

Figure 2: (2, 2)-VCS Scheme

The security conditions for both devices are identical, but the contrast condition differs. The half toning technique has been used to extend Naor and Shamir's [1] original concept in the 2-out-of-2 secret sharing scheme. It also goes a step farther than simple visual cryptography by supporting different picture versions.

III. VISUAL CRYPTOGRAPHY

Cryptography has a long and fascinating history within the security domain. Handling of sensitive images carrying confidential information is of prime concern in several departments such as sharing the maps over the internet in the military and in many others commercial sectors. To handle the security problems of sensitive images, various image secret sharing schemes have been evolved. One of the techniques named as **Visual cryptography (VC)** has been developed by Naor and Shamir [1] in the year 1995 to handle secret sharing for images.

VC is an approach in which a secret image containing confidential visible information is encrypted in a perfectly secure way such that the decryption can be performed directly by the human visual system (HVS), without the assistance of computers. VC allows encrypting any visual information such as printed text, handwritten notes, and pictures. It eliminates complex computation during decryption process, and the images can be restored by doing stacking operation on its shares. It combines the feature of perfect ciphers creation and secret sharing in cryptography. Secret image is usually divided into two or more pieces known as shares. When the required number of shares, print on transparencies and then superimposed, the secret images get recovered.

Naor et al. [1] introduced the technique of VC in which the binary image is decomposed into n number of shares. Figure 1.1 shows an example of share creation and recovery of a secret image using visual cryptography. In the scheme of *(k,n)*, shares when stacked over one another reveals the original secret image. Naor scheme is quite suitable for a binary image. The shares created in the original image are determined by randomly selecting pairs of sub-pixel matrices for black and white pixels [2].

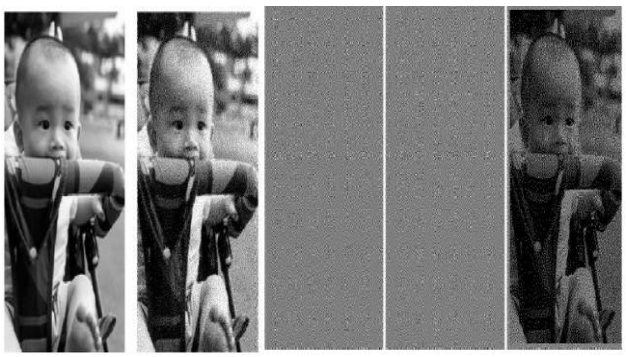

Figure 3: Original image, Halftone, Share-1, Share-2 and Decrypted image

VC scheme suggested by Naor et al. [1] requires no computer participation in any situation for decryption. Visual cryptography combines the notion of the perfect secret with a random image for the purpose of secret sharing [3]. The next section describes the common characteristics of VC schemes.

Generally, visual cryptography is used to preserve the privacy of raw images. Most of the business organizations need to protect data from disclosure[4]. As the world is more connected by computers, most organizations are afraid to store data in a single computer. So, VC provides a solution to distribute the data in several places and destroy the original one. As and when a need of original data arises, it could be reconstructed from the distributed shares. The information will not be available centralized at one point. The following characteristics made visual cryptography very popular among researchers and academicians to utilize it in various domains of security.

- Its implementation is very easy. The person who has even less knowledge about the scheme can implement it without any hassle.
- It does not require any intervention of computer or any other hardware or software device in most of the situations during the restoration of the secret.
- As there is no decryption algorithm, so its decryption is very simple. When all the required shares superimposed on each other, the original secret image is retrieved.
- Its computational cost is very low, as it does not involve any cryptographic computation. However, on the other hand, the quality of the image is compromised in the scheme.

Visual cryptography possesses mainly three characteristics: Perfect security, secret restoration without the aid of a computing device, and robustness against lossy compression [5]. This simple and yet secure approach made visual cryptography a popular and interesting research field.

