IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 3, March 2017

A Short Survey of Visual Cryptography and Secret Image Sharing Techniques and Applications

Hadi Abdolrahimpour[1], Elham Shahab[2]

Department of Biomehanic, Islamic Azad University – Yazd Branch[1]

Department of Computer Science, Islamic Azad University – Yazd Branch[2]

Abstract: Cryptography, in general, is a process of transforming original information into a format such that it is only read by the desired recipient .Visual cryptography(VC) scheme is a cryptographic technique which allows visual information to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. As it does not require any key to decrypt that is why this method is unbreakable. This method is useful in vast applications which handle high value assets. It can replace the second factor that is token or key in multifactor authentication system. It can be used in online shopping sites, online banking sites, government sites. This paper gives detailed survey of visual cryptography techniques and their applications.

Keywords: Visual cryptography, secret sharing, image encryption, VC applications.

I. INTRODUCTION

With rapid development in internet technology, different types of information can be transferred over internet. Hence there are security issues associated with transmitting high value assets like commercial data, user personal information, banking or transaction data, data related to military[23]. Security of such data transfer must be taken into consideration because hacker can use various methods and steal such high value assets which results in high monetary, social, personal loss. Various schemes are developed to protect such high value assets. Visual cryptography is introduced by first in 1994 Noar and Shamir [1] as a simple way to encrypt and decrypt sensitive data. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement. In visual cryptography, decryption is done by human visual system hence no need to securely store decryption key. In visual cryptography original image is divided into two parts called as shares. The single share doesn't give any information about original image. When the shares are superimposed together then we can see original image. Adi Shamir in 1979 published an article titled "How to share a secret" [3]. In this article, the following example was proposed to define a typical secret sharing problem:

"Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?
The minimal solution uses 462 locks and 252 keys per scientist."
In the paper, (k, n)-threshold scheme was introduced by Shamir to generalize the mentioned problem and formulate it [2]. It can be explained as follows: Let S be the secret to be shared among n parties. A (k, n)-threshold scheme is a way to divide S into n pieces $S_1, S_2, \ldots, S_n$ that satisfies the conditions[1]:
1. Knowledge of any k or more S_i pieces makes S easily computable.
2. Knowledge of any k−1 or fewer S_i pieces leaves S completely undetermined (in the sense that all its possible values are equally likely).

Secret Sharing scheme can be applied in different domains. One of the areas that are heavily used this approach is in Visual Secret Sharing (VSS). VSS is a powerful technique that combine the notion of perfect ciphering and Secret Sharing approach. This method uses the idea of hiding secrets within images. These images are encoded into multiple shares and later decoded without any computation. In fact, Visual Secret Sharing approach uses the characteristics of human vision to decrypt encrypted images. The decoding process is as simple as superimposing transparencies, which allows the main secret to be recovered. It would be a great advantage for this method that anyone can physically manipulate the elements of the system, and visually see the decryption process in action without any knowledge of cryptography and without performing any cryptographic computations.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 3, March 2017

SS schemes introduced in previous sections are based on algebraic calculations in their realizations [1]. But there are some different realizations from ordinal SS schemes. In such other realizations, some physical information are used instead of numbers on finite fields[1]. Table1 shows what kind of secret information is used to realize each SS scheme. In case of images as a secret information the VSS scheme.

Table1: Variations of secret sharing schemes [5].

Based on	Name	Secret information
Computers	SS schemes	Numbers infinite fields
Human sense	Visual cryptography Cerebral cryptography Optical cryptography Audio cryptography Tempo-based audio cryptography	Images 3D images Lights Sounds Rhythms
Quantum information	Quantum SS scheme Quantum SS scheme	Numbers Quantum states

II. VISUAL CRYPTOGRAPHY

The process behind VC is to generate shares randomly based on the input date (image) in such way that the outputs can stack together to show the input. Assuming that the message being encrypted is a binary image with p pixels, each of these pixels are separately encoded with a subpixel grouping with s pixels[5]. This allows n shares to be generated using these subpixel groupings. Each share is a collection of m black and white subpixels. These subpixel groupings are typically square to not distort the aspect ratio of the original image[5]. However, subpixel groupings that are not square do happen in VC algorithms and the aspect ratio of the image is altered accordingly. This structure can be described as an n×m Boolean matrix S. The structure of S can be described thus: $S = (s_{ij})_{m\times n}$ where $s_{ij} = 1$ or 0 iff the j^{th} sub-pixel of the i^{th} share is black or white.

