JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

VISUAL CRYPTOGRAPHY FOR BIOMETRIC PRIVACY, AUTHENTICATION AND GENERAL ACCESS STRUCTURE: A REVIEW

B. Rebecca Jeyavadhanam[1], B. Angel Rubavathy[2]

[1,2]Department of Computer Applications, SRM Institute of Science and Technology, Kattankulathur.

Received: 14 April 2020 Revised and Accepted: 8 August 2020

ABSTRACT: Biometric has influenced our daily activity tremendously. Many countries have planned to use biometric for national ID cards, immigration control, law enforcement and so on. In our day to day activities, we use biometric for banking, workplaces, abode, mobile phones even in healthcare organizations. Biometric is the metric that is used to identify a person to grant access. The various biometric traits may be in the form of fingerprint, face, iris, voice, hands, DNA and signature. Securing these biometric configurations is also important, because hackers can use these traits and pretend to be another person. One of the essential techniques used to secure the biometrics is visual cryptography. In this study we have provided state-of-th-art various existing techniques for securing biometric privacy using visual cryptography and also different processes concerning securing the biometric data. We have done a review on the schemes using visual; cryptography for authentication and biometric security. We have also discussed about the novel approaches of visual cryptography in various fields that have caught the importance in recent years. We made an extensive study and distinguished the different methods used for preserving the privacy of the biometrics, image security and authentication in various aspects. The challenges of working with biometrics are impersonation attacks, immutability of templates and preserving information private. In order to overcome these challenges, we are going to develop an algorithm that would help in preserving the biometric privacy of authenticated users using the general access structure.

I. INTRODUCTION:

We live in the era of technical advancement in communication and data transfer, on the other hand securing these communications and data would be a tedious job for techies. On account of securing the transferred data various algorithms based on various programming languages have been found. One such techniques is cryptography, which would help in protecting the information through encrypted text and these texts can be decrypted only by the specified person. The use of cryptography has begun much earlier than to be estimated certainly before four hundred decades in the form of hieroglyph by Egyptians to transfer the secret message to the kings. In today's world, we use cryptography for the secure transmission of data through internet channel but the disadvantage of using cryptography is that on both the end (sender and receiver) there should be a technical person which has paved way for visual cryptography, Where there is no need of the technical person in the receiver side because the decryption can be done with the help of the human visual system or by performing OR or XOR operations.

The convenient use of visual cryptography has laid the foundation for using this technique in various fields. The idea of visual cryptography was first introduced by Moni Naor and Adi Shamir in 1994[2]. The main plan of action for visual cryptography is that a single secret image would be split into two shares and are sent, on the receiver side these shares are collected, printed in transparency and overlapped one above the other to reveal the secret information.

Visual cryptography aided in moving information safe. Therefore, many fields have implemented this technique for image security, authentication, protecting biometric privacy, password protection, banking customer identification, key management, and son on. The traditional passwords do not exist any longer in the technical era, everyone has moved to biometrics to secure their information. There are various traits that are unique for every individual like iris, fingerprint, hand vein, palm print, ear, voice, signature, finger geometry, retina, DNA and grip recognition. The usage of biometric traits began in the 1800s where Alehouse Bertillon developed a method for identifying criminals using body measurements. In today's world, over 7.5 million people are using biometrics to secure their computers, mobile phones, employee identification in companies, banking. In the sequence of securing these traits, various techniques have been formulated one of the effective techniques is visual cryptography. In this paper, we have done an extensive review of the various schemes available in visual cryptography for securing biometric privacy, scheme for authentication, for image security, and schemes that have used general access structure along with visual cryptography.

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

II. VISUAL CRYPTOGRAPHY:

Whizzing increase in communication technology have caught eyes for various classification of data transfer. Which in turn leads to increasing issues in security for the concerns of having huge data to process like banking, universities, data communication in the military and so on [1]. In order to overcome these security issues, various secret sharing technologies have been implemented as one of the production methods for security is visual cryptography. This method emerged by Naor and Shamir in 1994 [2] which paved the way for the innovative way of sharing secret images through the internet. Visual cryptography is a cryptographic technique that would help I transmitting visual information in encrypted form through the internet. Encryption process involves in splitting the secret image into two shares by expanding the pixels of the image and creating noise in the image, during the decryption these separates shares are printed in transparent sheets and overlapped one above the other to reveal the secret information

In order to demonstrate the Noar and Shamir mechanism the secret image would be split into two shares, these shares do not have complete information about the confidential data, during the decryption the shares are superimposed to form the secret images or data. Even if one among the shares are missed, they do any reveal any information. There were various schemes proposed by authors in the various time periods which has helped in securing the secret information some of the schemes are described in this section. K out of n visual cryptography scheme [3], where the confidential image would be split into n shares. In this scheme not all shares are needed to reveal the information, only if k shares are available the secret can be disclosed. An extended version of this scheme was proposed in which k is considered to be constant for all the systems. Ateniese G et al. [4] projected definition got k out of n system upholding at least a convinced system state level may require a dissimilar number of mechanisms to be at a certain state or above; k. Shankar et al [5] have suggested a technique where in order to produce the 'n' transparencies certain condition has been given to the haphazard matrices and then XOR operation would be performed. Other schemes include two out of two schemes where each pixel of the binary image would have two subpixels and three out of three schemes in which the visual secret would be divided into three shares. Some

precursor of visual cryptography was in copyright from the 1960s [6]. Another precursor was in the work on observation [7] has sheltered communication Kafir and Keren 1987[8].

