AN OVERVIEW OF DIFFERENT VISUAL CRYPTOGRAPHY TECHNIQUES

[1]Omkar Pattnaik, [2] Ranishree Patel, [3] Aparna Mahapatra, [4]Sasmita Pani

[1]Assistant Professor, [2]Final year student, [3]Final year student, [4]Assistant Professor

[1] Department of Computer Science and Engineering,
Government College of Engineering, Keonjhar, Odisha, Postal Zip-758002, India.
**Corresponding author Email: omkar29in@gmail.com*

Abstract:
An emerging technology to overcome the issues with image privacy is visual cryptography. The keyword "visual" in visual cryptography refers to the ability of a user to recognize the decrypted secret using his or her visual system during the decryption step without the involvement of computers. In this process secret pictures are divided up into many shares and the original image is recovered by digitally or practically overlapping the shares. The metrics that are used to evaluate the viability of visual cryptography methods have been explained.
Existing studies that have already been written in this domain only discuss a few different visual cryptography techniques or which may not be compare different schemes properly. To fill this gap, this paper offers a thorough overview of the subject to help new researchers in finding appropriate visual cryptography techniques for their intended applications.

Keywords: Visual Cryptography (VC), Encryption, Decryption, Secret shares.

I. INTRODUCTION

In this world, information is transmitted via the internet as images, audio, video, text, etc. format. In today's increasingly cybercrime scenario, data security has become a major concern for the diverse communities that spend a lot of money securing their information. Visual cryptography is the encryption of visual information so that decryption can be performed by the human receiver with eye vision only.
In this survey, we highlight different applications of "visual cryptography", "such as converting a secret image into two or more irrational, non-identical shares without using any encryption keys. The invisible secret can only be revealed when the required number of shares are combined with each other. Today, visual cryptography is a desirable scheme as it embodies both the perfect secrecy scheme and a very simple mechanism to recover the secret."

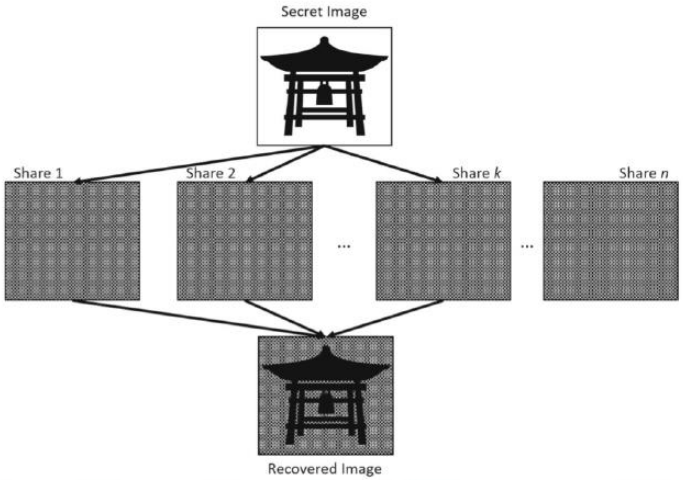

Fig-1: Visual cryptography with (k, n) process. [22]

In this technique, the visualization of the human system is the key factor for the decryption process. This allows anyone to take advantage of the system without doing any calculations or knowing any cryptographic knowledge. In addition, Visual Cryptography Techniques do not require any key for encryption/decryption as in other encryption techniques. This technique provides greater security and can be implemented without much difficulty. An electronic secret can be shared simply. Conversely, secrets can be printed on transparencies and superimposed to reveal the secret.

The "two main aspects of Visual Cryptography Techniques are contrast and security. Researchers have been recommending various techniques to increase contrast and safety for many years. The researchers suggested that in the case of binary images, logical XOR operation rather than OR operation can improve contrast. Shares created in visual cryptography techniques are random noise-like posts. Encryption Visual Cryptography Techniques have been proposed to increase the security of shares by making shares meaningful to reduce the suspicion that something is hidden there. In other words, the shares in Encryption Visual Cryptography Techniques include the cover image and the confidential information of the original hidden image. Cover art can be a binary image, grayscale image", or color image.

