Schemes and Applications of Visual Cryptography

Grusha Kaur Sahni
Department of CSE (Cyber Security and Digital Forensics), KLEF, Vaddeswaram, A.P, India.
grushakaursahni30@gmail.com

Hari Kiran Vege
Department of CSE, KLEF, Green Fields, Vaddeswaram, A.P, India.
hari.vege@kluniversity.in

Abstract – Visual cryptography is a form of encryption which is applied on images and all visual information such as handwritten data, signatures, financial documents etc. Here the data is encoded into unidentifiable format and to decrypt the encoded message no algorithm in cryptography was able to perform the decryption job. And the decryption was only done when all the shares are overlapped equally that too in a mechanical way of printing the shares on a transparent sheet. Here in this paper We explained different types of schemes in visual cryptography and the application in this technique. There are more number of schemes are proposed and these are popular and main schemes and application in visual cryptography.

Index Terms – Visual Cryptography, Shares, Visual information.

1. INTRODUCTION

1.1. Cryptography

Cryptography is a process of converting a readable data into an unreadable format which is used to provide security to the data which we want to hide from third party users or unauthorized persons. It helps us to keep data secure and protect the documents which are digitally signed. Figure1 shows the general procedure of the operation of cryptography. Encryption converts the readable data into unreadable format. Decryption converts the unreadable text into readable text.

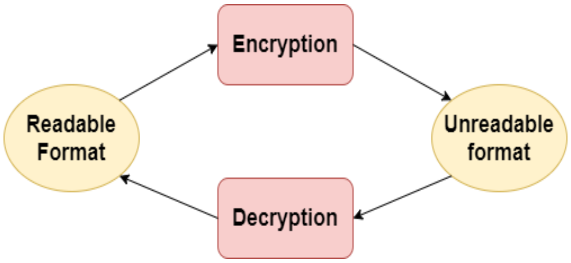

Figure 1: General Procedure of Cryptography

1.2. Visual Cryptography

Visual cryptography encrypts the visual data into the form of unidentified pixels and the specialty of this technique is it decryption process. The decryption process of this cryptography technique doesn't need any type of computational work or any other procedures. To decrypt the encrypted image user has to do it mechanically by taking the prints of the encrypted images in a transparent sheet and then has to overlap the images equally and remaining process was done by human visual system. The general procedure is shown in Figure 2.

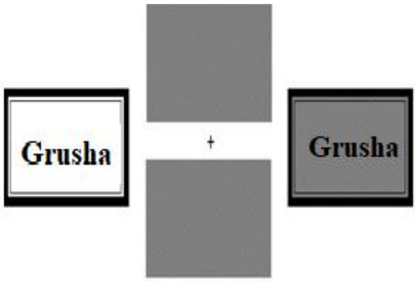

Figure 2: General Procedure

2. VISUAL CRYPTOGRAPHY SCHEMES (VCS)

2.1. 2 Out of 2 VCS

In this scheme, by using any one of these two shares information which was hidden wasn't displayed [1]. To see the original image from the share or parts, 2 out of 2 scheme is shown in Figure 3. It is also called as general visual cryptography scheme. At the time of superimposing two shares, the result will be black.

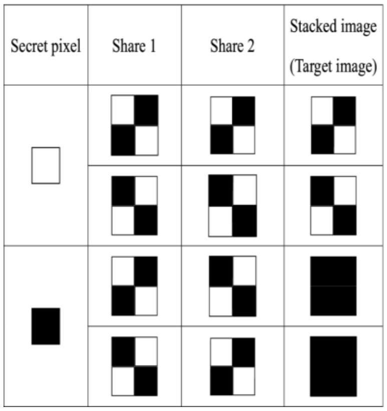

Figure 3: visual Cryptography (2,2) process

2.2. k Out of k VCS

This scheme is just like the above VCS. Here it was divided in k number of shares, and encrypted was only revealed by k number of shares only [2]. If the shares are k-1 the encrypted image doesn't reveal.

If the image was divided into 3 shares or parts, the encrypted image was only revealed by using all the shares without of any one of those three shares the encrypted image doesn't revealed [20].

If the image is divided into 4 share or parts, the image which was encrypted was revealed only by using the four parts without of any one of those four parts the image wasn't decrypt.