III. VISUAL CRYPTOGRAPHT FOR IMAGE SECURITY

Visual cryptography has been used for securing data that travel through internet channels. There are various approaches used to prtect the pictorial information and also to enhance the standard of the image has been elaborated in this section. Kezheng et al. 2008 [9] has proposed a sub-block coding technique, where the secret image is disordered by row-column; next, the disordered image is converted into two shares by interleaving and arithmetic operation is done to every t × t block for encryption. Hou 2003 [10] projected a scheme in which the secret image would be divided into four shares one share would be a black mask and the other three would be the normal share from the confidential image. In order to reveal the secret information, the receiver should have the black mask. Am extended version of this scheme was proposed by Leung et al. 2009 [11]. Where he has proved that by applying the scheme for the image with two-color the probability to disclose the secret information has improved. A visual cryptographic scheme that uses flipping the image for decryption has been proposed by Lin et al. 2010 [12]. It helps is transferring two secret images through the channel. In order to decode the two-secret image, the first image would be decoded by pilling the shares one above the other, whereas the second image would be revealed by flipping one of the shares and piled one above the other to decode the second image. A scheme for securing color image has been developed by S. and Loganathan 2011 [13], in this scheme two shares are created, the color image would be decomposed to from the monochromatic image which would be then converted into the binary image. Share one would be created by encrypting the binary image and binary key image together forms the cipher image, share two would be created by performing XOR operation on the binary key image and the halftones of the secret image. The efficiency of the image security depends on the channel where the image passes through.

Han et al. 2013 [14] has combined visual cryptography and digital watermarking which involves performing watermarking twice. The input image would be immersed with the discrete wavelet transform (DWT) followed by the second watermarking to create a share. Another share has to be combined with the low-frequency DWT which would result in high security. K out of k visual cryptography scheme was developed by Guo et al. 2014 [15] wherein any k shares can disclose the secret information. If there would be less than k shares would not reveal any information. A scheme for preserving the sixteen-segment text was propounded by Mukherjee and Gabguly 2015 [16]. Where sixteen-segmented text would be converted into an image and are divide into two shares using visual cryptography. The resultant of these scheme doesn't show any loss of information. The keyless data hiding method has been proposed by Ansari and Shaikh 2016 [17], in which the secret information would be divided into three shares in the form of an RGB channel wherein the importance is given to data binding which would result in data security. In order to secure the data K. and p. 2015 [18] proposed an approach where the secret image is spilt with the help of (2,2) XOR of visual cryptography, these shares are encrypted with the help

of Advanced Encryption Standard (AES) algorithm which produces encapsulated shares. Any single shares would not disclose any information. The proposed scheme offers effective encryption which results in secure data transfer.

The k out of visual cryptography was first initiated by Naor [19] where the confidential information would be divided into n shares and transmitted in the channel; in order to reconstructed the image k shares would be needed, shares less than k would not reconstruct the information. There are many extended versions for this scheme Shankar and Eswaran 2016

[20] has constructed a scheme to communicate images through a public channel, where the new condition has been implemented for random matrix creation and XOR operation is performed to create n shares. The secret data cannot be acquired by changing any illegal subsets which protect the data in public channels. Hierarchical visual cryptography for the grayscale image has been projected by Patel and Srivastava 2016 [21]. Hierarchical visual cryptography involves encrypting the secret image at various levels which would result in high secured transmission.

These shares are transported on the internet channel; all the shares are necessary to reconstruct the confidential information. The resultant image has high quality and it is the same size as the input image. By combining visual cryptography along with the discrete cosine transform (DCT) for image compression to secure the confidential information has been developed by Ravella and Chavan 2017 [22]. The procedure of this scheme is that the secret image would split into shares with the help of visual cryptography later the obtained shares would be compressed with the help of the IDCT and transferred through internet, all the shares would be necessary to reconstruct the information; in this scheme, the storage for the image has reduced. Dhiman and Kasana 2018 [23] has given two extended approaches for visual cryptography in which the first scheme involves in extending the (k, k) VC where the secret image would be divided into three shares corresponding the R, G, B components respectively; all the shares would be necessary to reconstruct the information. On the other hand, the second technique has been the extended technique of the (k, n) VC in this scheme the image involves in creating shares corresponding to RG, GB, RB components respectively; any two shares would be needed to restore the confidential information. All the shares created in this approach are meaningful and resulted in lossless transactions and can be applied in a real-time environment. An approach for the color image was developed by Prakash et. al., 2011[24], In which the color images would be encoded with the help of the half-toned meaningful share and along with the direct binary search (DBS). The results of the recovered images are lossless and have good visual quality.

To enhance the calibre of the confidential information Chaturvedi et at. 2018 [25] has proposed a scheme in which denoising and logical resizing of the image has been applied in order to maintain the quality of the shared image. Digital image security has been developed by Bhatia et al. 2018 [26]. In the proposed various methods have been implemented like RC4 cipher algorithm, RGB companies, image division, pixel shifting, combing using visual cryptography resulting in the creation of share of images that are then opened into the network. The result shows high security for shares. The probabilistic scheme has been proposed by Wu and Yang 2020 [27]. A cryptographic technique based on a color image, black image and white image have been suggested in this a paper where in general methodology when the pixel expansion increases the size of the images increases there here the probabilistic color-black-and white visual cryptography has been implemented by separating n X m distribution into n X 1 column matrices. This method has been feasible for security and contrast conditions. Many schemes proposed to suffer from noise in image and security, in order to overcome the technique with a shared key concept. In this method secret share would be encoded by dividing into 3 shares corresponding to the imposed scheme, and also 2 out of 3 schemes have been used for reducing the time for decryption which result in the security of the data and contrast correction proposed by Tripathi et al. 2020 [28].

Even though there were many schemes propounded to improve the caliber of the confidential information, the outcome of the scheme has not given picture quality because of contrast and pixel expansion. Prisco et al., 2011 [29] have given an approach as a color model that produces a random share for color images in the form of black and white secrets; the results of the images show a meaningless color image. With reference to this model [30] Hsiao and Wang 2012 constructed a model in which the input black and white image would be injected with the color pixels into a shared image, the results of this model show a high caliber for the reconstructed secret image. Pujari et al. 2014 [31] have established a system with the Jarvis halftoning and encoding tables to encrypt the information. In the same way, the Average filters and decrypting tables are used to decode the information and to maintain the caliber of visual information.