The remainder of this paper is organized as follows: In Section II, Literature survey work is mentioned; Section III represents the Basics terminology of cryptography; section IV describes various Visual cryptography schemes; Section V includes Visual Cryptography Metrics; Section VI provides the idea regarding Applications of Visual Cryptography; Section VII represents Other Cryptography Technologies; Section VIII concludes with possible future extensions.

II. LITERATURE SURVEY

SL NO.	TITLE	AUTHOR NAME	YEAR PUBLISHED	FINDINGS
1	"Extended visual cryptography techniques for true color images."	Kirti Dhiman, Singara Singh Kasana	2018	Two EVCT techniques have been proposed for sharing color images. The first technique is (3,3) ECVT and the second is (2,3)ECVT. Finally, a color hidden image can be shared without any information loss.
2	"Design and Implementation of a Secure QR Payment System Based on Visual Cryptography."	Lina Ahmad1, Rania Al-Sabha2, Ali Al-Haj3	2021	A secure payment application is proposed that provides a user-friendly interface for users to perform QR code-based payment transactions. When the VC is integrated with the QR system, it becomes extremely secure and very difficult to tamper with the QR code.
3	"Design and implementation of a visual cryptography application."	Petre Anghelescu , Ionela Mariana Ionescu, Marian Bogdan Bodea	2020	According to the VC algorithm, an image between 2 and 4 pages will be formed after encryption. Decryption is accomplished by superimposition "and visual recognition by the human eye. Input data can be images or text, and "visual cryptography" can be based on the black and white method or the color method."

4	"Novel Authentication System Using Visual Cryptography."	Jaya, Siddharth Malik, Abhinav Aggarwal	2011	The application of VC in the financial field is examined. The "proposed system improves the security level for authentication by checking the decrypted client image and signature."
5	"An Extended Visual Cryptography Algorithm for General Access Structures."	Kai-Hui Lee and Pei-Ling Chiu	2011	Previous approaches to EVCS have suffered from pixel expansion issues. Therefore, this article proposes a method to solve this problem. In the first stage, "meaningless shares are created with an optimization technique and configuration for conventional VC schemes. In the second step, cover images are added directly to each post using a stamping algorithm. Experimental results show that this approach provides a better result in terms of imaging, contrast, reconstruction of black hidden pixels, and maintaining the same aspect ratio as in the original image."
6	"Applications and Usage of Visual Cryptography: A Review."	Anjney Pandey, Subhranil Som	2016	This article presents a study "on the application areas of visual cryptography from different research articles. The main focus is on the use of encryption segments, which is the most important" feature of "visual cryptography".
7	"An Extensive Review on Visual Cryptography Schemes."	J.Ramya, B.Parvathavarthini	2014	This article analyzes the performance of VC based on pixel expansion, "number of hidden images, image format and

				generated share type. In addition, different schemes were studied and their performance was evaluated on the basis of four main parameters such as the number of hidden images, pixel expansion, image format and the type" of sharing created.
8	"Visual cryptography: A brief survey."	P. Punithavathi & S. Geetha	2017	Different "visual cryptography schemes and metrics are discussed in this survey document. In VC it becomes very important to ensure that the input images are completely lost and a clear hidden image is recovered, which could be another image."
9	"An overview of visual cryptography techniques."	DyalaR.Ibrahim, JeSenTeh, RosniAbdullah	2021	This article discusses current issues in VC "such as pixel expansion, poor quality of recovered image quality, computational and memory complexities. There are schemes that can encrypt multiple secrets but are inefficient or difficult to use." More research is still needed in this area.