The important parameters of the scheme are[3]:

- m, the number of pixels in a share.
- α the relative difference in the weight between the combined shares that come from a white and black pixel in the original image (the loos in contrast).
- γ the size of the collection of C_0 and C_1
- C_0= the sub pixel patterns in the shares for a white pixel.
- C_1= the sub pixel patterns in the shares for a black pixel.

The Hamming weight H(V) of the ORed m-vector V is interpreted by the visual system as[3]:

- Interpreted as black if H(V)≥ d for threshold d
- Interpreted as white if H (V)≤ d-α m for relative difference α >0
- 1 ≤d ≤m

The shares can be generated in the following manner:
1. If the pixel of the original binary image is white, randomly pick the same
pattern of four pixels for both shares.
2. If the pixel of the original image is black, pick a complementary pair of patterns,

The most commonly used subpixel groupings in VC algorithms are shown in Figure 1. The image is encoded in n shares and the message can be revealed by stacking k of those n shares. The generation of the shares is based on the value of the pixel and the probability of a subpixel group occurring[5]. A share generation scheme corresponding to k=2 and n=2 is shown in Figure 1. This is applied to a binary image by assigning the corresponding subpixel grouping to the pixels throughout the image. This results in two random shares where the message cannot be identified.

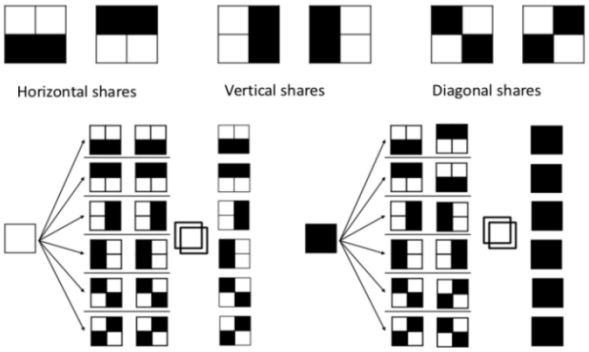

Figure 1: Shares most commonly used for Visual Cryptography [11].

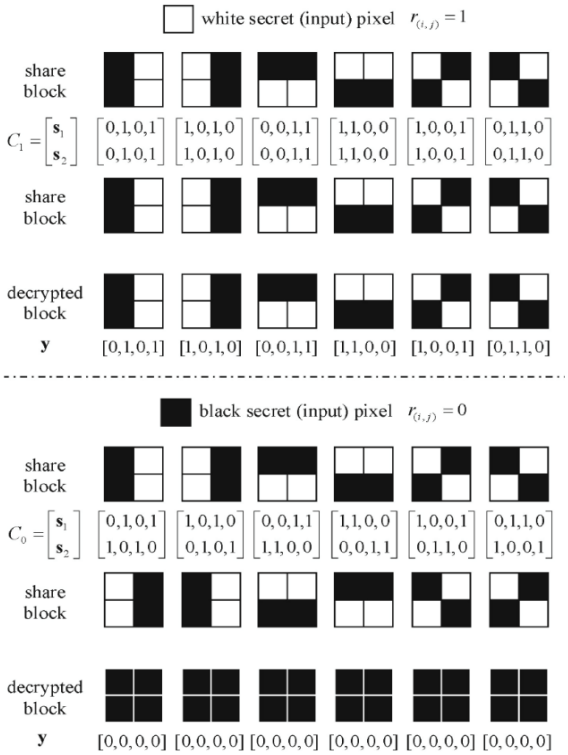

Figure 2: Encryption and decryption in Visual Cryptography [10].

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 3, March 2017

Figure 2 shows the principle of both encryption and decryption used in visual cryptography. If a secret pixel is white, i.e. r(i, j) = 1, then each pixel in s1 is equivalent to each pixel in s2, and thus, $[s1,s2]^T$ can be any member of set C_1. If a secret pixel is black, i.e. r(i, j) = 0, then each pixel in s1 should complement each pixel in s2 and thus, $[s1,s2]^T$ should be selected from set C_0. The choice of $[s1,s2]^T$ is guided by a random number generator, which determines the random character of the shares.

III. VISUAL CRYPTOGRAPHY AND SECRET IMAGE SHARINGTECHNIQUES AND APPLICATIONS

Lots of algorithms and approaches based on visual cryptography have been proposed and as we expect they are trying to address security issues in communications. In the following section we review some of them.

A. Watermarking

The scheme in [14] explains the use of visual cryptography in watermarking which has two steps:

1. Watermark embedding.
2. Watermark retrieving.

In the first step, the watermark embedding, a watermark is split into two shares by using visual cryptography technique. Then, one of the two shares is embedded into the frequency domain of the host image, and the other is distributed to the owner[14]. To prove the ownership, the owner has to address his/her share, extract the other share from the image and then combine these two shares to reveal the watermark. Based on the security condition of visual cryptography, we can make sure that the two shares cannot leak any information about the watermark. This application is discussed in [14].