IV. VISUAL CRYPTOGRAPHY FOR BIOMETRIC SECURITY

There have been many issues relating to biometric data since the biometric system was impuissant Ratha et al. 2001[32]. It would be easy for the muggers to snatch the data; in order to secure these data various efficient techniques have been used like steganography, visual cryptography, watermarking and half-toning due to the introduction of the biometric traits the signatory of a person has lost their importance in individualism and production where the biometric is acquiring importance in acceptability and collectability [33]. There are

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

numerous techniques that are being suggested to safeguard the features of biometric traits. In this proposed work the Surya Devara et al. 2011[34] has done a novel approach of using the tongue biometric for the banking system, in order to safeguard the biometric data k out of n visual cryptography scheme has been used to improve the productivity of the approach. An iris biometric has been proposed in this system for employee authentication in a company by Chutake, Vinay et al. 2014[35]. In this system first, the iris features are extracted, visual cryptography is applied, and creates shares and stockpiled in the directory. The shares present in the directory and the features extracted by the employee iris are collected to authenticate the employee. To explicate the privacy of the biometric data [36] Meshram, S.P., & Longadge, R. 2014 has propounded an approach where inverted share image visual cryptography has been used, in which one of the shares would be inverted and stacked with the other share to produce a confidential image for authentication. He also added the non- expanded scheme so that the size of the image remains the same size which helps in maintaining the privacy and stabilizing image size. To determine privacy-preserving Rajanwar, Shubhangi, et al. 2014; Ibjaoun et al. 2018[37-38] have demonstrated a method in which the visual cryptography has been used. In order to execute this procedure one confidential information image and two cover images are involved, Floyd Steinberg Error Diffusion algorithm and halftoning are used to transform the large scale input image into small scale input image, shares are created using visual cryptography and superimposed with the image to cover secret image, both the cover image would be needed to reconstruct the sneaky information from the image; which helps in privacy- preserving This system has been followed by many companies for employment authorization. In this authentication system, a biometric feature of the fingerprint is taken and visual cryptography would be implemented to transform the image into shares, one of the shares would be safeguarded in the trusted entity and another share would be stored in the ID card. During the process of authentication, the user has to give the fingerprint and ID card, so the share safeguarded in the smartcard the share in the trusted entity would be collated and matched with the fingerprint of the user for authentication. Processing time would be low and it would be secured authentication because only one share would be available in the database which will not reveal any information [39]. The Privacy preserving method projected by Sarika, M.P. (2017)[40] has two processes: Enrolment process and Authentication process. During the enrolment process, the fingerprint of the user would be collected and processed to create two shares using visual cryptography, both the shares are stored separately in a trusted server; When the user wants to authenticate both the shares are taken from the server and superimposed and matched with the given image. Anusree and Binu 2014[41] have commingled visual cryptography, halftoning, and watermarking to procedure a new approach. As the first step of the approach, the secret image is decomposed with the basic visual cryptography, the decomposed image made to undergo the halftoning and encoded with the secret information; then the encoded images would be bonded together and creates the secret information. which then undergoes visual cryptography and forms shares; the shares created would be watermarked to get the encrypted share of the confidential information. All these procedures are reversed to reconstruct the original secret information. Rajanwar, Shubhangi et al. 2014[42] have used one secret image and two cover images. During the login stage, the user has to give the username, password, and the secret image. The image is processed with the Floyd Steinberg Error Diffusion algorithm for resizing the Simple Block Replacement algorithm for storing the pixels of the image in the database with proper order. One of the shrews would be kept in the directory and another share would be given to the user in the form of a smartcard. During authorization, these shares would be matched with the share given to the user would be termed authorized even if the pattern matching percentile would mark less than 98% the user would be considered unauthorized. Gupta and Sharma 2016 [43] have to be created a model for biometric privacy with the alliance of visual cryptography, steganography, and QR code. First the biometric of the user has to be taken and visual cryptography would be applied to them to create two shares, both shares are then converted into stegno image; one of the stegno images are saved in the database and the other segno image would be converted into QR code and given to the user for authentication. When user login the OR code would be given along with the fingerprint for matching.

In this approach, three traits have been used: iris, fingerprint, and face features. Three shares are formed for processing the first share would be created by the combination of iris image and cover image, the second share consists of the fingerprint image which would be kept in the smart card. The third share creation would be the share obtained in the first process would be rotated 90 degrees and combined with the facial feature. If all the features match, the user would be authenticated [44,45]. The user face features are extracted to decompose and combined with the host image to secure the information of the individual. The decomposed image would be split into shares called sheets and safeguarded in a trusted entity server. In the process of authentication server would request for the sheets and match the user features with Boolean operation [46]. This method proposed by Suganya 2017 [47] has the same features as the above mentioned by it does not combine any cover image to fingerprint biometric. It has the enrolment process in which the fingerprint would be created as shares using visual cryptography and would be stored in the third-party directory during the authentication the user fingerprint would be matched with the database data using XOR operation. This approach involves an iris trait evolved by Esai Puvanesh, S. et. al 2018 [48].

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

Where the iris feature of the user has to be recorded, the image has to undergo watermarking in order to maintain the integrity of the iris image, then the image involves the visual cryptography to produce shares; one share would be kept in the directory, other shares would be with the user, during authentication both the images are matched using OR operation.The face image of the user is extracted and they undergo pre-processing where the RGB image would be converted into a grayscale image and decomposed using DWT, then the image safeguarded in the directory. In order to authenticate the user, the sample image decrypted and matched for verification[49]. In this approach B.k et al. 2018; Madankar et al. 2018[50] use the face, fingerprint, and retina of the user. Each of the features would be given a cover image they combined to take the pixel value ratio and converted into binary image further shares are created and stored in a third-party server. authentication process involved in decrypting the image and matching with the user's share. Toli and Preneel 2018 [51] have given an application for mobile to preserve the biometric authentication of the e-Finance application; it works on the bases of pseudonymous biometric identities. It leads to the toolkits of various privacy management in financial services.