10	"Review of Models, Issues and Applications of Digital Watermarking Based on Visual Cryptography."	J.H Saturwar, D.N. Chaudhari	2017	In this paper, the different existing models of visual cryptography with digital watermarking and how their combination can provide better security has been studied. Some applications include Visual Authentication , Identification, Steganography and Image Encryption
11	Visual Cryptography-A Review.	Dipesh Vaya, Sarika Khandelwal, Teena Hadpawat	2017	In this post, a hidden image is transformed into many shares that are full of noise but meaningful. When we combine all the shares, we can only see the real image. In this study, a detailed examination was made on color images based on Shamir encryption method of n encryption method over k.
12	A Review On Visual Cryptography Schemes	Siddharth Nagar, Thottempudi Kiran, K. Rajani Devi	2012	In this article, we found the working and performance analysis of "visual cryptography" techniques based on pixel expansion, image format and share types created. Mainly, this article explains in detail the available image encryption methods.
13	"Secure Iris Authentication Using Visual Cryptography."	P.S.Revenkar, Anisha Anjum, W.Z.Gandhare	2010	In this article, "visual cryptography" technique is used in biometric templates stored in the central database, the real customer won't be allowed to access the data or information as it can be changed by the attacker. To deal with this

				issue, this article gives a complete idea of the security needs and the extra layer of authentication, it is also in the iris template for added security.
14	"A Comprehensive Study of Visual Cryptography."	Jonathan Weir, WeiQi Yan	2010	This article summarizes the complete work on the latest developments in visual cryptography since 1994. This article is based on the work done to summarize the current problems and their possible solutions. It also gives an idea about future VC work with appropriate vc applications.
15	"A Review New Methodology for Visual Cryptography in Color Image Based On Cyclic Shift Pixel Method."	Namrata Joshi, Vishal Sharma	2012	This article describes a new type of "visual cryptography implementation for native images. In this, a natural image is shared between different images. Here, vcs is studied and also the performance of the number of hidden images, pixel expansion, image format and created share types is evaluated. We also found vcs for color images based on cyclically changing pixels with cheater ID."
16	"RGB Based Secret Sharing Scheme in Color Visual Cryptography."	M.Karolin, Dr.T.Meyyapan	2015	In this paper, the authors proposed a unique technique for 256-color images converted to 16 standard RGB color formats. Floyd-Steinberg dither algorithm and XOR based VC are used here to do all the activities. We found the

				posts excellent security and quality visual image.
17	"Visual Cryptography."	Moni Naor Adi Shamir	1995	In this article, we found a safe and easy technique, i.e., from the problem of n secret sharing, where an image is divided into n shares and encrypted, and to decrypt this image, we found a safe and easy technique where the minimum k number of shares is sufficient to get the original image. We determined that if the minimum numerator is k-1, we cannot get the original image.
18	"Visual Cryptography: Review and Analysis of Existing Method."	Arun Kumar Chattonadhvav Debalina Ghosh Ram Sekher Pati	2019	In this article, we found out how VCS helps to transmit confidential data very securely in different electronic media. The authors provide detailed information on the various VCS available.
19	"Visual Cryptography Based Multilevel Protection Scheme for Visualization of Network Security Situation."	Hao Hua Yuling Liu Yongwei Wang	2018	In this paper, VC Scheme is proposed, which deals with encoding a secret image related to network security. The authors developed the AS(GAS)-based model called RIVCS, and also designed algorithms for the privacy level and created coding matrices. They provide a "multi-level security privacy protection scheme based on RIVCS."
20	"XOR-based visual cryptography schemes."	P. Tuyls H. D. L. Hollmann L. Tolhuizen	2015	This paper shows that there are n of n "schemes with optimal resolution and contrast, and (2, n)

				schemes are equivalent to binary codes." Basically, in this paper it was found that XOR based visual cryptography is much better than OR based visual cryptography.

III. BASICS TERMINOLOGY OF CRYPTOGRAPHY

Plain Text: Text that requires confidentiality when transmitted over the public network.

• Ciphertext or ciphertext: Plain text that is converted into an unreadable form after encryption is known as ciphertext.

• Encryption: The process of converting plain text to ciphertext using "an encryption approach and a secret key.

• Decryption: At the receiver side, the ciphertext is converted to plain text using the decryption approach and a secret key. This process is known as decryption.

• Key: The security of the encryption approach mainly depends on the key. It can be numeric or alphanumeric. Both encryption and decryption need the key to perform their respective operations. Strong keys are always needed for better information security."

