Webology (ISSN: 1735-188X)
Volume 19, Number 3, 2022

The Usefulness Of Visual Cryptography Techniques: A Literature Review

Ernesto Lee[1] , Lama A Alzahrani[2] , Faysal Rahman[3]

[1]Professor Department of Computer Science, Broward College United States.

[2]Researcher.

[3]Researcher University Teknologi Malaysia.

Abstract

Visual Cryptography is an encryption technique used to store the secret in graphics so that the observer can decode it if the right key image is applied. In the world of fast-growing technology, we face many security and privacy issues. In the exchange of images, privacy became an unavoidable issue. Visual cryptography (VC) is the modern cryptographic process used for Encryption, and it can securely share the files, and its details are kept secret. Visual cryptography approaches are discussed in this paper that is used to mask the original information from an attacker or an unwelcomed person. Images, text, and other types of visual data can be encoded and decoded to create an image when decrypted. Many things are involved in it, like; symmetric key cryptography, steganography, visual cryptography, invisible multiple watermarking, and secure document sharing using visual cryptography technique. A wide area of applications of visual cryptography is also a part of this paper. In addition, with that, security breaches and future technologies in the field of cryptography are discussed. In this paper, we compare different visual cryptography techniques, and further, we discuss the future trends and upcoming threats to visual cryptography.

Keywords: Encryption/Decryption, Visual Cryptography Techniques, Visual Cryptography Applications

1. Introduction

Using Visual Cryptography, we can encode visual data and decode it similarly. With advancements in technology, data privacy, security, and hiding are very worthy and important for many organizations. Many organisations spend millions of dollars on maintaining the security and privacy of their data. This technique is coming into being due to enlarging several security threats, cyber theft or crime. As technology becomes more advanced, criminals also have many ways to perform cybercrime. To overcome these issues, we need Visual Cryptography. The fast expansion of the internet and internet services, which involve the connection of various devices and computers to transport data, necessitates a high degree of security. Traditional encryption algorithms transform viewable pictures to an unreadable ciphertext format automatically. Encryption converts data to an unreadable and secure structure for transmission over the internet using a hash function and, indirectly, a mathematical function. Visual Cryptography is a term used to describe the

act of assigning a value to each part of an image. Photos, paintings, and so on can be used as secret pictures. Encryption in the form of visuals is an important part of exchanging and distributing intimate images.
Naor and Shamir [1] presented the concept of visual cryptography in 1994. With it, you may encode visual data (such as written material, notes, and photos) and have the human visual system decipher it on its own. In 1994, [1] developed a novel security method called visual cryptography, which they termed "visual cryptography." The white pixel in the early assassination attempts of Naor and Shamir indicates translucent colors because of the treatment of the black and white pixels. An example of a simple (2,2) visual threshold method is in Table 1.

Table 1. (2, 2) Visual Threshold schemes

Pixel	Block 1	Block 2	Block 1 superimposes on block 2
■	■□ (1, 0)	□■ (0,1)	■■ (1, 1)
■	□■ (0, 1)	■□ (1, 0)	■■ (1, 1)
□	■□ (1, 0)	■□ (0, 1)	■□ (1, 0)
□	□■ (0, 1)	□■ (1, 0)	□■ (0, 1)

This paper will elaborate on working on the visual cryptography techniques and their application in which their summaries are discussed, why they are used, and the type of issues we can solve. Analysis and comparison table are used to compare all the techniques to get the performance of all the techniques. We are discussing research papers related to visual cryptography usage on different platforms like visual cryptography in cloud computing, networks, online detection systems, and banking transaction systems. Also, VC is used for secret sharing halftone images, binary, CYAN images, and colored images. Architecture for (2,2) scheme is shown in Figure 1 share creation and Figure 2 authentication. We are discussing different types of Visual Cryptography techniques in this paper like symmetric key cryptography [2], text-based steganography and visual cryptography [3], Multiple Watermark Embedding extends SWE [4], Secured Document Sharing Using Visual Cryptography [5], Hou's third algorithm [6], secure (2,2) extended cryptography scheme [7], Encryption of facial photographs, employing visual cryptography and zero-watermarking [8], the synchronization of visual information pixels (VIP) and the dispersion of errors [9], Fourier transforms (FrFT) and visual cryptography (VC) [10], XOR-based visual cryptography scheme (XVCS) [11], Encryption and decryption using elliptic curve cryptography [12] and describing many others techniques like this. Our main motive is to hide or private our data from unauthorized access so that no one can breach our confidentiality, integrity, and authenticity. Visual cryptography techniques ensure all those constraints positively.