An approach where both the secret image and cover image should be of the same size. An extended visual cryptography scheme has been used to produce the shares and is used to restore the size of the image. Actual VC only for black and white images. The digital halftoning method used to print the maximum number of shades; the error diffusion method has been used for quantization error [52]. This paper protection-related-behaviours which helps in securing the biometric systems. They have done a survey on the students of the university to involve in the protection of biometric content with the help of the Theory of planned behaviour and attitude aspects. It has changed the user by giving them security information. This survey was conducted by Oh et al. 2018[53].

V. VISUAL CRYPTOGRAPHY FOR AUTHENTICATION

Security plays a vital role in data transfer through internet channels. In order to overcome the security issues, various authentication methods have been proposed. In this section, we will see about the authentication of the user to access a document or credential by implementing visual cryptography for authentication was the first demonstration was done by Naor and Pinkas where they have propounded the visual secret sharing for authentication of documents and confidential information [54]. An image while stored in the public channel it would be predominant to safeguard the image (data), which cannot be achieved by storing them in one area for which Ross A. et, al[55] has proposed a technique where the single picture would be split into shares and stored in different servers and gathered to form the secret image. Giuseppe A. et al has defined a protocol that utilizes the visual Cryptography for authentication of the user. [56] In the process a password would be created in the form of a visual image, then visual cryptography would be applied to form shares. These shares are combined together for authentication. This proposed method can be applied to multiple users. Multiple user authentication protocols have been developed by Prakash. A.et al. 2016 [57] where the secret image would be split into shares and kept in third-party server; these shares would be given as the password for the authentication, therefore when user wants to access the combination of multiple user's passwords would only authenticate else it would remain unauthenticated. This protocol would help in the multi-user authentication

A secret image transmission proposed by [58] Mandal and Ghatak 2011 with a meaningful share. To demonstrate an LSB would be applied to the binary cover image which would produce grayscale image further (2, 2) VC would be applied to produce shares. These shares are hidden in meaningful shares separately and sent in through an internet channel. At the decryption end, the shares would be extracted from the image and superimposed to get the confidential information; noise reduction would be applied to reconstruct the original image. Horng et al. 2006 [59] have initiated the threat of cheating that could happen while using k out of n visual cryptographic scheme where the forged confidential information has to be swapped with an actual secret image. Authentication based cheating prevention has been proposed by Prisco et al. 2010 [60]would place on the designated end which will do the authentication and prevent the image from cheating. Chen et al. 2012 [61] has attempted to create authentication based cheating prevention with the help of the other author and has implemented a specific verified pattern which would in turn secure the share and authenticate the user. In order to prevent the attacker's traditional visual cryptography scheme combined with the authentication traits to transport secure data was developed by Fang 2006 [62]. On the other hand, Huang and Chang 2013 [63] have proposed a system with the help of the non- expanded scheme where the shares are created and one among the shares are shifted and transported along the channel; this method would give high prevention of the data. Lossless watermarking has been proposed by Wang et al. 2013 [64] where visual cryptography has been used for authentication. The author has created one share with the help of cover image and another share has been created with the help of the watermarked image, where the disposable and re-constructible characteristics of the share would help in authentication of the user and for reliability.

Hierarchical visual cryptography has implemented this method for authentication. In this demonstration, the signature of the user has been saved as the image hierarchical visual cryptography would apply to create four shares, where three shares would be used to create the key for authentication one of the shares has to be given to

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

the user for verification in the form of the smart card. During the authentication, the share of the user would be matched to verify [65]. Maeng et al. 2015 [66] have propounded an authentication protocol for the bank transaction with multiple users. It provides a novel visual cryptographic scheme where a single share can have more than one user and also adopted complementary colors in color mixing models. During the authentication, the user share would be superimposed with the saved details to provide results. The security of the biometric image cannot be secured if they are stored in one location, therefore [67]Rao and Patil 2015 has suggested a method where the biometric image would be separated into 2 shares; each share would be converted into QR code and stored

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

in different server; in order to reconstruct the image, the QR code would be converted into share image to form the private image. Nandhini Preetha and Radha 2016 [68] has projected an approach which has used finger-vein along with the signature in which both the images would be taken from the user and the features of the images are extracted using cross number concept and principle compound analysis. These features are fused together to form an image, which then goes through a visual cryptographic scheme to form shares and stored in different databases. During authentication, it would be necessary to have both the images.

An IoT device for secret sharing has been proposed by [69] Arafin and Qu 2016 where the additive and monotonic nature of RRAM has been combined with the secret sharing. The device has multiple user authentication and robustness which helps in securing the primitives and resource constraints. Sterilization based visual cryptographic scheme has been suggested by Dalvi and Wakde 2017 [70] where the secret image would be separated into red, green, blue channel respectively; in each channel 8 shares and 8 key would be created using sterilization technique, these shares would be then combined to form 3 shares for each channel like 3 shares for red, 3 shares for green and 3 shares for blue; all these shares would be combined together and forms a single encrypted image and would be transferred to the user. In order to decrypt the user will have to apply desterilization using the key and the final decrypted image would be extracted. In this (n, n) visual cryptographic scheme the Daisy et al. 2017 [71]has used the cover images to conceal the secret image after encryption. During the demonstration, Jarvis Filter and Halftoning have been used to create the shares. These shares would be hidden underneath the cover image and sent to the specified person, during the authentication process the shares imaged would be used. Thus, the visual cryptography would help in the process of authentication of the user in various methods.

VI .VISUAL CRYPTOGRAPHY SCHEMES USING GENERAL ACCESS STRUCTURE

General access structure (GAS) has been initiated by [72] Ateniese et al. 1996 where the participants would be divided into two sets one the qualified set another one would be forbidden set. The secret image would be split into shares using visual cryptography and each participant would have a separate share. The combination of the qualified set could only reveal the secret image whereas the forbidden set would not be able to construct the image or information. Xu et al., [73] have suggested a method in which a group signature would be created using the authorized subset any unauthorized subset cannot access the information. The security of the method would be based on the discrete log problem; this method would be more secure than the Lagrange interpolation polynomial for GAS. A multi-pixel encoding has been done with the help of the pixel block wherein the pixels of the image would be read in zigzag manager and they can be scanned in the same manner which would work prompt for both threshold access structure and also for general access structure without pixel expansion and contrast diffusion projected by [74] Zhang et al. 2008.