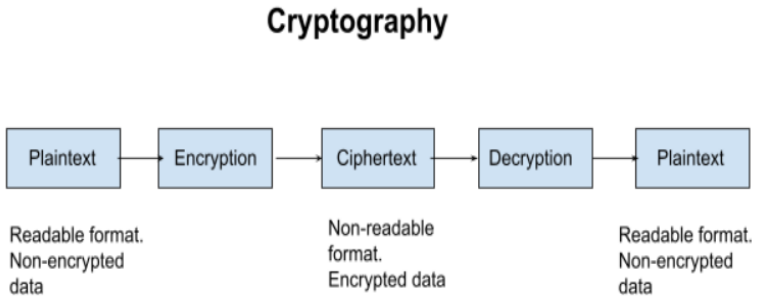

Fig-2: Process of Cryptography

- Cryptography mainly divided into two groups like: Symmetric Cryptography (Same Key is used for encryption and decryption) and Asymmetric Cryptography (Different Key is used for encryption and decryption).

- Symmetric Cryptography:

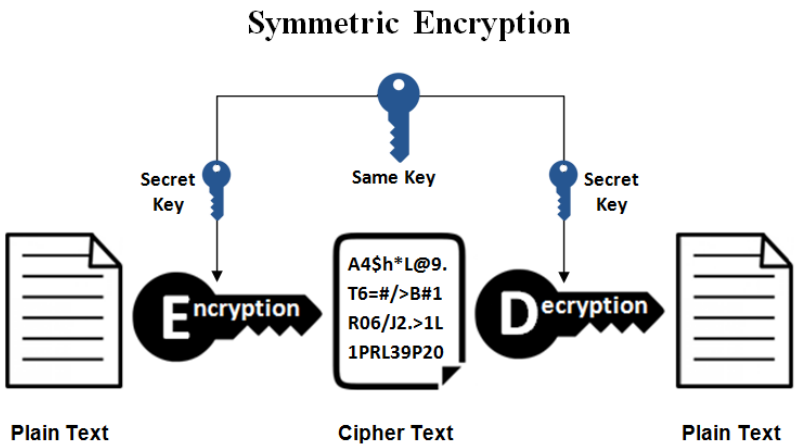

Fig-3: Symmetric Cryptography Process

- Asymmetric Cryptography:

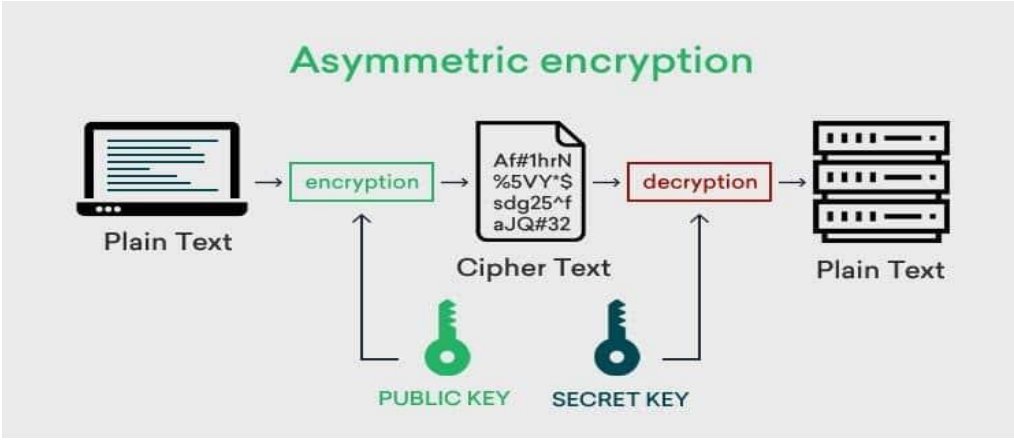

Fig-4: Asymmetric Cryptography Process

IV. DIFFERENT VISUAL CRYPTOGRAPHY TECHNIQUES

An essential method for security purposes is visual cryptography (VC). These visual cryptography techniques are mostly used to distinguish between machines and people. Only human eye can repair an image that has been encrypted using visual cryptography; a computational approach can never do so.