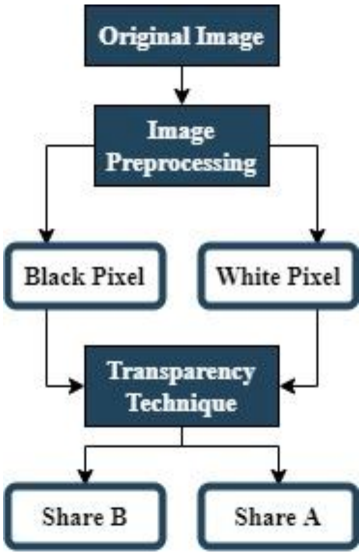

Figure 1. Share Creation

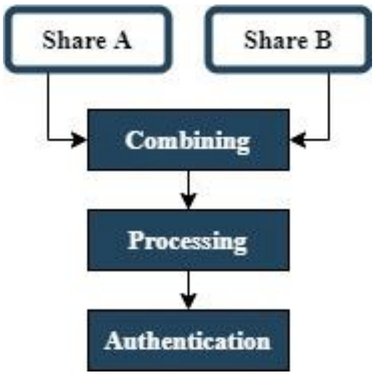

Figure 2. Authentication in the (2,2) scheme

Furthermore, the document includes the following list. All the previous strategies and comparisons are discussed in Section II. Section III will be followed for future trends and predictions in visual cryptography. Section IV discusses the conclusion.

2. Literature Review

Symmetric key cryptography involves supplying the cryptosystem with an image and a key. An encrypted image is generated by the encryption method and communicated to the recipient. Upon receiving the encrypted image, the recipient decrypts the unedited version by entering a key. The quality of the restored image is one of the most critical aspects in evaluating the efficacy. Since most computer input and output systems employ the RGB color scheme, the color image is typically represented in this color space [2].

It is a technique that minimizes the exchange of information between the end-user and the online merchant but allows for successful fund transfer from the consumer's account to the merchant account, ensuring that consumer information is protected and that the data is not misused at the merchant's end. Thanks to the Multiple Watermark Embedding feature, it's possible to integrate more than one watermark in the same image. For example, the cover image of SWE [4] has many watermarks inserted in it. A new methodology called SDSUVC is utilized for effective document management, which takes up to a lesser extent storage capacity on the cloud and takes less time complexity to recover the actual document using this technique.

A new authentication mechanism has been developed using Hou's third method for color photos. Voting and banking applications can be made electronically using the fundamental process (2,2). Using this technology, it is possible to obtain high-quality reconstructed images without pixel expansion [6]. Here, you can find a secure (2,2) extended cryptography system [7]. It explains how we don't need more pixels to retrieve or share an image, and it delivers high quality for both [8–9].

The author presents a new and secure method for creating shares in this paper. As a result, a helpful tool for safeguarding equity is designed secret. Encapsulated sharing visual encryption system and difficulties in revealing the identity of secret images [13] will be demonstrated [14, 15]. We are aware of its importance in protecting digital biometric data contained in a database. We're looking into the possibilities of utilizing VC to encrypt biometric data [14] in this study. Using threshold visual cryptography, a private image can be included among n shadow images with k or more people able to access it, but k-1 or few people will have no idea what it is [15]. A new XOR-based visual cryptography system (XVCS) was presented [11]. To create a visual cryptography system, we will use two strategies for general access structure. Authors look at the VCS's architecture and find that it restricts the amount of money each user gets [16].

Secret sharing mechanisms are examined in this research. They learn about the pros and cons of using this technique and its contribution to the development of the secure secrete system for sharing photographs over the network [17]. To suppress an image, we can divide it into two or more pieces, each of which can be used to restore the initial impression when the time comes [18]. Visual cryptography systems are compared based on the number of secret images, pixel expansion, image format, and the nature of share produced in this comparison paper to exchange an encrypted image. We'll examine various visual cryptography approaches and compare them [19]. Here, we will look at the uses of Visual Cryptography, focusing on four multiple research publications that concentrate on the core aspect of Encryption. [20]. To analyze the performance of each VC encryption method, we used the pixel expansions and image format share generation, as well as the total number of shares, in this paper [21].