In this approach Wei et al. 2008 [75] have used a one-way function where the discrete log problem of the previous method has been rectified and the user can impose additional secrets into the channel and the participation set of the authorized set could be modified dynamically. The complexity of the scheme has been minimized for reliability. Multiple secret sharing schemes have been proposed by Ye et al. 2009 [76] where (p-1) the degree Lagrange interpolation polynomial in which p number of confidential information could be transferred through a secured passage and the secret shadow for the candidate would be chosen by themselves. In this method the qualified set would be changed dynamically with refreshed shadow images; it would be more flexible since the scheme has been formed using GAS. While the data travels through the channel it would go through management problems. Lee and Chiu 2012 [77] have constructed a scheme to rectify this problem. In which they designed two steps where in the first phrase a meaningless share would be constructed with GAS and in the second stage the share would be covered by the meaningful image directly on the shares using the stamping algorithm. The proposed method has reduced pixel sharing and visual identification of the secret message.

A scheme for a random grid has been propounded by Shyu 2013 in which any binary or color image would be split into shares and distributed to various participants[78]. A combination of the shares of the qualified set would reveal the secret whereas the forbidden set would not give any information. In this method, excessive pixel expansion would be reduced. A method using tagged image has been suggested by Chen et al. 2014 [79] tagged image meaning printing the pattern of secret onto the meaningless share. In this proposed work, the author has used a qualified set of participants to access the secret image and other unauthorized would not be able to reconstruct the image and form the pattern. The problem of image reconstruction and contrast has been rectified. Turmoil shares would successfully transfer the images to the receiver but it would suffer the management problem since the decoder would not be able to identify the proper to superimpose in order to rectify them the extended visual cryptography scheme would stamp the cover image over the turmoil share so that the decoder would identify. The random grid would take care of the pixel expansion and reconstruction of the image done by [80] Mishra and Biswaranjan 2015.

In this work, the (k, n) visual cryptography scheme has been reconstructed as an integer linear program and made them general to all the images. The pixel expansion in the general visual cryptography scheme has been

compared and the results show minimal expansion and the unauthorized set cannot reveal any information that makes it more secure proposed by Shyu and Chen 2015 [81]. A visual secret sharing has been propounded by [82]S Yan et al. 2016 where the decryption can be done with multiple ways like using OR operation and XOR operation it also includes the random grid which would involve in minimizing the pixel expansion and the random grid would involve in acquiring the properties of progressiveness and GAS. Only the qualified sets would be able to decode the image with minimal pixel expansion and no codebook design. In this process share transforming, multiple users should contain multiple secrets in order to overcome this the collaborative scheme would be converted into multiple secret schemes with the favour of GAS. The construction of this collaborative visual scheme has been done with the help of the integer linear programming which would help in the minimal pixel expansion and each user would have only one secret to transfer in the channel projected by [83] Jia et al. 2018.

The threshold-based scheme has been projected by [84]Meng et al. 2018 where GAS does not acquire all shareholders therefore universal GAS scheme has been propounded where it also implements the Chinese remainder theorem to make sure these structures would accept all the

general access structure. According to number theory, Chinese remainder theorem can be defined as the one can recognize the remainder formed by the Euclidean division which has been performed on the n integer by several integers, [85] the remainder formed by this division would could the division of the integer with a particular condition that it should be coprime. Color black and white visual cryptography scheme has been constructed by Wu and Lai 2019

[86] which would whippy in sharing the images It also included the random grid to overcome the unwanted pixel expansion The author has also included the GAS, therefore, the secret could be accessed only by the qualified set of participants, which can be implemented for binary or color images. It would result in predominant pixel expansion and secured transmission.

VII. APPLICATION OF VISUAL CRYPTOGRAPHY IN OTHER FIELD:

The internet has become the fastest-growing communication medium where the data move through the network channels, therefore it is necessary to transfer the data tenable. Consequently, so the application of visual cryptography in various fields has increased, some of the application of visual cryptography has been mentioned in this section. The banking sector has got the large importance of visual cryptography. This scheme developed by Jain and Soni 2017[87] implies image processing and visual cryptography. The procedure of this image is that the banking is pre-processed using image processing and combined to create a secret image this procedure was developed by Shyu 2018[88]. In the next step the combined secret image separated into shares by (2, 2) VCS(XOR), one image for bank executives another for users; combined together reveals the secret image used for bank transactions. The resultant images were the same size as the input image and secured. An extended (n, n) scheme has been proposed by Salama et al. 2018 [89]. In this technique a master key is generated with the help Station-to-Station Diffie Hellman algorithm; another method of hierarchical share has been generated depending on the degree of security which means the user decided the number of shares per secret. The proposed method has been proved to be robust and secured. Yang et al. 2018 [90] have developed an open EMR system for electronic health records (EHR) management. In this method the EMR is saved in the private system by management, the patients are given a separate password for authentication to reveal the EMR image. The result shows a high performance.

In order to hide data which could not be read by the normal form the combination of the visual cryptography and steganography has been executed in this approach by Abboud et al. 2010

[92] where the original image would be combined with the hidden information with the help of the steganography, the image with this information would be separated into shares and sent in the public channel; in the receiver end the shares would be collected and superimposed to extract the hidden information. which would result in efficiency in security and prominent reconstruction. A contemporary approach for data hiding has been formed by Rudraksha and Giri Prasad 2019 [93] where the original image would be combined with the hidden secret with the help of steganography using plane coding algorithms. Next, the stegno image would be diverged into bits called shares with the help of a k-n visual cryptography scheme and would be hidden beneath the envelope image using LSB replacement and transferred into the channel. During decryption, the information can be caught by performing reverse LSB which would

result in advanced data hiding. Finding a problem in cryptography would not be difficult but finding a proper API to resolve the problem would be a difficult task for most of the researcher therefore in order to overcome the issue [94] Linden et al. 2018 has formed a software which would help in finding the appropriate API for the specific problem with the help of the visual metaphor. It would help in identifying the relevant function for the particular cryptographic problem.