An overview of different visual cryptography systems will be covered in this section. To use a sharing formation approach, the secret picture is separated into two or even more portions inside the VC. The binary, grayscale, and color input picture types and the result of conducting applied throughout sharing restoration are the basis for the VC categorization addressed in this article.
The details of each scheme are described below:

A. IDEA ON VISUAL CRYPTOGRAPHY USING BINARY IMAGE

"Visual Cryptography" schemes for sharing 2 hidden images in two shares are presented in [12]. During this scheme, it is assumed that 2 hidden binary images are hidden in two random shares, namely share A and B. Decryption is accomplished by combining 2 shares with XOR operation like A XOR B, and the second secret is discovered by the first returning share. Θ counterclockwise with respect to angle A[14].
In these two hidden images, it is hidden in 2 share images with impulsive rotation angles. Two sets of latent data are encoded into shadow images under completely different overlapping angles. This scheme is one of the most promising approaches to visual cryptography.

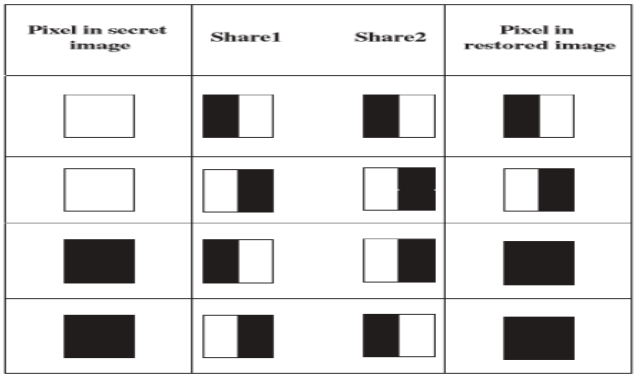

Fig-5: Coding table of share blocks [23].

B. REVIEW BASED ON "EXTENDED VISUAL CRYPTOGRAPHY"

"The concept of enlarged visual cues was first introduced in 2001 [20] but the authors [19] did a great job and that was amazing. This was entirely based on the pixel based visual cryptography proposed in 1995 [1]."

Basically, it is a type of encryption technique that encodes a set of pictures in a way that when the picture reflections are put together, without altering the appearance of the main image, the concealed message is revealed. EVCS (Extended Visual Cryptography Scheme) can also be considered as a steganography technique. One application of EVCS is the removal of custom checks, there will be less possibility that stocks will be questioned and discovered since this EVCS supplied images are significant. EVCS performs better than VC, however pixel expansion is a little higher.

Therefore, the authors explain [10] to stop pixel enlargement, a new updated visual coding approach was proposed. This approach involves placing random shares on meaningful overlay shares, also known as embedded EVCS.

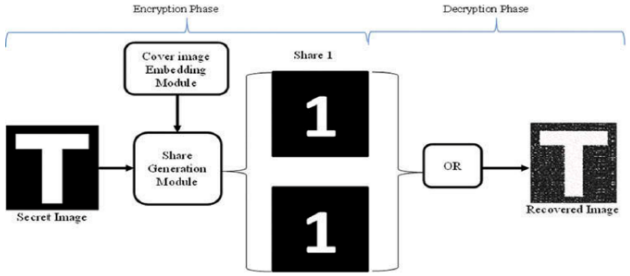

Fig-6: Extended Visual Cryptography [23].

C. GRAYSCALE AS WELL AS COLOR IMAGE VISUAL CRYPTOGRAPHY-BASED ANALYSIS

Visual Cryptography scheme makes sure that attackers cannot deduce any information around a concealed image from a cover image. Before encrypting, grayscale and color photos need to be preprocessed to transform those to binary data. Typically, the halftoning procedure is used to do this. “Halftoning is just a photocopy technique that simulates continuous-tone” pictures by using dots with varying sizes or spacings to produce an impression akin to a transition. There is infinity many shades of grey or colors in this picture. [23].

Through the use of halftone processes, visual representations are reduced to an image created using only one ink color at locations with varying sizes or spacings. The visual functioning of the human eye combines these small halftone bits into uniform tones. Visual cryptography enlarges the image area by incorporating halftoning techniques since halftone "visual cryptography" (HVC) increases number of pixels. By acquiring valuable visual input in visual privacy preserving schemes, a concealed picture can be encrypted into halftone bits. Different halftoning methods exist, including “thresholding, error propagation, random dithering,” and many others.