An Elliptic Curve Diffie Hellman algorithm and a visual cryptography tool are working. The secret images and visual sharing are scrambled with the ECDH secret key and then converted into encrypted data in base64 format [22] to ensure safe delivery. An algorithm based on image processing and VC is developed for securing and authenticating your data. The customer's signatures will be processed by this method, and then they will be broken into shares [23]. To guarantee the digital image's security, robustness, and transparency. A digital image's copyright is safeguarded using the watermarking method, which is the subject of this study [24]. A visual cryptography-based copyright protection solution is being proposed. Our hidden and public images can be generated using this technology, which doesn't require watermarks to be embedded directly into the secured image. [25]. Extendable VC and QR codes can prevent online fraud transactions from taking place. The VC is used to generate shares, while the OTP identifies a phishing website. [26]. A cloud-based picture storage security system protects images in real-time [27]. Some algorithms protect cloud data, but they necessitate a significant investment in computing power, storage, and other factors. They propose a method to address these concerns by Utilizing visual cryptography to encrypt portable document formats. It provides data secrecy and integrity with minimal compute and storage space [28].

The SDPBDVC (Secure Data Processing on Big Data Using VC) approach protects critical data [29]. Cloud storage security is hard to maintain since data is stored in plain text or unencrypted form, making it easier for attackers to obtain our personal information. Proposing a visual cryptographic approach to data obfuscation to solve this problem [30].