B. Anti- Phishing Systems

Phishing websites aims to steal sensitive and personal information such as passwords, credit cards numbers, pins, etc [23]. They trick customers by making identical web site to a real one where the customer submits his information [23]. In [15] the author tries to address that issue by applying visual cryptography technique. In this context, customer can ensure if this is the genuine web site or not by typing his user name. The server will send a share from its database. The client will superimpose his own share with the one sent by the site to ensure this is not phishing web page and then user can type the information[15].

C. Human machine identification

The author in [3] proposed a scheme for the identification of human and terminal. They further extended Katoh and Imai's [4] scheme into a more generalized form, in which their extended form concealed several query images in a single display image [3]. They then extended Droste's [36] scheme into a generalized scheme such that the combination of the transparent shares concealed independent secret images. The steps for the human-machine identification are as follows [3]:

1. The user and the terminal both are associated with an identity (ID) and they both share a secret. A slide is distributed to the user which is generated by a (2, 2) Visual Secret Sharing Scheme.
2. The user provides his ID to the terminal so as to acquire access to the service.
3. The display image is then displayed on the screen on which the user overlaps his initially acquired share to get the secret message.
4. A simple operation is then carried out by the user in which he uses the message and the share secret (which was shared initially). The inference of this operation is then provided to the terminal.

D. Authentication for Data Matrix Code

Sharma and Rao [6] used Visual Cryptography authentication for Data Matrix Code in Identity cards. They proposed two levels of security of the Identity Card.

1. The authentication of the Identity Card.
2. The identity of the Identity Card owner.

Data Matrix Code is used to address the authenticity and security of the vital information of the owner such as credit card number, contact number, address or even photograph[6]. Data Matrix Code is an optical, machine readable representation of data which uses the vertical dimension to store and retrieve information. Two 2D Data Matrix Codes are used in an Identity Card for storing private and public data. The first Data Matrix Code stores information that helps in digital logging and recording of information from the Identity Card. The second Data Matrix Code contains private information in the encrypted form. The first Data Matrix Code is known as the "Public Data Matrix Code" and the second Data Matrix Code is known as the "Private Data Matrix Code".

The authentication process contains two levels. In the first level the Public Data Matrix Code and a master seed is used both of which is unknown to the owner of the Identity Card. The master seed contains the key for authentication of the Identity Card[6].

The second level authenticates the owner of the Identity Card. This level uses both the Data Matrix Codes as its shares and reveals the facial image of the owner hence authenticating the owner of the Identity Card[6].

E. Offline QR Code Authorization

Fang [7] proposed an algorithm for the authentication of offline QR (Quick Response) code. He used Visual Secret Sharing Scheme for the authentication. A QR code is matrix barcode which is readable by specific readers dedicated to QR code [7]. The code consists of a white background on which black modules are arranged in a square pattern. The information that is encoded in a QR code can be any text or URL or any other data [7]. There are six important features of a QR code [7]:

1. High capacity encoding of data.
2. Small printout size.
3. Dirt and damage resistance.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 3, March 2017

4. Readable from any direction in
5. A structure append feature.

A QR code can append 7089 numeric characters for numeric data. A QR code must contain an encoding region and a function pattern viz., finder, separator, timing patterns and alignment pattern. Function pattern should not be used for encoding data. The code is surrounded by a quiet zone on all the four sides [7].

F. Defense System

Visual Cryptography Scheme is an encryption method that uses combinational techniques to encode secret written materials[17]. This can be very useful in defense system to protect very sensitive data, when data like password or any code is to transferred from one place to another that secret data can be it can hidden in cover image, the share of the image is to be converted into shares. Those multiple shares can be kept with multiple partners[17]. Any one partner cannot retrieve the secret code from the single share he has, all the shares from all the partners are required to retrieve secret information hidden in the image[17].

G. CAPTCHA

CAPTCHA was proposed in [8] as a method for authentication based on Visual Cryptography. It stands for Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA). Their method consists of three processes:

Share Creation Process: User registers by furnishing their credentials such as name, date of birth, address, PIN, etc[8]. These credentials are stored in the database. The secret PIN number provided by the user will act as a basis for the creation of the CAPTCHA image unique in nature. The CAPTCHA is then divided into two shares. One share is stored in the database and the other is given to the customer[8].

Hash Code Generation: MD5 is used for the hash code generation. MD5 transforms a variable length message into a fixed length output of 128 bit. The input message is divided into blocks of 512 bits. The message is padded in such a way that its length becomes completely divisible by 512[8].