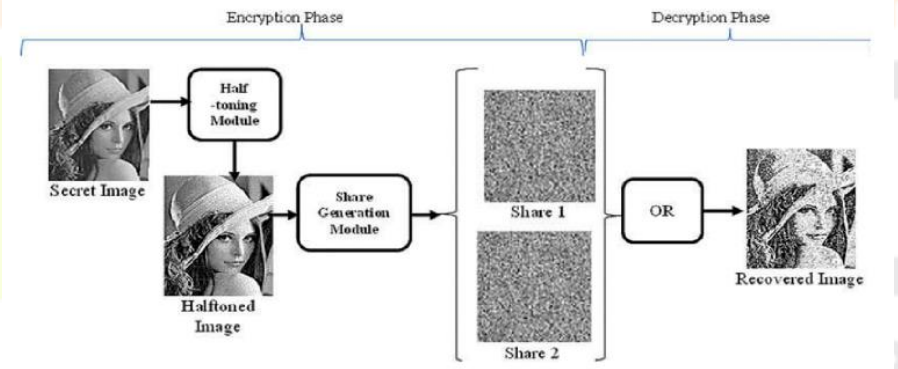

Fig-7: VC for grayscale image using halftoning technique [23].

The authors [1] proposed a new VC (visual cryptography) “for grayscale images using error diffusion. Their method embedded one latent image into two carrier images with high quality and low computational complexity. The hidden image is decrypted using human vision by stacking two carrier images.” Halftone image

encryption is the same as color image encryption. In [2], the color visual cryptography (CVC) method was introduced by the authors. Shares were produced using error transmission and "visual information pixel (VIP)" synchronization. Also with matrix rearrangement, VIP synchronization prevents color and contrast degradation of the source images. The authors of [3] described a method to compromise biometric data security. The original image is divided into two images using this technique, and the picture is only seen when both pictures are shown at the same moment; otherwise, each individual photo will show nothing.

Since color images are more common and beneficial in many practical scenarios, color visual cryptography (CVC) provides numerous benefits over binary as well as grayscale VC. Additionally, it lessens the possibility of someone learning that it includes sensitive information. The primary default position for CVC is the approach suggested in [4]. Three VC techniques for color and grayscale photos based on “black and white” images were among his suggestions. In order to use standard VC to encryption the concealed image to several shares, color and grayscale photos are transformed to “black and white” format. In other words, “its methods are able to support color and grayscale images, while retaining the features of black and white VC.”

D. REVIEW BASED ON LOGICAL OPERATION VISUAL CRYPTOGRAPHY

Decryption in VC (visual cryptography) is very simple. Shares are combined with each other to recreate the message from individual shares. Logical operations such as 'OR' and “ 'XOR' operations can be used during recovery operations. Based on this, the VC system is classified” as:

i. VC Using OR

When the shares merge, the hidden image is re-established. This is “equivalent to the logical OR operation at the end. VC (visual cryptography) schemes that use the logical OR operation to recover the hidden image are called OR based VC. Pixel-based VC recommended in [11] and [19].”

ii. VC Using AND

In XOR-based VC (visual cryptography), when merging shares, the reconstructed hidden image has “lower visual quality, as the recovered image becomes darker. Examples of XOR-based VCs are noted in [16], [17] and [18]. It is informed that it is an important branch of VC that can regenerate the secret without darkening the background when more shares are used. XOR-based VC has better color, good contrast resolution characteristics than OR-based VC systems.”