In accordance with the motivation of the Naor's visual cryptography scheme Liu et al. 2019

[95] has propounded a peculiar approach where the secret image would encrypt with the help of the n-qubit

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

which act as the share for this scheme and transferred to the participant in order to view the secret information all the n-qubits are gathered to XOR operation would be performed. Unlike pixel expansion, this approach does quantum expansion which would result in loss lessness in the resolution. An encryption algorithm has been formulated with the help of the edge detection process; the end results of the process give two images one would be the share of the visual cryptography other would be the key for the ciphertext both would be combined together to form the actual secret information. The efficiency of this algorithm was not high but it would help in combing the work of calligraphy and technology projected by Zihan et al. 2019 [96]. A unique approach of cryptographic share has been done propounded by [97] Du et al. 2019 in which there are two shares of a secret image one would be a public image other would be the private image. The public share would be printed on the conventional display whereas the private image would be on the contemporary display when both are superimposed the secret information would be revealed and this technique has been proved tolerant in tracking.
A new novel approach of visual cryptography has been applied using Cascading Style Sheet blend modes proposed by Lee et al. 2019 [98] where there can be more than one blend mode which would help in the decryption of the information. This method would help in resisting the compression of the image and the lossless transaction since the decryption happens on the webpage. OR or XOR operation can be done on the web to decode the information. An approach of visual cryptography for the medical image has been propounded in this paper by Maurya et al. 2020 [99] in which the medical image would be encrypted with the help of the circular shift encryption method and produce three shares which are covered with three cover image and sent to the user for decryption end where the image would be reconstructed with the help of circular shift decryption. This approach has been proved reliable and maintains the contrast of the image. Online voting has got importance in recent years [100] Rane et al. 2020 has implemented this approach in Maharashtra Carrom Association where the voters can vote from any part of the state. In order to vote the voter has to register first so that user id and password would be generated and visual cryptography would be applied to form shares and one share would be sent to the voter through email. Therefore, when the user login the share given by the user and the share stored by the system would be matched in order to maintain the further security the password generated would act as the CAPTCHA and then the voter would vote and count would be updated.

VIII. CONCLUSION:

Visual cryptography is one of the most efficient cryptographic technique which helps in
transferring visual information across the information highway; the main advantage in using visual cryptography is that it wouldn't need any complex computation to decode the information it would be done by printing the shares in transparency piled and tested by the human visual system to reconstruct the confidential information. This paper is the compendium of the various schemes that have been developed by authors for image security, authentication and biometric security using visual cryptography. We have also discussed about the novel application of visual cryptography in various fields. In our future work, we are going to put forth an application of visual cryptography for preserving the biometric of authenticated users using a general access structure. This scheme would be useful for the fields implementing biometrics like law enforcements, access control, banking transaction, workforce management.

IX. REFERENCES

[1] D. Akhawe, A. Barth, P. E. Lam, J. Mitchell, and D. Song, "Towards a Formal Foundation of Web Security," *2010 23rd IEEE Computer Security Foundations Symposium*. 2010, DOI: 10.1109/csf.2010.27.

[2] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology — EUROCRYPT'94*. pp. 1–12, 1995, DOI: 10.1007/bfb0053419.

[3] Verheul, E.R., van Tilborg, H.C.A. Constructions, and Properties of k out of n Visual Secret Sharing Schemes. *Designs, Codes, and Cryptography* 11, 179–196 (1997).

[4] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Computer Science*, vol. 250, no. 1–2. pp. 143–161, 2001, DOI: 10.1016/s0304-3975(99)00127-9.

[5] K. Shankar and P. Eswaran, "A new k out of n secret image sharing scheme in visual cryptography," *2016 10th International Conference on Intelligent Systems and Control (ISCO)*. 2016, DOI: 10.1109/isco.2016.7726969.

[6] Cook RC, inventor; Cook Richard C, assignee. Cryptographic process and enciphered product. United States patent US 4,682,954. 1987 Jul 28.

[7] Arazi B, Dinstein IH, Kafri O. Intuition, perception, and secure communication. IEEE transactions on systems, man, and cybernetics. 1989 Sep;19(5):1016-20.

[8] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Opt. Lett.*, vol. 12, no. 6, pp. 377–379, Jun. 1987.

[9] L. Kezheng, F. Bo, and Z. Hong, "Visual Cryptographic Scheme with High Image Quality," *2008 International Conference on Computational Intelligence and Security*. 2008, DOI: 10.1109/cis.2008.106.

[10] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, no. 7. pp. 1619–1629, 2003, DOI: 10.1016/s0031-3203(02)00258-3.

[11] B. W. Leung, F. Y. Ng, and D. S. Wong, "On the security of a visual cryptography scheme for color images," *Pattern Recognition*, vol. 42, no. 5. pp. 929–940, 2009, DOI: 10.1016/j.patcog.2008.08.031.

[12] S.-J. Lin, S.-K. Chen, and J.-C. Lin, "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion," *Journal of Visual Communication and Image Representation*, vol. 21, no. 8. pp. 900–916, 2010, DOI: 10.1016/j.jvcir.2010.08.006.

[13] G. K. S. and D. Loganathan, "Color image cryptography scheme based on visual cryptography," *2011 International Conference on Signal Processing, Communication, Computing, and Networking Technologies*. 2011, DOI: 10.1109/icsccn.2011.6024584.

[14] T. Guo, F. Liu, and C. Wu, "k out of k extended visual cryptography scheme by random grids," *Signal Processing*, vol. 94. pp. 90–101, 2014, DOI: 10.1016/j.sigpro.2013.06.003.