2.1. Taxonomy Diagram

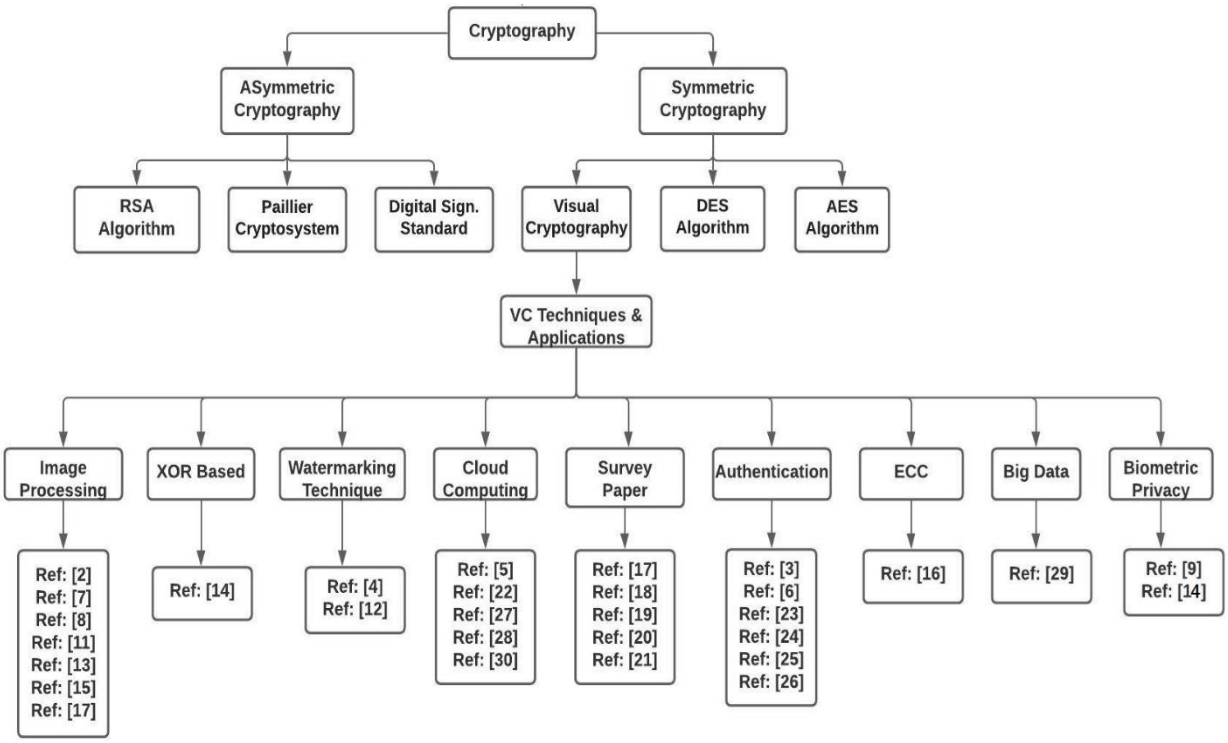

Figure 3. Taxonomy Diagram

2.2. Analysis Table

The analysis table has presented all discussed approaches in a table manner. This table allows us to keep track of all the paper highlights elaborated in the literature review. References, challenges, solutions, contributions, limitations, and dataset are included in this Table 2. This table provides us with the contribution of different authors that they have done in their papers and which type of data set was used by them.

Table 2. Analysis Table for Visual Cryptography Techniques

Ref.	Problems	Solution	Contributions	Limitation	Data Set
[2] 2010	Image security and privacy Image Theft	Symmetric Key Cryptography.	Process of Symmetric key cryptography. Quality of Image reconstruction	It gives us a solution only when we transfer the image through the network.	SSIM is the image of any format.
[3] 2014	Debit or Credit card fraud. Unauthorized access to data	Steganography and VC.	Authentication system using VC.	The payment system does not extend to physical banking	Transactions. Credit or debit cards

[4] 2010	Easy access facilitates information piracy,	Multiple, Invisible and Digital image watermarking	Multiple Watermarking techniques using master share and ownership share.	Limited scope just focuses on watermarking techniques	Secret Binary Image. XOR gate,
[5] 2015	Unauthorized access, Plain data	Secured document sharing using VC.	SDSUVC technique	Focus on the cloud computing environment.	User Data. Cloud Storage.
[6] 2011	Unauthorized access to data. Multiple attacks.	Visual cryptography and Hou's third algorithm.	Pixel expansion, size, and quality of the reconstructed image	All the work is done by using Hou's algorithm.	Image shares. Customer data Database etc.
[7] 2013	Image Processing and confidentiality Issues. Image shares theft	A secure (2, 2) extended visual cryptography scheme. Biometric information	A secure (2; 2) extended VCS does not require more pixels to recover the image.	It provides pixel expansion for just a halftone image.	Image and its shares. Biometrics identifier.
[8] 2017	Privacy breaches. Limited protection provided by cloud computing	Zero Watermarking. Visual Cryptography for fog edge computing	Zero-watermarking for sharing biometrics. Visual Encryption for biometric security.	VC and zero watermarking only focus on biometric images.	Biometrics. Cloud Storage
[9] 2011	The previous method cannot apply to colored share. Low visual quality	VIP synchronization. Error Diffusion	Maintain pixel position. Share can be readable. Digital halftoning	It will give in low contrast.	Color EVC scheme. Image and pixels.
[10] 2011	Data authentication issues. Intellectual property rights issues.	FrFT scheme. Blind Watermarking. VC.	PRNG, Singular value decomposition. Generation of master and ownership share.	Complexity due to mathematical models involves in it.	Master and ownership shares. Complex mathematics
[11] 2017	Cannot access secret image information from parts less than k.	XOR-based VC. General access structure. Linear algebra techniques	The linear algebraic approach is used to construct XVCS with perfect contrast. With lower pixel	I need complex computational knowledge to understand this. Linear Algebra	Data on which we can perform complex computation.