V. VISUAL CRYPTOGRAPHY METRICS

In Visual Cryptography schemes, we first introduce ourselves to a few important metrics which are pertinent and frequently employed to assess or characterize the process.

i. Pixel enlargement

The amount of “sub-pixels utilized to represent every pixel in a concealed image determines the size of tokens generated using pixel-based VC (visual cryptography).” When the parts are merged, the recovered picture has less contrast and loses resolution at the same quality as the original picture. This attribute also affects the size of the returned image, that should preferably be as equivalent to the previous secret as possible [5]. Transmission of data and processing are impacted by pixel enlargement. A bit - wise VC strategy can be used to reduce this.

ii. **Contrast**

Pixels in a hidden image are transferred to a mixture of "black and white subpixels in pixel-based VC (visual cryptography)." Reflects the clarity of an image. The hidden image is recreated by combining the shares. Black pixels in the sharing that correspond to the concealed image's white pixels throughout this procedure reduce contrast. The intensity of the retrieved (decrypted) images for VC methods is calculated like a quality indicator. Conversely, VC ("visual cryptography") encryption and decryption typically result in a loss.

iii. **Security**

security-l the "visual cryptography" "scheme represents the strength of the encryption stage. Each share created during the encryption phase should never reveal anything less than k-1 in the (k, n) schemes. unless they overlap. The security level of the encrypted share can be measured using metrics such as the number of pixels changed and the combined average density change."

iv. "**Complexity** "

Decryption shouldn't take a long time; instead, it should be completed quickly without the need of any external hardware and only by direct perception of the human eye. Complex "visual cryptography" algorithms are more complex in terms of computation and storage., requiring larger assistance from machines.

VI. APPLICATIONS OF VISUAL CRYPTOGRAPHY

i. **Secure QR Payment System**

Quick Response (QR) code is a two-dimensional barcode, which is a machine-readable optical label with fast reading, error-correction capability, and large data formats. QR code is widely used in payment information, business cards, education, finance and healthcare. The structure of the QR code is similar to the Visual Cryptography Scheme share, both are black and white images (binary images). The payment process is not visible to the user, so it is more secure. First, an "original QR code is split into two shares using visual cryptography. Second, the two shares are sequentially pinned to the same image, and the fixed results are combined with the same QR code, respectively, using the XOR operation of RS and the QR code error correction mechanism. Finally, the two QR codes" were combined to obtain the original QR code. This is an example of a "visual cryptography" scheme in a secure communication system.

ii. **Secure electronic ballot using VC**

The VC (visual cryptography) in [15] has been used to validate election results even where entire electoral systems and records are compromised. The system can be used to determine its access, robustness, etc. economically preserves voting secrecy. Also, the use of blockchain with visual cryptography provides greater transparency and security to the voting system.

iii. **Watermarking**

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

- Watermarking Embed
- Watermarking Retrieve

In the embedding method, the watermark is split using visual cryptography [6]. After splitting into shares, a share is embedded in the frequency domain of the hidden image and sent to another share owner. Owner's share helps to prove ownership on the image and watermark. When we combine the owner's numerator with another numerator embedded in the original image in the frequency domain [7].
The two shares individually do not give any information about the watermark.

iv. **Defense System**

In general, "visual cryptography" splits images into two shares, and the encrypted image is decrypted only by merging those shares, not any other shares [8]. This technique can be used for images, codes, handwritten texts, etc. It helps to encrypt all visual data such as This helps in defense to post a hidden picture like below. First, an image was encrypted in two parts and some of it was given directly to the person to whom it wanted to send a message, and the other part was sent as a fax or printout when that code was used. And it helps to share the message discreetly and visually. Using this technique, we are able to secretly send more than two messages to a person working as a secret agent in a remote and dangerous location, and the decryption of the data was done only by the person who received the message. just share.

v. **CAP-T-CHA**

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

- Shares Creation Process
- Hashed Codes Generation
- Authentication Process
- First, the two shares are matched and grouped together and the sound is removed from the allotment. Thereafter the confirmation will be accepted otherwise the confirmation will be rejected [9].

Fig-8: Captcha image [25].

VII. OTHER CRYPTOGRAPHIC TECHNOLOGIES

i. Passwords

Criminals use password protection to prevent direct intrusion. This is an effective way to protect a person's identity from outside world. Hackers utilize passwords significantly more frequently than methods connected to encryption.

ii. **"Compressing Digital Files"**

Digital compression reduces the size of just a digital file without sacrificing any of the file's crucial data. Oppression serves two purposes for criminals.: -

a) Compressed file creates it challenging for "law enforcement officials to seize crucial files."
b) It could be challenging to execute system crashes before encryption.

iii. "Steganography"

Steganography is the process of encrypting private information in a file or a private message for transmission without being detected. This makes it very secure.