[15] Y. Han, Y. Shang, and W. He, "DWT-Domain Dual Watermarking Algorithm of Color Image Based on Visual Cryptography," *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. 2013, DOI: 10.1109/iih-msp.2013.100.

[16] I. Mukherjee and R. Ganguly, "Privacy-preserving of two sixteen-segmented images using visual cryptography," *2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*. 2015, DOI: 10.1109/icrcicn.2015.7434275.

[17] N. Ansari and R. Shaikh, "A Keyless Approach for RDH in Encrypted Images using Visual Cryptography," *Procedia Computer Science*, vol. 78. pp. 125–131, 2016, DOI: 10.1016/j.procs.2016.02.021.

[18] S. K. and E. P., "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography," *Procedia Computer Science*, vol. 70. pp. 462–468, 2015, DOI: 10.1016/j.procs.2015.10.080.

[19] O. M. Naor and A. Shamir, Visual cryptography, Pre-proceedings of Eurocrypt '94 (1994) pp. 1–11

[20] A. Sharma and D. K. Srivastava, "K-N Secret Sharing Scheme of Visual Cryptography for Hiding Image Using 2 × 2 Blocks Replacement," *Proceedings of the International Conference on Recent Cognizance in Wireless Communication & Image Processing*. pp. 511– 521, 2016, DOI: 10.1007/978-81-322-2638-3_58.

[21] T. Patel and R. Srivastava, "Hierarchical visual cryptography for grayscale image," *2016 Online International Conference on Green Engineering and Technologies (IC-GET)*. 2016, DOI: 10.1109/get.2016.7916685.

[22] Y. Ravella and P. Chavan, "Secret encryption using (2, 2) visual cryptography scheme with DCT compression," *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*. 2017, DOI: 10.1109/iccons.2017.8250740.

[23] K. Dhiman and S. S. Kasana, "Extended visual cryptography techniques for true color images," *Computers & Electrical Engineering*, vol. 70. pp. 647–658, 2018, DOI: 10.1016/j.compeleceng.2017.09.017.

[24] N. K. Prakash, N. Krishna Prakash, and S. Govindaraju Govindaraju, "Visual Cryptography Scheme for Color Images Using Halftoning Via Direct Binary Search with Adaptive Search and Swap," *International Journal of Computer and Electrical Engineering*. pp. 900–904, 2011, DOI: 10.7763/ijcee.2011.v3.440.

[25] R. N. Chaturvedi, S. D. Thepade, and S. N. Ahirrao, "Quality Enhancement of Visual Cryptography for Secret Sharing of Binary, Gray and Color Images," *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*. 2018, DOI: 10.1109/iccubea.2018.8697870.

[26] S. Bhatia, S. K. Khatri, and A. V. Singh, "Digital Image Security Using Hybrid Visual Cryptography," *2018 7th International Conference on Reliability, Infocom Technologies, and Optimization (Trends and Future Directions) (ICRITO)*. 2018, DOI: 10.1109/icrito.2018.8748622.

[27] X. Wu and C.-N. Yang, "Probabilistic color visual cryptography schemes for black and white secret images," *Journal of Visual Communication and Image Representation*, vol. 70. p. 102793, 2020, DOI: 10.1016/j.jvcir.2020.102793.

[28] J. Tripathi, A. Saini, Kishan, Nikhil, and Shazad, "Enhanced Visual Cryptography: An Augmented Model for Image Security," *Procedia Computer Science*, vol. 167. pp. 323–333, 2020, DOI: 10.1016/j.procs.2020.03.232.

[29] R. D. Prisco, R. De Prisco, and A. De Santis, "Using Colors to Improve Visual Cryptography for Black and White Images," *Lecture Notes in Computer Science*. pp. 182–201, 2011, DOI: 10.1007/978-3-642-20728-0_17.

[30] C.-Y. Hsiao and H.-J. Wang, "Enhancing image quality in Visual Cryptography with colors," *2012 International Conference on Information Security and Intelligent Control*. 2012, DOI: 10.1109/isic.2012.6449718.

[31] V. G. Pujari, S. R. Khot, and K. T. Mane, "Enhanced visual cryptography scheme for secret image

retrieval using an average filter," *2014 IEEE Global Conference on Wireless Computing & Networking (GCWCN)*. 2014, DOI: 10.1109/gcwcn.2014.7030854.

[32] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of Minutiae Matching Strength," *Lecture Notes in Computer Science*. pp. 223–228, 2001, DOI: 10.1007/3-540-45344-x_32.

[33] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2. pp. 125–143, 2006, DOI: 10.1109/tifs.2006.873653.

[34] S. Suryadevara, R. Naaz, Shweta, S. Kapoor, and A. Sharma, "Visual cryptography improvises the security of tongue as a biometric in the banking system," *2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011)*. 2011, DOI: 10.1109/iccct.2011.6075146.

[35] S. Urkude, P. Vaidya, and S. Rajguru, "Visual Cryptography Authentication for Locker Systems using Biometric Input," *International Journal of Computer Applications*, vol. 130, no. 1. pp. 15–19, 2015, DOI: 10.5120/ijca2015906855.

[36] S. Sowkarthika and N. Radha, "Securing iris and fingerprint templates using fuzzy vault and symmetric algorithm," *2013 7th International Conference on Intelligent Systems and Control (ISCO)*. 2013, DOI: 10.1109/isco.2013.6481146.

[37] S. Ibjaoun, A. A. El Kalam, V. Poirriez, and A. A. Rahman, "Biometric Template Privacy Using Visual Cryptography," *Advances in Intelligent Systems and Computing*. pp. 309–317, 2018, DOI: 10.1007/978-3-319-76354-5_28.

[38] H. R. Sah, "A novel privacy-preserving visual cryptography based scheme for telemedicine applications," *Biomedical Research*. 2018, DOI: 10.4066/biomedicalresearch.29-17-519.