Authentication Process: The customer needs to provide his share for any transaction. A hash code is generated for the share and the value is compared with the value already stored in the database[8]. If a match occurs, the customer share is stacked with the share present in the database server. The stacked image is then processed to remove any noises. Then the authentication testing is done to accept or reject the user.

H. Signature Based Authentication

Visual cryptography can be applied for user authentication. In this context, authentication can be done using shares to prevent the systems from some attacks[20,21]. Any institute can be considered as an application for this scenario. Firstly, employees will register in the system, the signature of the employee is scanned and entered in the system to get its key share this key is printed on a card and given to the employee and the simple share is entered to the system database[18,32]. During authentication, the employee inserts his own card in the card reader mounted in the entrance to read the key share from the card and superimposes over the corresponding simple share available in the database.

I. Fingerprint based Authentication

Biometrics is the detailed measurements of human body [32, 36]. It deals with the automated methods of identifying on individual and verifying his identity. The scheme proposed by [9] consists of two processes:

Registration process: In the registration process they considered the fingerprint as the secret image and made two shares out of it. One share is stored in the database. The other share is embedded into the photo identity card of the user[9]. The share stored in the database is known as the "dummy share" and the share that is passed on to the user is known as the "participant share".

Authentication process: In the authentication process the photo identity card of the user is produced[9]. The participant share is extracted from the identity card and is overlapped with the dummy share. This gives the fingerprint of the user which authenticates his identity[9].

IV. CONCLUSION

Visual cryptography (VC) scheme is a cryptographic technique which allows visual information to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. The main advantage of visual cryptography is that no computation required to decrypt the final result. This paper is a compilation some of the major applicable areas of Visual Cryptography. There are still many areas which have not been coupled with Visual Cryptography which otherwise would prove beneficial.

The most important part of any visual cryptography is the contrast of the recovered secret from a particular set of shares, as it is not going to be the same as the input image. So there is still room for developing more efficient ways to address this problem.

REFERENCES

[1] Naor, Moni, and Adi Shamir. "Visual cryptography." In Workshop on the Theory and Application of of Cryptographic Techniques, pp. 1-12. Springer Berlin Heidelberg, 1994.
[2] Lin, Chang-Chou, and Wen-Hsiang Tsai. "Visual cryptography for gray-level images by dithering techniques." Pattern Recognition Letters 24, no. 1 (2003): 349-358.
[3] Kim, Mi-Ra, Ji-Hwan Park, and Yuliang 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] Katoh, T., and H. Imai. "An Application of Visual Secret Sharing Scheme Concealing Plural Secret Images to Human Identification Scheme." In Proc. of SITA, vol. 96, pp. 661-664. 1996.
[5] Lin, Chang-Chou, and Wen-Hsiang Tsai. "Secret image sharing with steganography and authentication." Journal of Systems and software 73, no. 3 (2004): 405-414.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 3, March 2017