IV. Authentication and Secure Share Problem in Visual Cryptography

As the discussion of the VC scheme has progressed, it has become clear that the security of the secret image is inextricably linked to the trustworthiness of VC shares. The decryption and analysis of VC shares are required for VC scheme cheating. Because people will validate and accept a faked image, the

act of cheating may bring harm to victims. Many researchers have experimented with the idea of cheating with VCS and have proposed solutions for its protection as well.
Authentication methods that focus on identification between two individuals to help in the prevention of any form of cheating have been recommended as a way to prevent cheating. Tzeng et al. [9] offered two different types of cheating deterrents. The first makes use of an online trust authority to conduct participant authentication. The second form comprises a tweak in the VC scheme that displays a verification symbol by stacking two shares. If the specified symbols for the stacked VC shares do not display, the authentication process fails. This solution, however, necessitates the insertion of extra pixels to the secret.
Horng et al. [60] describe yet another cheating prevention technique. The hacker will be able to successfully attack and cheat the scheme by observing the exact distribution of black and white pixels of each of the shares of honest players. To prevent cheating, adopt a method that stops the attacker from acquiring this distribution. Hu et al. [14] also discussed cheating strategies and how to avoid them. Tzeng system also showed improvements over Yang scheme, as well as a novel cheating prevention scheme that tries to reduce the overall number of extra pixels.
Several attempts have been made in the past to propose cheating immune VCS [15]. In visual secret exchange systems, Yang et al. presented a method of separating the secret into two barcodes [15]. Barcodes and, in some cases, the braille character are examples of commonly used cyphers. A barcode has just black or white pixels, and because to its graphic organisation structure, it is difficult to distinguish by human eyes. Its data is traditionally encoded in one-dimensional barcodes with parallel lines. It is feasible to use these symbols as part of a VC blind authentication process.
Chen et al. and Tsai & Horng examined a number of well-known cheating activities and Visual Secret-sharing Schemes for Cheating Prevention (CPVSS). They divided cheating into three categories: meaningful, non-meaningful, and meaningful deterministic cheating. Furthermore, they examined the CPVSS research issues and developed a new cheating prevention strategy that is superior to prior systems in terms of security requirements.
Not only should the process of creating shares throughout the encoding process be robust, but so should the process of cheating. In all such circumstances, the scheme loses its knowledge to the relevant participant if the scheme generates the artefact of a hidden image in any of the created shares. As a result, the development of secure shares, as well as cheating prevention methods, will be an attempt to develop an ideal scheme for safe VCS.

V. Applications of Visual Cryptography

Aside from the obvious application of information concealment, visual cryptography can be used in a variety of domains, including access control (bank vault opening), threshold signatures (wallet security via multiple devices, e.g. bit coin), copyright protection, watermarking, visual authentication, ticket validation, and human identification, among others. The banking industry, satellite imagery, and commercial applications for safeguarding collected biometric data are all examples of visual cryptography applications.

The user will find visual cryptography to be quite intuitive. However, just a few recommendations for applying it to real situations have been presented in the last two decades since its birth by Naor and Shamir. Naor and Pinkas [6] described a method for using visual cryptography to safeguard online transactions against manipulation, while Chaum et al. [7] suggested using it to verify the integrity of election results [18].

The user receives a numbered set of transparencies from the transaction server in order to secure online money transactions. The server sends a visual message to the user's screen with the transaction data, which is encoded using visual cryptography. If the user overlays a transparency with a specific number on top of the encoded image, the message contained within the image can be seen by the screened individual.

If the server receives the correct TAN, the transaction is completed; otherwise, it is not. In this approach, banking transactions can be made more safe. VC is particularly well-known for its usage of Moiré patterns and watermarking. When a revealing layer is put on top of an image with periodically repeating

shapes, Moirés patterns are created. Researchers have sought to implant the Moiré pattern onto VC shares. The original secret can be discovered by superimposing the shares and viewing the embedded image when the shares are separated.

Watermarking is another popular application for VC. Watermarking is crucial for information concealment and embedding. The application of VC in watermarking is based on a basis matrix, and the final recovered secret is perceived utilising the contrast between white and black hues, similar to standard VC.

Luo et al. [8] investigate the use of watermarks in visual cryptography as well. Hwang [9] has presented a visual cryptography-based digital image copyright method. Embedding VC-based watermarking into products is a useful technique of preventing cheating, particularly in fields where watermarking is already beneficial.

These recommendations did not result in applications that are employed for serious reasons due to obstacles such as adjustment, size, and prices of special equipment. However, further developments of the principles provided in alternative techniques, as well as new ideas, could spread visual cryptography's practical applications[19]. Using VC in conjunction with recent picture hatching techniques, VC could be extended to the monetary domain, such as in the banking industry. It's also worth considering the use of shares in the secure printing sector. It's also possible to scan a share into a computer system and then digitally superimpose its matching share.