VIII. CONCLUSION AND FUTURE WORK

This study presents several visual cryptography techniques. have been discussed such as contrast, pixel expansion, security and complexity of shares generated. Also, we discussed few major applications of visual cryptography. Through this survey, the investigators can learn about various visual cryptography strategies and their effectiveness. There are various other cryptographic technologies as well like steganography, compression etc.

The Visual Cryptography technique is a very important research topic as it is very secure in real world applications. Multiple secret sharing scheme can cause some problems with alignment points. Therefore, the multiple sharing technique for additional rows may be a research topic in the future. Visual Cryptography using another option to consider is a print as well as scan application in the future for better research work. We can also use some "visual cryptography" schemes in real life applications to increase efficiency for multiple confidential sharing, color images and meaningful sharing. In the future, some researchers may also focus on Pixel broadening and contrast loss, which is a major threat to Visual Cryptography Scheme.

REFERENCES

[1]Myodo E, Takagi K, Miyaji S, Takishima Y (2007) Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique. In: Multimedia and Expo, 2007 IEEE International Conference on. IEEE

[2]InKoo Kang, Gonzalo R. Arce and Heung-Kyu Lee,"Color Extended Visual Cryptography Using Error Diffusion," IEEE Transaction on Image Processing, vol. 20, No. 1, pp.132-145 , 2011.

[3]Arun Ross and Asem Othman, "Visual Cryptography for Biometric Privacy," IEEE Transaction on Information Forensics and security, vol. 6, No. 1, pp. 70-81, 2011.

[4]Hou Y-C (2003) Visual cryptography for color images. Pattern Recogn 36(7):1619–1629. https:// doi.org/10.1016/s0031-3203(02)00258-3

[5]. Ramya J, Parvathavarthini B (2014) An extensive review on visual cryptography schemes. In: 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). IEEE

[6]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

[7] Shamir, A., 1979. How to share a secret. Communications of the ACM, [online] 22(11), pp.612-613.

[8] 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

[9] 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.

[10] Feng Liu and Chuankun Wu, "Embedded Extended Visual Cryptography Schemes," IEEE Transaction on Information Forensics and Security, vol. 6, No. 2, pp. 307-322, 2011

[11]Naor, M. and Shamir, A. 1995. Visual Cryptography, in Advances in Cryptology – Eurocrypt. A. De Santis, Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp 1-12, 1995.

[12]Wu, L. and Chen H. A Study On Visual Cryptography, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998

[13]] D.Vaya, S. Khandelwal, and T.Hadpawat, "Visual Cryptography: A Review," International Journal of Computer Applications, vol. 174, pp. 40-43, Sep 2017.

[14]Hsu, H., Chen, T. and Lm, Y. The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing, in Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001, March 2004.

[15]D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," in *IEEE Security & Privacy*, vol. 2, no. 1, pp. 38-47, Jan.-Feb. 2004

[16]Tuyls, P., Hollmann, H. D., Van Lint, J. H., & Tolhuizen, L. M. (2005). XOR-based visual cryptography schemes. Designs, Codes and Cryptography, 169–186

[17]Wang,D.,Zhang,L.,Ma,N.,& Li,X.(2007).Two secret sharing schemes based on Boolean operations. Pattern Recognition, 40(10), 2776–2785

[18]X. Wu and W. Sun, "Generalized Random Grid and Its Applications in Visual Cryptography," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1541-1553, Sept. 2013

[19]Ateniese, G., Blundo, C., Santis, A., & Stinson, D. (2001). Extended capabilities for visual cryptography. Theoretical Computer Science, 250(1–2), 143–161

[20]Droste, S. (2001). New results on visual cryptography. Advances in Cryptology — CRYPTO '96 Lecture Notes in Computer Science, 1109, 401–415

[21]Yan, W.Q., Jin, D., Kankanhalli, M.S.: Visual cryptography for print and scan applications. In: Proceedings of International Symposium on Circuits and Systems,Vancouver, Canada, May 2004, pp. 572–575 (2004)