			expansions, the difference is excellent.		Mathematic models
[12] 2017	When all shares are heaped up, they reveal the image's secret.	Using Elliptic Curve Cryptography. Using a visual secret sharing scheme.	Creating multiple shares of the picture with the aid of ECV. Using PSNR value	Creating a share that only works for the RGB contrast-based.	Mathematical models. XOR and matrices models.
[13] 2015	Image privacy leakage and theft.	Using Advanced Encryption Standard (AES) algorithm. Encapsulated Share.	A novel secure creation scheme. Encapsulated share mechanism that protects the share.	Not used for different share creation procedure	AES algorithm. Shares of pictures. Matrix calculations.
[14] 2011	Issues with the storage of the biometric system.	VC for biometric privacy. Apply XM2VTS and IMM face databases.	Securing iris and fingerprint template, Private face image.	Image can be reconstructed only when both sheets are available.	Candidate host Image. MGBC database. Pixel Expansion
[15] 2003	Existing VCS for binary images is applied to gain work of creating shares	Using VCS for a gray-level image by dithering techniques. Watermarking	The dithering technique tells the advantages of inheriting any developed SFCOD algorithm	It's for a gray-level image, not focusing on other formats.	Original image. Visual Patterns.
[17] 2016	Vulnerability on networks. Privacy breaching	Different schemes of visual cryptography.	Providing a survey for many VC techniques.	Focus on sharing data or images only through a network.	Image and different types of techniques.
[19] 2013	Privacy issues while transferring data or images through the channels.	Different techniques of visual cryptography	Comparing several visual cryptography approaches.	Its limited enhancement and progress in the field of VC.	Written, financial documents, text images, internet voting
[20] 2016	Facing privacy and confidentiality issues due to using plain data.	Four different types of Visual cryptography encryption schemes.	Working on VC encryption schemes to enhance privacy and confidentiality.	Using only four papers to make a comparison.	Data like images, multimedia files, etc.

[22] 2020	The cost of computing required to encrypt the picture is expensive.	VC approach and Diffie Hellman EC methodology.	Elliptic Curve Diffie Hellman methodology.	It just has limited scope because focusing on just time.	Image of any format included in it.
[23] 2008	Authenticity issue in banking applications. Data theft issue,	An algorithm is proposed based on image processing and VC	Process the customer's signature, and then it will break it into shares.	Facilitate the banking customer and application only.	Customer data related to bank. Important transactions.
[26] 2017	Phishing attacks, Security breaches.	System for preventing online fraud transactions using extended VC and QR codes.	Share generation. Extended VC convert QR code into two shares	It's more work focusing on overcoming the issue of a phishing attack.	Important data of anyone.
[28] 2017	Data security in cloud storage is a difficult job for cloud customers.	Using enhanced VC, secure portable document format files.	Ensures data confidentiality and integrity with minimum computation.	Focusing on just cloud computing	The document, Storage Computational issue, and cost.
[29] 2020	Difficult to process a large amount of data in cloud storage.	SDPBDVC	MapReduce handles a large amount of data.	Does not perform any process for the small amount of data.	Organizational and company data in huge amounts.

2.3. Comparative Table

The comparative table will compare multiple previously proposed techniques based on the attributes mentioned in Table 3. This table shows that all the visual cryptography techniques described in this paper use which type of technologies.

Table 3. Comparative table

Ref:	Share Creation	Biometric Based	Device Mobility	Cloud-Based	Auth. Based	Image Process
[2]	✓	✗	✗	✗	✗	✓
[3]	✓	✗	✗	✓	✓	✗
[4]	✗	✗	✗	✗	✗	✗

[5]	✗	✗	✗	✓	✗	✗
[6]	✓	✗	✗	✗	✓	✗
[7]	✓	✗	✗	✗	✗	✓
[8]	✗	✓	✗	✗	✗	✓
[9]	✗	✗	✗	✗	✗	✗
[10]	✗	✗	✓	✗	✗	✗
[11]	✗	✗	✗	✗	✗	✓
[12]	✓	✗	✗	✗	✗	✗
[13]	✗	✗	✗	✗	✗	✓
[14]	✓	✓	✗	✗	✗	✗
[15]	✓	✗	✗	✗	✗	✓
[16]	✗	✗	✗	✗	✗	✗
[17]	✓	✗	✓	✗	✗	✓
[25]	✗	✗	✗	✗	✓	✗
[26]	✗	✗	✗	✓	✓	✗
[27]	✗	✗	✗	✓	✗	✗
[28]	✗	✗	✗	✓	✗	✗
[29]	✗	✗	✗	✗	✗	✗
[30]	✗	✗	✗	✓	✗	✗

3. Future Predictions and Trends

Visual cryptography is a complex technique that combines the ideal ciphers and steganography elements of Encryption with graphics. A digital image may be divided into segments and then reassembled to resemble the original. We have seen a vast rise in digital data processing, the usage of sensitive data, and the growth of laws and regulations to assist manage and preserving it all today. As security experts, we should develop solutions to secure our clients' data by avoiding privacy violations as we navigate through these phases of growth and development. Researchers believe cryptography will be a highly crucial tool for securing this data when used in combination with several other security standards. This section will discuss the security breaches in recent years and methods that will tackle these breaches by using visual cryptography. In addition, emerging technologies are provided, which will help protect data.