[6] Sharma, M. Agnihotra, and M. Chinna Rao. "Visual cryptography authentication for data matrix code." International Journal of Computer Science and Telecommunications 2, no. 8 (2011): 58-62.
[7] Fang, Wen-Pinn. "Offline QR Code authorization based on visual cryptography." In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011 Seventh International Conference on, pp. 89-92. IEEE, 2011.
[8] Vinodhini, A., and L. Jani Anbarasi. "Visual Cryptography for Authentication Using CAPTCHA." International Journal of Computer and Internet Security 2, no. 1 (2010): 67-76.
[9] Rao, YV Subba, Yulia Sukonkina, Chakravarthy Bhagwati, and Umesh Kumar Singh. "Fingerprint based authentication application using visual cryptography methods (improved id card)." In TENCON 2008-2008 IEEE Region 10 Conference, pp. 1-5. IEEE, 2008.
[10] Walden, Disa E. "A Benchmarking assessment of known visual cryptography algorithms." PhD diss., Rochester Institute of Technology, 2012.
[11] Hou, Young-Chang. "Visual cryptography for color images." Pattern recognition 36, no. 7 (2003): 1619-1629.
[12] James, Divya, and Mintu Philip. "A novel anti phishing framework based on visual cryptography." In Power, Signals, Controls and Computation (EPSCICON), 2012 International Conference on, pp. 1-5. IEEE, 2012.
[13] Houmansadr, Amir, and Shahrokh Ghaemmaghami. "A novel video watermarking method using visual cryptography." In Engineering of Intelligent Systems, 2006 IEEE International Conference on, pp. 1-5. IEEE, 2006.
[14] He, Warren, Devdatta Akhawe, Sumeet Jain, Elaine Shi, and Dawn Song. "Shadowcrypt: Encrypted web applications for everyone." In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 1028-1039. ACM, 2014.
[15] Reddy, L. Siva, and Munaga VNK Prasad. "Extended Visual Cryptography Scheme for Multi-secret Sharing." In Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, pp. 249-257. Springer India, 2016.
[16] Russ, John C. The image processing handbook. CRC press, 2016.
[17] Arafin, Md Tanvir, and Gang Qu. "Secret sharing and multi-user authentication: From visual cryptography to RRAM circuits." In Proceedings of the 26th edition on Great Lakes Symposium on VLSI, pp. 169-174. ACM, 2016.
[18] Doroodchi, Mahmood, Azadeh Iranmehr, and Seyed Amin Pouriyeh. "An investigation on integrating XML-based security into Web services." In GCC Conference & Exhibition, 2009 5th IEEE, pp. 1-5. IEEE, 2009.
[19] Martin, V. Maria Antoniate, K. David, and P. Mesiya. "A Survey on Visual Secret Sharing Scheme." Software Engineering and Technology 8, no. 4 (2016): 91-96.
[20] Pouriyeh, Seyed Amin, and Mahmood Doroodchi. "Secure SMS Banking Based On Web Services." In SWWS, pp. 79-83. 2009.
[21] Garfinkel, Simson, and Gene Spafford. Web security, privacy & commerce. " O'Reilly Media, Inc.", 2002.
[22] Pouriyeh, Seyed Amin, Mahmood Doroodchi, and M. R. Rezaeinejad. "Secure Mobile Approaches Using Web Services." In SWWS, pp. 75-78. 2010.
[23] Akhawe, Devdatta, Adam Barth, Peifung E. Lam, John Mitchell, and Dawn Song. "Towards a formal foundation of web security." In Computer Security Foundations Symposium (CSF), 2010 23rd IEEE, pp. 290-304. IEEE, 2010.
[24] Zhou, Zhi, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography." IEEE transactions on image processing 15, no. 8 (2006): 2441-2453.
[25] Sharma, M. Agnihotra, and M. Chinna Rao. "Visual cryptography authentication for data matrix code." International Journal of Computer Science and Telecommunications 2, no. 8 (2011): 58-62.
[26] Allahyari, Mehdi, Krys J. Kochut, and Maciej Janik. "Ontology-based text classification into dynamically defined topics." In Semantic Computing (ICSC), 2014 IEEE International Conference on, pp. 273-278. IEEE, 2014.
[27] Yan, Wei-Qi, Duo Jin, and Mohan S. Kankanhalli. "Visual cryptography for print and scan applications." In Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on, vol. 5, pp. V-V. IEEE, 2004.
[28] Shahab, Elham, and Hadi Abdolrahimpour. "A Comprehensive Investigation of Visual Cryptography and its Role in Secure Communications."
[29] Safaei, Saeed, Hajar Mozaffar, and Babak Esmaeili. "Solving Minimum K-Center Problem in the Adleman? Lipton Model." In FCS, pp. 251-255. 2008.
[30] Liu, Feng, and Wei Qi Yan. Visual Cryptography for Image Processing and Security. Vol. 2. Springer, 2014.
[31] Assefi, Mehdi. "Optimizing The Locking Methods in Distributed Database Systems." In Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA), p. 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012.
[32] Hegde, Chetana, S. Manu, P. Deepa Shenoy, K. R. Venugopal, and L. M. Patnaik. "Secure authentication using image processing and visual cryptography for banking applications." In Advanced Computing and Communications, 2008. ADCOM 2008. 16th International Conference on, pp. 65-72. IEEE, 2008.
[33] Blundo, Carlo, Alfredo De Santis, and Moni Naor. "Visual cryptography for grey level images." Information Processing Letters 75, no. 6 (2000): 255-259.
[34] Tunga, Harinandan, and Soumen Mukherjee. "Design and Implementation of a Novel Authentication Algorithm for Fool-Proof Lock-Key System Based On Visual Secret Sharing Scheme." IJCSI International Journal of Computer Science Issues 9, no. 3 (2012): 1694-0814.
[35] Ko, Teddy. "A survey on behavior analysis in video surveillance for homeland security applications." In Applied Imagery Pattern Recognition Workshop, 2008. AIPR'08. 37th IEEE, pp. 1-8. IEEE, 2008.
[36] Droste, Stefan. "New results on visual cryptography." In Annual International Cryptology Conference, pp. 401-415. Springer Berlin Heidelberg, 1996.