Review Based on Visual Cryptographic Scheme and Applications

[1]Pramod Bachiphale, [2]Nitish Zulpe
[1]Research Scholar, College of Computer Science and Information Technology, Latur India
[2]Principal, College of Computer Science and Information Technology, Latur India
Email: [1]pbachiphale@gmail.com, [2]nitishzulpe@gmail.com

Abstract: Technologies demand more security and less computation. Visual cryptography is a powerful encoding technique that divides the secret image into multiple shares. Decryption Is performed just by a human visual eye without complex mathematical operations and extra hardware. This review paper covers some visual cryptography techniques overview and lacks some visual cryptography techniques. Analysis of some visual secret-sharing schemes enlightens the new researcher about problem identification, and research gaps for using techniques to their application. Visual cryptography enhanced the applicability of old visual cryptography schemes through different application areas such as image encryption, data hiding, verification or authentication, access control, etc. This paper also enlightens about different enrichment in existing algorithm complexity, pixel expansion, multi-secret encoding, and progressive VC code book
Index terms: Visual cryptography, QR-Code, Captcha, Water Marking, Secret Sharing Scheme

I. Introduction

Visual Cryptography is pioneered and initiated in 19994 by Moni Naor and Adi Shamir Eurocrypt conference. Visual Cryptography is an advanced cryptographic scheme, which can reveal information of hidden images without complex calculation [1]. As the name recommends Visual Cryptography reveals image Information just by the Human eye or Stacking k images together. This is the main benefit over other cryptographic schemes that visual cryptography can be used without or lack knowledge of other secret schemes or cryptography and complex computation. Moni and Adi Shamir proposed A model in which message and information are illustrated by black and white pixel, each pixel is considered a separate piece of information and where white denote transparent contrast. Two shares having n number of black pixels and m number of white pixels superimposed to get the desired result, the constructed output is not so clear and it affects the contrast in an image, this is a drawback of the proposed model and later scheme for gray and color image it reduced [2].

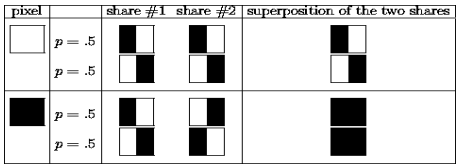

Fig 1. (2,2) VSS SCHEME

The above figure shows two out of two basic visual cryptographic schemes, the white pixel is divided into either black or white share, and superimposition of pixel shares generates a black and white pixel image.Gray and Color images scheme minimized the contrast problem in the previous pixel model scheme, it uses Halftoning scheme. A Visual Pattern of dots forms an image for the human eye, it consists of a range of colors or gray produced binary image. Halftoning produces a continuous tone image with a loose process not an exact image as the original image [3-6]

II. Review

The key advantage of VC is to generate share images and decoding is performed only through Visual cryptography is an important technique for information and Data security Most importantly it is used to differentiate humans and machines. The key benefit of visual cryptography is it is decrypting the image of hidden information the by human visual system without complex computation operation. Following section more general review of various schemes of visual cryptography.

I. REVIEW CONSTRUCTED ON MONOCHROME VISUAL CRYPTOGRAPHY IMAGES

Visual secret sharing scheme where monochrome images are used as secret images and different operations of visual cryptography like XOR and OR are applied on monochrome images to construct meaningful share or different combinations of these operations with NOT operator [7]. A secret sharing scheme based on random Permutation applied on four different images with efficient secret sharing and reconstruction of two shares based on random permutation novel method. The Halftone technique can further expand this scheme to gray and color images [8]. Multiple secret-sharing schemes use visual cryptography to share the secret with a master key. The master key is constructed for each image or share and applied to n number of images for sharing different secret images [9].

All the above scheme supports black or white images as secret, the demand for adapting and using color images has increased to meet that demand further shifted to color visual cryptography

A. REVIEW CONSTRUCTED ON COLOR VISUAL CRYPTOGRAPHY IMAGES

I. REVIEW BASED ON SINGLE SECRET SHARING

Verheul and Van Tilborg proposed the first color visual cryptography scheme before that up to the year 1997 visual cryptography scheme was applied to black and white pixels only. In this proposed scheme each pixel is divided into several subpixels and the number of sub-pixels is again divided into several regions, Color secret sharing can be constructed with the concept of arc, and further schemes improved pixel expansion with this scheme [28]. The proposed new color visual cryptographic scheme is an extension of the black-and-white scheme. The proposed scheme improves the block length and infrastructure of the sub-pixel as an extension to the black-and-white scheme and creates n transparencies to share with k participants, no k-1 participants can reveal secrets, and all k participants reveal secrets [29].