VI. Conclusion

Visual cryptography is a useful tool for securing images that contain sensitive information. As a subset of secret sharing, VC has gotten a lot of press for its security mechanism, which takes into account both image processing and cryptography. The applications of VC appear to be growing and more realistic as VC develops in the fields of dealing with various forms of secret images. This project is primarily concerned with issues of identity theft and consumer data security in joint account transactions. Visual cryptography is used for safe banking transactions.

References

[1] M. Naor and A. Shamir, ―Visual Cryptography,‖ Advances in Cryptology ,EUROCRYPT-94, LNCS-950, pp. 1–12, Springer, Berlin, Heidelberg, 1994.
[2] B. W. Leung, F. Y. Ng, D. S. Wong, ―On the security of a visual cryptography scheme for color images,‖ Pattern Recognition Journal, Elsevier, Vol. 42, no. 5, pp. 929-940, May, 2009.
[3] S. K. Das and B. C. Dhara, ―An image secret sharing technique with block based image coding,‖ , 2015 Fifth International Conference on Communication Systems and Network Technologies, pp. 648-652, April, 2015.
[4] C.Y. Wang, N.S. Shiao, H.H. Chen, and C.S. Tsai, ―Enhance the visual quality of shares and recovered secret on meaningful shares visual secret sharing,‖ in Proceedings of the 4th International Conference on Uniquitous Information Management and Communication - ICUIMC ’10, 2010.
[5] F. Liu and W. Yan, Visual Cryptography for Image Processing and Security : Theory, Methods, and Applications, 2nd edition, Springer, 2015.
[6] M. Naor and B. Pinkas, ―Visual authentication and identification,‖ Advances in Crypto, Crypto-97, LNCS-1294, pp. 322–336, Springer, Berlin, Heidelberg, 1997.
[7] D. Chaum, ―Secret-ballot receipts: true voter-verifiable elections,‖ IEEE Security & Privacy Magazine, vol. 2, no. 1, pp. 38–47, Jan. 2004.
[8] H. Luo, J.-S. Pan, Z.-M. Lu, and B.-Y. Liao, ―Watermarking-Based Transparency Authentication in Visual Cryptography,‖ in Seventh International Conference on Intelligent Systems Design and Applications (ISDA 2007), pp. 609–616, 2007.
[9] R.J. Hwang, ―A Digital Image Copyright Protection Scheme Based on Visual Cryptography,‖ Tamkang Journal of Science and Engineering, vol. 3, no. 2, pp. 97–106, Sep. 2000.
[10] F. Liu and W. Q. Yan, ―Various Problems in Visual Cryptography,‖ in Visual Cryptography for Image Processing and Security, pp. 23–61, Springer International Publishing, 2014.

[11] G.R. Blakley, "Safeguarding cryptographic keys," Proc. of the National Computer Conference1979, vol. 48, pp: 313–317, 1979.
[12] M. Naor and A. Shamir, "Visual cryptography, in Workshop on the Theory and Application of Cryptographic Techniques, pp: 1–12, Springer, 1994.
[13] S. Roy, P.Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," Proceedings of IEEE Students' Conference on Electrical, Electronics and Computer Science, 2014.
[14] V. Suruthikeerthana1 , Dr. S.Uma , "An Extended Visual Cryptography With Dynamically Authenticated Error Avoidance Scheme For Bank Applications", International Journal Of Research In Computer Applications And Robotics, vol 4, no. 4, pp: 15-23, 2016.
[15] C.M. Hu and W.G. Tzeng, ―Cheating Prevention in Visual Cryptography,‖ IEEE Transaction on Image Processing, vol. 16, no. 1, pp. 36–45, Jan. 2007.
[16] G. Horng, T. Chen, and D. Tsai, ―Cheating in Visual Cryptography,‖ Design, Codes and Cryptography, vol. 38, no. 2, pp. 219–236, Feb. 2006.
[17] J. Weir and W. Yan, ―Authenticating Visual Cryptography Shares Using 2D Barcodes,‖, In: Shi Y.Q., Kim HJ., Perez-Gonzalez F. (eds) Digital Forensics and Watermarking. IWDW 2011. Lecture Notes in Computer Science, vol 7128, pp. 196–210, Springer, Berlin, Heidelberg, 2012.
[18] Akhilesh Pandey, Amitash " Digital watermarking for image using 3-level DWT and PSO algorithms" International Journal of Advanced Research and Technology" Volume (7) Issue (2) June 2019.
[19] Akhilesh Pandey, Nisha Pal, Dr Dinesh Goyal " A Survey on MRI Brain Image Segmentation Technique" International Journal of Advance Engineering, Management and Science" Volume (2) Issue (12) December 2016.