3.1. Threats in Visual Cryptography

Publishers are continuously forced to keep ahead of the curve, especially when it comes to ensuring the protection of their clients. As a result, they could be the next three breakthroughs in data encryption. Table 4 discusses the major encryption technologies.

Table 4. Emerging Technologies in VC

New Technology	Problem	Description
Homomorphic Encryption	Decrypting data when it is at rest in storage space.	Individuals handle encoded data and generate encrypted outputs using homomorphic Encryption.
Quantum Cryptography	Eavesdropping	Using quantum physics principles,

		quantum cryptography encodes and sends data in an extremely secure way.
Visual Cryptography	Secret Sharing	Visual Cryptography allows Encryption and decryption of visual information.
Whole disk encryption	Device Lost	This protects it when a laptop or gadget is lost or destroyed, and a key is needed to decode the data.

Because the healthcare business is a requirement, it is a great target for cybercriminals for many purposes. Identity fraud, self-benefit, and smear campaigns are among them. Between 2009 and 2015, the healthcare business reported a significant growth in data theft. "During 2009 and 2018, there were 2,546 information exposures containing more than 500 records," according to the HIPPA journal. One hundred eighty-nine million nine hundred forty-five thousand eight hundred seventy-four records were stolen or exposed because of these incidents. And over 59 percent of the population of the United States is represented by this figure. Data breaches in healthcare are currently reported more than once per day.

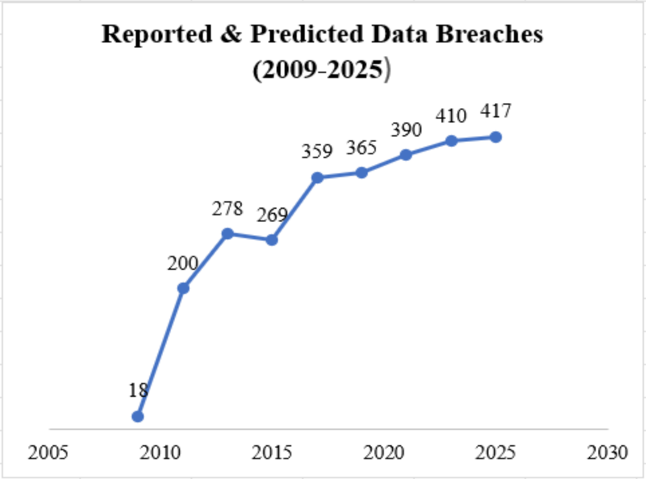

Figure 4. Number of Data Breaches from 2008-2025

While studying the various research, we concluded that hackers and unauthorized individuals discover additional and varied methods to infiltrate data as technology progresses.

According to (Recognition of MitM attacks techniques using physical layer wireless security), they recorded 438.9 million MITM assaults in 2015 and 565.4 million in 2016. By combining these data, we can create a graph that shows how many attacks took place in 2018 and how many will occur in 2022.

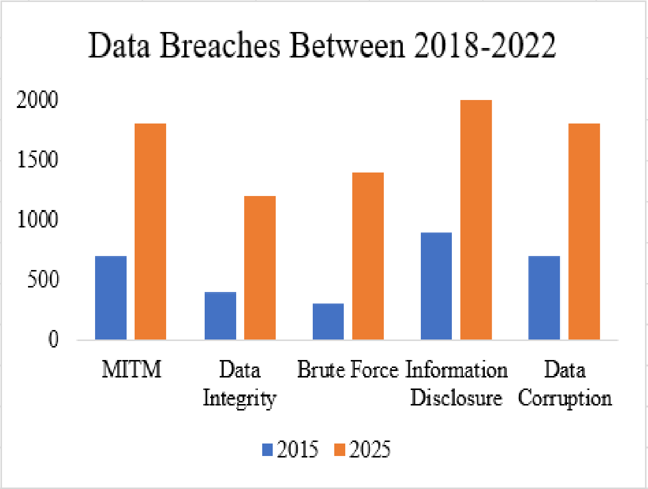

Figure 5. Data Breaches from 2018-2022 [31]

4. Conclusion

As we know, that Visual Cryptography is an important encryption technique to hide information in images. In this paper, we have discussed the applications and specialty of visual cryptography (VC). We have seen the visual cryptographic techniques used to hide the original information. So basically, visual cryptography techniques are being used for security and privacy, and it has a wide range of its applications. This paper proposes different techniques of VC for the authentication of visual cryptography. We maintain the security and privacy of all visual gadgets like (photos, pictures, etc.) and secure data transfer to communicational channels. And finally, we analyze the future directions in cryptography with recent data breaches in recent years.