II. REVIEW BASED ON MULTI-SECRET SHARING

M. Karolin and T. Meyyappan proposed an encrypted method that generates RGB images and shares using AES and Blowfish algorithm. Original image constructed after decrypting blowfish algorithm and overlapping generated shares. The proposed method creates a resultant better-quality image along with confidential encrypted and decrypted images over network transmission [30]. P. Mohamed Fathimal and P. Arockia Jansi Rani introduced the method (k,n) multiple secret sharing scheme, a proposed scheme with simple mathematics operation, less computation, and no pixel expansion[31].

2022-proposed two new schemes to fully reconstruct the color images along with no pixel expansion. These two proposed schemes produce some meaningful shares and some meaningless shares. The proposed scheme decryption process speed depends on the size of the QR code, the size of QR-code increases speed increases. Proposed scheme X-OR to reconstruct the image and experimentally proven as feasible [32].

B. REVIEW BASED ON VARIOUS SECRET-SHARING SCHEMES

Wu Z et al. [17] have planned a scheme of an efficient secret-sharing scheme with a polynomial derivative. The proposed method eliminates concentration operation while sharing phase and creates shadow same size and minimum size. The proposed scheme is very simple to compare traditional (t,s,k,n) ESIS schemes and overcome problems of smaller non-essential and essential shadows.Chen J et al. [18] stated a simple novel method for data security and data hiding where four different shares are hidden and the first two shares are exposed by stacking hollow cylinders, rotating at fixed angles. The other two shares are revealed by flipping shadow images at different angles, rotating fixed angles, and overlapping each other.

The Proposed scheme was applied to color images and produced higher-quality images after overlapping two shares. The cryptographic encoding scheme and randomness are improved to provide

a better and more secure scheme than traditional schemes and also very difficult for intruders to predict the share generated after stacking shares together [19].[20] Fu Z and Yu B proposed a rotation-based visual cryptographic scheme to solve the distortion problem in resultant images by using random permutation and correlative matrices set. This scheme creates two shares and the scheme is extended to color and gray images with halftoning technique.Multi secret sharing scheme is proposed to increase the usability and feasibility of the images and this scheme also improves security by assigning arbiter random points of decryption. This scheme creates 3 shares and provides multi-secret sharing with 2 shares only, there is a chance of contrast improvement of images [21]. The proposed method is based on QR-CODE efficiency and needs less computation. Images are encoded into different shares and each share is just like a QR code and decryption is performed by the xor operator. The scheme assists the higher performance of the scheme than traditional schemes and alignment issue problem recovery [22]A newly proposed scheme to provide secure transmission of images over the internet and solves the alignment problem. The sender encodes the images into shares and sends them to a receiver and the receiver accepts shares favorably with the master sharing the image with XOR operation [23].
The proposed scheme with visual cryptography and secret sharing scheme enhances the security and quality of the desired generated image. The quality of the image is measured through statistical methods such as PSNR and Mean Square errors are minimized. This scheme efficiently transfers gray images as color cover images on the internet and complexity is minimized and efficiency is improved as compared to the old visual secret sharing scheme [24].
The proposed method discusses the hierarchical relation between different shares and this scheme gives a simulated experiment approach based on the robustness, anti-jamming, and feasibility of the proposed scheme. The scheme reduces problems like pixel expansion, distortion, and multiple secret sharing schemes [25].[26] EPVCS-based proposed scheme reveals the secret in two stages with (k,n) Threshold construction for avoiding pixel expansion. This scheme resolves the overhead of the resultant image and contrast image, complexity problems, and avoids residual trace based on the cover image for the better progressive reconstruction of the image.The proposed scheme states about advanced schemes based on face recognition and also put light on different face recognition techniques like 3D model (infrared), and multi-model for face recognition. This scheme advances performance as compared to remodeling face recognition [27].