2.3. VCS for General Access

As I explain in k out of n VCS image will be decrypt with k number of shares, and it is not revealed with k-1 or less shares than k. This scheme divides the given n share of the encrypted image are divided into two subsets named as permitted and not permitted or forbidden [3]. And from forbidden subset k or more shares don't reveal any secret image. Like this security will be increased in k out n VCS with this scheme.

2.4. Halftone VCS

In this, the process of share creation it replicates the tone continuously to image. They called as halftone cells and these cells are stored in each and every 'n' share [10]. By the usage of halftone cells with a particular size, then the halftone shares will be obtained. And this technique increases the quality and makes the good contrast to the shares.

2.5. VCS for Colour Images

This scheme was first proposed in the year 1997 by Verheul and Van Tilborg[5]. All the remaining scheme only work on black and white only, but this scheme works on both black & white and colour images also. Colour region is filled with a colour and other colour regions are coloured in black.

After the proposal of this scheme authors F.Liu [6] proposed three approaches in this scheme. The new approaches are as follows:

In first method, Shares are printed directly with colour. This works just like the normal visual cryptography[3], and it leads to some limitations like decoded image quality is reducing and it need large pixel expansion

In second method, there are three colours Red, Green, Blue are used as channels for additive operation and another three colours Cyan, Magenta, Yellow used as channels for subtractive operation [23]. After this general procedure of visual cryptography which was applied. This overcome the limitation of pixel expansion by reducing the expansion of pixels, but the image quality is reduced due to the process of halftoning.

In third method, it is represented in binary and is encrypted at bit-level [14]. This method overcomes the other limitation of image quality, and it gives the resultant image in a better quality.

2.6. Extended VCS (EVCS):

The share which has noise will gets the attention of hackers and the hacker who identifies this noise in share may suspect that there is a content in the noise like image [21]. This may lead to the security issues. And maintaining the noise like images is also a risk.

To overcome this risk Yamaguchi, Y. developed a scheme called EVCS [7]. This scheme helps to create meaningful shares and it helps to ignore noise problems.

2.7. Segment based VCS:

This is a new scheme in Visual Cryptography, and it was proposed by Bernd Borchert to overcome the limitation of pixel-based VCS loss its contrast while decrypted or restored image which is directly proportional to the expansion of pixel.

And in this scheme, it doesn't use pixels, but it works based on segments. This scheme is very useful to encrypt a message which contain symbols with text can be represent in segment display [2]. The advantage of this scheme is secret symbols and images are shown easily.

2.8. Region Incrementing VCS:

In general procedure of visual cryptography [18], while decrypting it may reveal the full image or nothing. And this is a limitation in general procedure of visual cryptography.

To overcome this limitation Ran-Zan Wang developed a scheme and it is called as Region Incrementing VCS [8]. This scheme can able to share multiple levels of secrecy in a single image, because here for a secret image different encoding rules are applied based on secrecy level.

Here in this scheme a different type of rules are applied to each and every region and for every region there is a separate rule is applied and it provides a different level of security[15] than applying the same encoding rule to the entire image and increases the security level when compare with other schemes in visual cryptography.

3. VISUAL CRYPTOGRAPHY APPLICATIONS

3.1. Watermarking

The watermarking works on using visual cryptography technique. And its process is of following steps:

- Watermarking Embed

- Watermarking Retrieve

In embedding method, the watermark is divided by using visual cryptography technique [17]. After dividing into share one share was embedded into the secret image's frequency domain and another share is dispersed to the owner.

The share owner contains a share which helps to prove the ownership on the image and watermark like by combining the share which was the owner has and the other one which was embedded with original image at frequency domain[16]Based on the visual cryptography technique the two shares don't reveal any kind of information about watermark.

3.2. Anti- Phishing System

As we know phishing is an attack which steals the sensitive information like passwords, pin numbers and other details by replicating the original website [9]. By using visual cryptography technique to a website, a user can identify the difference between the duplicate website and an original website.

This works as whenever a user tried to enter information then the website server sent a share to the user, then the user superimposes those two shares and then user get some code which was assigned.

By seeing the code user can able to understand that the user was accessing original website and if the user doesn't get any share image like from the original then the user can able to identify that the user accessing a fake website.