References

[1] Ashutosh and S. D. Sen, "Visual cryptography," Proc. - 2008 Int. Conf. Adv. Comput. Theory Eng. ICACTE 2008, pp. 805–807, 2008, doi: 10.1109/ICACTE.2008.184.

[2] B. SaiChandana and S. Anuradha, "A New Visual Cryptography Scheme for Color Images," Int. J. Eng. …, vol. 2, no. 6, pp. 1997–2000, 2010.

[3] S. Roy and P. Venkateswaran, "Online payment system using steganography and visual cryptography," 2014 IEEE Students' Conf. Electr. Electron. Comput. Sci. SCEECS 2014, pp. 1–5, 2014, doi: 10.1109/SCEECS.2014.6804449.

[4] B. Surekha, D. G. Swamy, and D. K. S. Rao, "A Multiple Watermarking Technique for Images based on Visual Cryptography," Int. J. Comput. Appl., vol. 1, no. 11, pp. 78–82, 2010, doi: 10.5120/236-390.

[5] K. Brindha and N. Jeyanthi, "Secured document sharing using visual cryptography in cloud data storage," Cybern. Inf. Technol., vol. 15, no. 4, pp. 111–123, 2015, doi: 10.1515/cait-2015-0058.

[6] Jaya, S. Malik, A. Aggarwal, and A. Sardana, "Novel authentication system using visual cryptography," Proc. 2011 World Congr. Inf. Commun. Technol. WICT 2011, pp. 1181–1186, 2011, doi: 10.1109/WICT.2011.6141416.

[7] I. Canadian, C. Of, and E. Engineering, "AN EXTENDED VISUAL CRYPTOGRAPHY SCHEME WITHOUT PIXEL EXPANSION FOR HALFTONE IMAGES N . Askari , H . M . Heys , and C . R . Moloney Electrical and Computer Engineering Faculty of Engineering and Applied Science Memorial University of Newfoundland," 2013.

[8] W. Abdul, Z. Ali, S. Ghouzali, B. Alfawaz, G. Muhammad, and M. S. Hossain, "Biometric Security Through Visual Encryption for Fog Edge Computing," IEEE Access, vol. 5, pp. 5531–5538, 2017, doi: 10.1109/ACCESS.2017.2693438.

[9] I. Kang, G. R. Arce, and H. K. Lee, "Color extended visual cryptography using error diffusion," IEEE Trans. Image Process., vol. 20, no. 1, pp. 132–145, 2011, doi: 10.1109/TIP.2010.2056376.

[10] S. Rawat and B. Raman, "A blind watermarking algorithm based on fractional Fourier transform and visual cryptography," Signal Processing, vol. 92, no. 6, pp. 1480–1491, 2012, doi: 10.1016/j.sigpro.2011.12.006.

[11] G. Shen, F. Liu, Z. Fu, and B. Yu, "Perfect contrast XOR-based visual cryptography schemes via linear algebra," Des. Codes, Cryptogr., vol. 85, no. 1, pp. 15–37, 2017, doi: 10.1007/s10623-016-0285-5.

[12] K. Shankar and P. Eswaran, "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography," China Commun., vol. 14, no. 2, pp. 118–130, 2017, doi: 10.1109/CC.2017.7868160.

[13] K. Shankar and P. Eswaran, "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography," Procedia Comput. Sci., vol. 70, pp. 462–468, 2015, doi: 10.1016/j.procs.2015.10.080.

[14] A. Ross and A. Othman, "Visual cryptography for biometric privacy," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 1, pp. 70–81, 2011, doi: 10.1109/TIFS.2010.2097252.

[15] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," Pattern Recognit. Lett., vol. 24, no. 1–3, pp. 349–358, 2003, doi: 10.1016/S0167-8655(02)00259-3.