III. Analysis

Table .1. Analysis based on different types of images and No of Secrets

Author NAME	NO Of Shares	Type of Secret	Image Type	Share Type
Moni and Nor[1]	2	Single	Binary	Meaningless
Wu Z, Liu Y-N, Wang D, Yang C-N [17]	2	Single	Color	Meaningful
Chen J, Chen T-S, Hsu H-C, Lin Y-H[18]	2	Multiple	Color	Meaningful
Kamath M, Parab A, Salvankar A, Dholay S[19]	4	Multiple	Color	Meaningful
Fu Z, Yu[20]	2	Multiple	Grayscale	Meaningless
Shyu SJ, Huang S-Y, Lee Y-K, Wang R-Z, Chen K[21]	2	Multiple	GrayScale	Random
Wan S, Lu Y, Yan X, Wang Y, Chang C[22]	n	Single	color	Meaningless
Salama MA, Mursi MFM, Aly M[23]	n	Multiple	Binary	Meaningless
A JB, Raj C, Sukumaran R, G SM[24]	3	Single	Grayscale	Meaningful
Zhao T, Chi Y [25]	5	2	Grayscale	meaningless
Sridhar S, Sudha GF [26]	n	1	Binary	Meaningful
Li P, Ma J, Yin L, Ma Q [27]	3	2	Binary	Meaningless

Moni and Nor [1] introduced a single secret sharing scheme using binary images and share construction is meaningless. The proposed scheme applied to binary images creates two shares.
Wu Z et al. [17] stated that color images split into two meaningful shares for sharing only one secret image.

Chen j et al. further expanded the secret share scheme from a single to multiple secret sharing scheme. The scheme is applied to different color images to construct two meaningful shares [18]. Kamath M et al. introduced another technique to create more shares than previous methods. Scheme based on multiple secrets and four secret constructions with meaningful share [19]. Fu Z and Yu introduced another method based on grayscale images and multiple secrets with two meaningful share constructions [20]. A similar method based on gray and multiple secrets is introduced in [21] but the share created is meaningless. Another scheme introduced in [22], construct share depends on our need that is 'n' number of shares constructed in a single secret with meaningless share. Similar schemes are based on n-share construction but the difference is it is based on multi-secret and binary images [23]. A JB et al. introduced further little advanced grayscale-based schemes and construct three meaningful shares [24]. another grayscale based, improved five secrets shared efficiently with meaningless share and two secret sharing schemes [25]. Li P et al. introduced scheme improvement in the basic binary image and applied to a single image to spilt into three shares with Meaningless share [27]. similar scheme based on the binary image but differ concerning the number of shares created and a single image secret is being shared, the share created is meaningful.

IV. Applications Of Visual Cryptography

The application of visual cryptography is rapidly increasing due to its reliability and security of information sharing. In this paper, we discuss some applications.

1. WATERMARKING

In the Water Marking process split the watermark image into 2 shares with the support of visual cryptography schemes. Watermarking is a two-stage process.

A. Embedding Watermark
B. Retrieving Watermark

One share created by visual cryptography technique is united with the host image and another share is kept with the owner [10]. To generate the original image owner, need to extract another share from the image and that extracted stake and owner stake are stacked together.

2. ANTI-PHISHING SYSTEM

Phishing is highly stealing owner important Credential information like Passwords, pins, and Debit and Credit card numbers by intruders or hackers. Cryptography deals with these types of Highly important issues related to Security. To prevent phishing attacks visual cryptography is one of the advanced, safe, and reliable cryptography methods used, by applying visual cryptography two shares are created one is on the server and another is kept with the user [11]. This saves users from website Phishing by combining two shares one from the server and another from the user.

3. HUMAN-MACHINE IDENTIFICATION

Human Machine identification scheme is suggested by Kim et al. [12] A User and Distributor associated with ID. Distributor share slides on screen and users overlap their share with screen images to generate messages. This is a secret way distributor identify users by a visual secret sharing scheme.

4. SECURE BANKINCOMMUNICATION

The Major issue in core banking is avoiding hacking or information stolen from an online database that is the authenticity of the customer. Visual cryptography is the most reliable and secure cryptographic method used to construct secret shares one is kept on a bank server and another on the customer side. The customer uses their share on each bank secure transaction and then server share and customer share are combined and decoded by the bank for authentication of the customer.

5. DEFENSE SYSTEM

Visual cryptography uses an advanced combination of all its share to reveal the secret information, this technique is very much beneficial for defense systems. A secret image is divided into multiple shares and shares are shared with multiple participants. Every participant must have one share and not one or two participants can reveal the code but it is revealed when all participant combines their shares.