3.3. Authentication for Data Matrix Code

This application applies two levels of security, it works on the identity cards and it was proposed by Sharma and Rao [11]. Authentication goes through the owner's identity card and in this level, it uses both DMC and shares of the facial image of the owner [22]. By comparing the shares from identity card and data base the user was identified then the identity card owner.

If the process doesn't get any kind of information through the shares which are gathered from the card owner and from data base was superimposed, then the card owner doesn't able to claim that he was the owner of the data.

3.4. Offline QR Code Authorization

This application was proposed by Fang and it is an algorithm which works on offline QR code authentication. The QR code looks like a black square are randomly spotted on a white sheet [12]. Here in this application the author applied visual cryptography and the QR code will become into two shares and the share nearly looks like as QR code so it cannot be scanned by any third-party user and it is very easy and secure to do the transaction with QR codes.

3.5. Defense System:

Generally visual cryptography encrypts the images into of two shares and the encrypted image was only decrypted by those shares only not with other shares [4]. This technique helps to encrypt all visual data like images, codes, handwritten text, etc. This helps in defense to send a secret image like as follows.

First an image was encrypted into two parts and one part was directly given to the person who they want to send message and the other part was sent through the fax or in the form of printed when the time of using that code. And it helps to share the message secretly and in visually.

By using this technique, we can able to send more than two messages secretly to a person who works as a secret agent in a distance location and in a dangerous place, and the procedure to decode the data was only done by that person who receive the share only.

3.6. CAP-T-CHA

CAP-T-CHA is of three processes and work using the visual cryptography and the processes are as follows.

- Shared Create Process
- Hashed Codes Generated
- Authentication Process

If the two shares are matches and then stacked together and then removes noise from the share after that authentication will be accepted otherwise authentication will be rejected [13].

3.7. Signature Based Authentication

This application is used in authentication process of an employee. This works as follows first the employee was registered here, after registration signature is taken and saved After generating, that key share will be printed on the employee identity card, and then if it matches the user can enter otherwise the user is identified as an intruder.

3.8. Fingerprint Based Authentication

Fingerprint is one of the unique identifications of human and it is unique because every two humans doesn't have the same type of fingerprint because of the ridges on the finger [19]. Authentication by using fingerprint helps us to do the operation very fast and easily and using visual cryptography in this system helps to protect the fingerprint from stealing from the database.

This application deals with self-operating methods of identifying and verifying and it consists of two processes, one is registration process and the second one is authentication process.

In the process of registration fingerprint considered as secret image and divided into two parts one is called as dummy share and other is called as participant share and the participant share is saved into user id.

In authentication process the id of user is inserted into the scanner and it scans the participant share and superimposes that share with dummy share in the database [21]. If it matches, then the user can able to authenticate.

If the participant and dummy share doesn't reveal original image, then the user doesn't able to authenticate and easily identified the unauthorized person

4. CONCLUSION

Visual cryptography is to get final result (decryption) of technique the user doesn't require computation. This paper is a collection different schemes and applications of it. It is also applicable to visual cryptography including the applications which are mentioned here. The interesting point of it is that the encrypted shares doesn't appear as same as the real image and without any one of those divided shares no one able to see the real encrypted image. So, no third-party person is able to identify the secret image.

The main motive behind this was to encode and decode images that were to be kept as a secret. The technique to be used depends on many influential functions, some of them are format, size, shapes, and the number of shares. To decrypt all the images, the unified key will be helpful. Our future work will be to decode number of images using a single or a unified key.

REFERENCES

[1] Arafin, M. and Qu, G., 2018. Memristors for Secret Sharing-Based Lightweight Authentication. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 26(12), pp.2671-2683.

[2] Bojjagani, S. and Sastry, V., 2017. A secure end-to-end SMS-based mobile banking protocol. International Journal of Communication Systems, 30(15), p.e3302.

[3] Chaturvedi, A. and Bhat, I., 2015. Analysis of Schemes proposed for improving the Segment Based Visual Cryptography. International Journal of Computer Trends and Technology, 30(1), pp.26-30.