[16] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual Cryptography for General Access Structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, 1996, doi: 10.1006/inco.1996.0076.

[17] A. C. S. M. A. Kalekar, "Visual Cryptography for Sharing Digital Image Using Diverse Media," Int. J. Sci. Res., vol. 5, no. 10, pp. 1141–1144, 2016, [Online]. Available: https://www.ijsr.net/archive/v5i10/ART20162204.pdf.

[18] S. A. Thomas and S. Gharge, "Review on Various Visual Cryptography Schemes," Int. Conf. Curr. Trends Comput. Electr. Electron. Commun. CTCEEC 2017, vol. 3, pp. 1164–1167, 2018, doi: 10.1109/CTCEEC.2017.8455136.

[19] A. B. Dhole and P. N. J. Janwe, "An Implementation of Algorithms in Visual Cryptography in Images," Int. J. Sci. Res. Publ., vol. 3, no. 3, pp. 1–5, 2013.

[20] A. Pandey and S. Som, "Applications and usage of visual cryptography: A review," 2016 5th Int. Conf. Reliab. Infocom Technol. Optim. ICRITO 2016 Trends Futur. Dir., pp. 375–381, 2016, doi: 10.1109/ICRITO.2016.7784984.

[21] J. Ramya and B. Parvathavarthini, "An extensive review on visual cryptography schemes," 2014 Int. Conf. Control. Instrumentation, Commun. Comput. Technol. ICCICCT 2014, pp. 223–228, 2014, doi: 10.1109/ICCICCT.2014.6992960.

[22] A. K. J and G. Ganapathy, "A Visual Cryptographic Technique for Transferring Secret Image in Public Cloud," Int. J. Innov. Technol. Explor. Eng., vol. 9, no. 3, pp. 2257–2260, 2020, doi: 10.35940/ijitee.c9037.019320.

[23] C. Hegde, S. Manu, P. D. Shenoy, K. R. Venugopal, and L. M. Patnaik, "Secure authentication using image processing and visual cryptography for banking applications," Proc. 2008 16th Int. Conf. Adv. Comput. Commun. ADCOM 2008, no. Vc, pp. 65–72, 2008, doi: 10.1109/ADCOM.2008.4760429.

[24] R. J. Hwang, "A digital image copyright protection scheme based on visual cryptography," Tamkang J. Sci. Eng., vol. 3, no. 2, pp. 97–106, 2000, doi: 10.6180/jase.2000.3.2.04.

[25] D. C. Lou, H. K. Tso, and J. L. Liu, "A copyright protection scheme for digital images using visual cryptography technique," Comput. Stand. Interfaces, vol. 29, no. 1, pp. 125–131, 2007, doi: 10.1016/j.csi.2006.02.003.

[26] S. Khaimar and R. Kharat, "Online Fraud transaction prevention system using extended visual cryptography and QR code," Proc. - 2nd Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2016, 2017, doi: 10.1109/ICCUBEA.2016.7860061.

[27] D. Liu, J. Shen, A. Wang, and C. Wang, "Secure real-time image protection scheme with near-duplicate detection in cloud computing," J. Real-Time Image Process., vol. 17, no. 1, pp. 175–184, 2020, doi: 10.1007/s11554-019-00887-6.

[28] K. Brindha and N. Jeyanthi, "Securing portable document format file using extended visual cryptography to protect cloud data storage," Int. J. Netw. Secur., vol. 19, no. 5, pp. 684–693, 2017, doi: 10.6633/IJNS.201709.19(5).05.

[29] K. Brindha and N. Jeyanthi, "SDPBDVC: Secure data processing on big data using visual cryptography," Int. J. Serv. Technol. Manag., vol. 26, no. 2–3, pp. 237–251, 2020, doi: 10.1504/IJSTM.2020.106685.

[30] K. Brindha and N. Jeyanthi, "DOVC: Data obfuscation visual cryptography to protect cloud storage," Int. J. Soft Comput., vol. 11, no. 6, pp. 374–381, 2016, doi: 10.3923/ijscomp.2016.374.381.

[31] Qadeer, B., Shah, M.A. and Ishaq, A., 2021. PRIVACY PRESERVATION IN DIGITAL ECONOMY PLATFORMS