6. REMOTE VOTING SYSTEM

In today's world the of internet most of the work is done by using Remote systems. Visual cryptography is used for a secure and reliable voting process. Visual cryptography generates multiple shares some are kept with election offices and some are with voting servers and some with customer email. The customer has to use their id and share while online voting. The voting system combines all shares related to the customer and the vote is validated.

7. CAPTCHA

Captcha is an automated process telling the computer that humans and machines are different. Visual cryptography provides the way secure and reliable authentication of a captcha. User register with credential information like password, pin, id, etc. [14]. It consists of three stages.

A. Creation of share
B. Hash code creation
C. Authentication process

Captcha is created using a personal id number written by the user and an image of the captcha spilt into two shares one is kept within information and the other with the user. The hash code of the share is generated using the Md5 function then it's compared with the value in the database. if the match is found then two shares join to get the original image and depending on the outcome accept the authentication or reject the authentication of the captcha.

8. OFFLINE QR-CODE AUTHORIZATION

Authentication of QR codes by stacking transparencies together for authentication of QR code, this scheme is proposed in [14]. This scheme uses a Visual cryptographic algorithm in reverse order with Quick Response information like URL, V-card, and other types of information represented in the form of an opaque model in a black square with white background, and the response reader reads information on the QR code. The key features of QR code are:

A. QR Code is small in size
B. Easily readable and Damage resistance
C. Feature of high capacity to encode data and appending structure.
D. Feature of dirt and harm resistance, tiny output signal size.

9. SIGNATURE-BASED AUTHENTICATION

Visual cryptography algorithms with correlation methods can be used to accept and reject the authentication of customers based on signatures stated in [15]. Other methods like retinal, fingerprint, voice identification, and biometric-based are expensive whereas password authentication matching with database password is needed to prevent from hacking password. these problems are solved by a visual cryptographic signature-based authentication process in which shares are created based on the customer signature and one share is put on the bank server. database and another share on the customer side. The customer has to use their share for each transaction and that is matched with the server database share for the secret transaction and validated by correlation method.

10. FINGERPRINT-BASED AUTHENTICATION

Visual cryptographic algorithm development based on fingerprint authentication for the identification of individual persons is suggested in [17]. Here are two stages of fingerprint authentication

A. Registration
B. Authentication

A visual cryptographic (2,2) scheme is used in the registration process to create two shares. The first share is kept within the identity proof of the customer and the second share is stored on a database.

In the second phase, one share is extracted from the photo id and that extracted share is compared with the database share for authentication.

IV. CONCLUSION AND FUTURE DIRECTION

In current years numerous efforts are taken to enhance the security of different methods of visual cryptography, still, visual cryptography has lots of disadvantages to applying real-life applications. To overcome these disadvantages one of the directions is to analyze and survey existing schemes with different types of images and specific types of applications. A study was performed on the different schemes by applying them to different applications and noted their advantages to apply real-life problems, which cannot be exaggerated by scheme disadvantages.

The state of art spotlight on various applications such as encryption, authentication, data hiding, etc., and analysis helps to provide techniques suitable for real applications, prevent cheating, and suggest an enhancement in pixel expansion, multi secret encoding techniques.

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] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology - EUROCRYPT'94 Lecture Notes in Computer Science, vol. 950, pp. 1- 12, 1995.

[3] J. Lee, “Hybrid (2 , n) Visual Secret Sharing Scheme for Color Images,” no. 083, pp. 1–8, 2009.

[4] Chang, C. Tsai, and T. Chen, "A New Scheme For Sharing Secret Color Images In Computer Network," In Proceedings of IEEE International Conference on Parallel and Distributed Systems, Iwate, pp. 21–27, July 2000.

[5] [B. W. Leung, F. Y. Ng, and D. S. Wong, “On the security of a visual cryptography scheme for color images,” vol. 42, pp. 929–940, 2009, doi: 10.1016/j.patcog.2008.08.031.

[6] Ran-Zan Wang, "Region Incrementing Visual Cryptography," IEEE Signal Processing Letter, Vol. 16, No. 8, pp. 659-662, 2009.

[7] W. Fang, “Non-expansion Visual Secret Sharing in Reversible Style,” vol. 9, no. 2, pp. 204–208, 2009.

[8] Z. Fu and B. Yu, “Research on Rotation Visual Cryptography Scheme,” pp. 538–541, 2009, doi: 10.1109/IEEC.2009.118.

[9] Jonathan Weir and Wei Qi Yan, "Sharing Multiple Secrets using Visual Cryptography," IEEE International Symposium on Information Engineering and Electronic Commerce, Taipei, pp. 509-512, 2009.