[4] Freyberger, M., He, W., Akhawe, D., Mazurek, M. and Mittal, P., 2018. Cracking ShadowCrypt: Exploring the Limitations of Secure I/O Systems in Internet Browsers. Proceedings on Privacy Enhancing Technologies, 2018(2), pp.47-63.

[5] Gu, Y., Ye, M. and Gan, Y., 2010. Web Services Security Based on XML Signature and XML Encryption. Journal of Networks, 5(9).

[6] Hou, Y., 2003. Visual cryptography for color images. Pattern Recognition, 36(7), pp.1619-1629.

[7] International Journal of Science and Research (IJSR), 2015. A Review of Image Steganographic Technique Based On Extended Visual Cryptography Scheme. 4(11), pp.935-937.

[8] James, D., 2012. A Novel Anti Phishing Framework Based On Visual Cryptography. International Journal of Distributed and Parallel systems, 3(1), pp.207-218.

[9] Jesalkumari A., J. and Sedamkar, R., 2013. Modified Visual Cryptography Scheme for Colored Secret Image Sharing. International Journal of Computer Applications Technology and Research, 2(3), pp.350-356.

[10] Jin, D., 2005. Progressive color visual cryptography. Journal of Electronic Imaging, 14(3), p.033019.

[11] Jolve. J, M., 2017. Secure Authentication using Image Processing through Visual Cryptography. International Journal Of Engineering And Computer Science,.

[12] Kotthapalli, D. and Anitha, D., 2013. EXTENDING THE VISUAL CRYPTOGRAPHY ALGORITHM USING IMAGE WATERMARKING TECHNIQUE. INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY, 5(2), pp.120-123.

[13] Patel, S. and Rao, J., 2016. A Survey on Sharing Secret Image using NVSS Scheme. International Journal of Computer Applications, 133(16), pp.17-20.

[14] Ran-Zan Wang, 2009. Region Incrementing Visual Cryptography. IEEE Signal Processing Letters, 16(8), pp.659-662.

[15] Shahab, E. and Abdolrahimpour, H., 2017. A Comprehensive Investigation of Visual Cryptography and its Role in Secure Communications. IARJSET, 4(2), pp.1-5.

[16] Shamir, A., 1979. How to share a secret. Communications of the ACM, [online] 22(11), pp.612-613. Available at: <https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf>.

[17] Shyu, S., Huang, S., Lee, Y., Wang, R. and Chen, K., 2007. Sharing multiple secrets in visual cryptography. Pattern Recognition, 40(12), pp.3633-3651.

[18] Wang, R., Lan, Y., Lee, Y., Huang, S., Shyu, S. and Chia, T., 2010. Incrementing visual cryptography using random grids. Optics Communications, 283(21), pp.4242-4249.

[19] Weir, J., Yan, W. and Kankanhalli, M., 2012. Image hatching for visual cryptography. ACM Transactions on Multimedia Computing, Communications, and Applications, 8(2S), pp.1-15.

[20] Yamaguchi, Y., 2004. Enhancing registration tolerance of extended visual cryptography for natural images. Journal of Electronic Imaging, 13(3), p.654.

[21] Yan, X., Wang, S. and Niu, X., 2015. Threshold progressive visual cryptography construction with unexpanded shares. Multimedia Tools and Applications, 75(14), pp.8657-8674.

[22] YU, B., WANG, Y. and FANG, L., 2009. Anti-cheating visual cryptography scheme based on probability. Journal of Computer Applications, 29(7), pp.1782-1784.

[23] Zhang, X., 2018. A Visual Cryptography Scheme-Based DNA Microarrays. International Journal of Performability Engineering.

Authors

Grusha Kaur Sahni is pursuing her M.Tech in the field of Cyber Security and Digital Forensics - Department of CSE, KLEF, Vaddeswaram, Andhra Pradesh, India. She is a university innovation fellow, of the Stanford's D-School. She is a graduate who completed her B.Tech at Godavari Institute of engineering and technology, Rajahmundry, Andhra Pradesh, India.

Mr Hari Kiran Vege is an Experienced Lecturer with a demonstrated history of working in the higher education industry. Skilled in Oracle Database, Computer Science, Data Science, Full Stack Web Development and Algorithms. Strong education professional with a (PhD) Masters in Engineering Science (Research) focused in Microelectronics from The University of Western Australia.