[10] L. S. Reddy and M. V. N. K. Prasad, “Extended Visual Cryptography Scheme for Multi-secret Sharing,” pp. 249–257, 2016, doi: 10.1007/978-81-322-2529-4.

[11] Kim, M., Park, J. and Zheng, Y. 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.

[12] 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.

A. Srivastava, “A Secret Sharing Scheme for Secure Transmission of Color Images,” pp. 857–860, 2014.

[13] W. Fang, “Offline QR Code Authorization Based on Visual Cryptography,” no. 1, pp. 2–5, 2011, doi: 10.1109/IIHMSP.2011.10.

[14] Hegde, S. Manu, P. D. Shenoy, K. R. Venugopal, and L. M. Patnaik, “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications,” no. Vc, pp. 65–72, 2008.

[15] Y.V. Subba Rao, Y. Sukonkina, B. Chakravarty and U. K. Singh, “Fingerprint Based Authentication Application using Visual Cryptography Methods”, TENCONIEEE, pp. 1-5, 2008.

[16] Wu Z, Liu Y-N, Wang D, Yang C-N (2019) An efficient essential secret image sharing scheme using derivative polynomial. Symmetry 11(1):69. https://doi.org/10.3390/sym11010069

[17] J. Chen, T. Chen, H. Hsu, and Y. Lin, “Using multi-ringed shadow image of visual cryptography to hide more secret messages,” vol. 57, pp. 101–109, 2009, doi: 10.1179/174313108X384656.

[18] M. Kamath, A. Parab, A. Salyankar, and S. Dholay, “Extended Visual Cryptography for Color Images Using Coding Tables,” pp. 1–6, 2012.

[19] Z. Fu and B. Yu, “Research on Rotation Visual Cryptography Scheme,” pp. 538–541, 2009, doi: 10.1109/IEEC.2009.118.

[20] S. Jian, S. Huang, Y. Lee, R. Wang, and K. Chen, “Sharing multiple secrets in visual cryptography,” vol. 40, pp. 3633–3651, 2007, doi: 10.1016/j.patcog.2007.03.012.

[21] S. Wan, Y. Lu, X. Yan, Y. Wang, and C. Chang, “Visual secret sharing scheme for (k , n) threshold based on QR code with multiple decryptions,” J. Real-Time Image Process., 2017, doi: 10.1007/s11554-017-0678-3.

[22] M. A. Salama, M. F. M. Mursi, and M. Aly, “Safeguarding images over insecure channel using master key visual cryptopgraphy,” Ain Shams Eng. J., 2018, doi: 10.1016/j.asej.2018.03.002.
[23] J. B. A, C. Raj, R. Sukumaran, and S. M. G, “Enhanced semantic visual secret sharing scheme for the secure image communication,” 2019.
[24] T. Zhao and Y. Chi, “Hierarchical visual cryptography for multisecret images based on a modified phase retrieval algorithm,” 2020.
[25] (2021) Two in one image secret sharing scheme (TiOISSS) for extended progressive visual cryptography using simple modular arithmetic operations. 74, 102996. https://doi.org/10.1016/j.jvcir.2020.102996
[26] P. Li, J. Ma, L. Yin, and Q. Ma, “A Construction Method of (2 , 3) Visual Cryptography Scheme,” IEEE Access, vol. 8, pp. 32840–32849, 2020, doi: 10.1109/ACCESS.2020.2973659.
[27] Verheuland H. V. Tilborg, ”Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes. ”Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.
[28] C.Yang and C. Laih, “New Colored Visual Secret Sharing Schemes”. Designs, Codes and cryptography, 20, pp. 325– 335, 2000.
[29] M. Karolin and T. Meyyapan, “RGB Based Secret Sharing Scheme in Color Visual Cryptography,” vol. 4, no. 7, pp. 151–155, 2015, doi: 10.17148/IJARCCE.2015.4734.
[30] M. F. P and A. J. R. P, “(N , N) Secret Color Image Sharing Scheme with Dynamic Group,” vol. 06, no. June, pp. 46–52, 2015, doi: 10.5815/ijcnis.2015.07.06.
[31] Jeng-Shyang Pan a, Tao Liu a , Hong-Mei Yang a , Bin Yan b , Shu-Chuan Chu a,∗ , Tongtong Zhu b, “Visual cryptography scheme for secret color images with color QR codes,”.