[39] M. Sarvabhatla and C. S. Vorugunti, "A Secure Biometric-Based User Authentication Scheme for Heterogeneous WSN," *2014 Fourth International Conference of Emerging Applications of Information Technology*. 2014, DOI: 10.1109/eait.2014.23.

[40] P. PradeepBhirud and N. Prabhu, "Secured Biometric Authentication using Visual Cryptography and Transforms," *International Journal of Computer Applications*, vol. 77, no. 8. pp. 23–28, 2013, DOI: 10.5120/13415-1081.

[41] K. Anusree and G. S. Binu, "Biometric privacy using visual cryptography, halftoning and watermarking for multiple secrets," *2014 IEEE National Conference on Communication, Signal Processing and Networking (NCCSN)*. 2014, DOI: 10.1109/nccsn.2014.7001156.

[42] J. Rao and V. Patil, "Visual cryptography for image privacy protection using diverse image media," *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. 2015, DOI: 10.1109/icgciot.2015.7380582.

[43] H. Gupta and N. Sharma, "A model for biometric security using visual cryptography," *2016 5th International Conference on Reliability, Infocom Technologies, and Optimization (Trends and Future Directions) (ICRITO)*. 2016, DOI: 10.1109/icrito.2016.7784975.

[44] I. D. Judith, I. Diana Judith, G. J. Joyce Mary, and M. Mary Susanna, "Three-factor biometric authentication for spiraling of security," *2016 International Conference on Emerging Trends in Engineering, Technology, and Science (ICETETS)*. 2016, DOI: 10.1109/icetets.2016.7603017.

[45] Z. An, W. Deng, and J. Hu, "Deep transfer network for face recognition using 3D synthesized face," *2017 IEEE Visual Communications and Image Processing (VCIP)*. 2017, DOI: 10.1109/vcip.2017.8305094.

[46] B. Swathi and T. Madhavi Kumari, "Iris biometric security using watermarking and visual cryptography," *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*. 2017, DOI: 10.1109/icpcsi.2017.8391904.

[47] Suganya, M., And S. Suganya. "A Fingerprint Biometric Privacy Using Visual Cryptography." (2017).

[48] J. Oh, U. Lee, and K. Lee, "Reminder as 'Watch-Out': The Role of Privacy Salience at the Point of Interaction with Biometric Systems," *2018 International Conference on Platform Technology and Service (PlatCon)*. 2018, DOI: 10.1109/platcon.2018.8472767.

[49] M. Madankar, S. D. Sawarkar, and D. J. Pete, "Biometric Privacy Using Various Cryptographic Scheme," *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*. 2018, DOI: 10.1109/gcwcn.2018.8668637.

[50] Applications," *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. 2018, DOI: 10.5220/0006611303530360.

[51] C.-A. Toli, A. Aly, and B. Preneel, "A Privacy-Preserving Model for Biometric Fusion," *Cryptology and Network Security*. pp. 743–748, 2016, DOI: 10.1007/978-3-319-48965-0_54.

[52] Kumar and A. V. Senthil, *Biometric Authentication in Online Learning Environments*. IGI Global, 2019.

[53] S. B.k, B. K. Sapna, and K. L. Sudha, "Secured Transmission with Enhanced Security for Grayscale Images using Visual Cryptography," *2018 International Conference on Networking, Embedded and Wireless Systems (ICNEWS)*. 2018, DOI: 10.1109/icnews.2018.8903924.

[54] M. Naor and B. Pinkas, "Visual authentication and identification," *Advances in Cryptology — CRYPTO*

'97. pp. 322–336, 1997, DOI: 10.1007/bfb0052245.

[55] Giuseppe Ateniese1, Carlo Blundo2, Alfredo DeSantis2, and Douglas R. Stinson3 Extended Schemes for Visual Cryptography June 14, 1996.

[56] D. Wang, F. Yi, and X. Li, "On general construction for extended visual cryptography schemes," *Pattern Recognition*, vol. 42, no. 11. pp. 3071–3082, 2009, DOI: 10.1016/j.patcog.2009.02.015.

[57] K. K. Prakasha, K. Krishna Prakasha, B. Muniyal, Srushti, and D. Shetty, "Multi-user authentication protocol using visual secret sharing," *2016 International Conference on Inventive Computation Technologies (ICICT)*. 2016, DOI: 10.1109/inventive.2016.7830205.

[58] J. K. Mandal and S. Ghatak, "Secret image/message transmission through meaningful shares using (2, 2) visual cryptography (SITMSVC)," *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*. 2011, DOI: 10.1109/icrtit.2011.5972344.

[59] G. Horng, T. Chen, and D.-S. Tsai, "Cheating in Visual Cryptography," *Designs, Codes and Cryptography*, vol. 38, no. 2. pp. 219–236, 2006, DOI: 10.1007/s10623-005-6342-0.

[60] R. D. Prisco, R. De Prisco, and A. De Santis, "Cheating Immune Threshold Visual Secret Sharing," *The Computer Journal*, vol. 53, no. 9. pp. 1485–1496, 2010, DOI: 10.1093/comjnl/bxp068.

[61] Y.-C. Chen, D.-S. Tsai, and G. Horng, "A new authentication based cheating prevention scheme in Naor–Shamir's visual cryptography," *Journal of Visual Communication and Image Representation*, vol. 23, no. 8. pp. 1225–1233, 2012, DOI: 10.1016/j.jvcir.2012.08.006.

[62] W.-P. Fang, "Visual cryptography with the extra ability to hide confidential data," *Journal of Electronic Imaging*, vol. 15, no. 2. p. 023020, 2006, DOI: 10.1117/1.2193912.

[63] Y.-J. Huang and J.-D. Chang, "non-expanded visual cryptography scheme with authentication," *2013 International Symposium on Next-Generation Electronics*. 2013, DOI: 10.1109/isne.2013.6512319.

[64] Y.-R. Wang, W.-H. Lin, and L. Yang, "A lossless watermarking using visual cryptography authentication," *2013 International Conference on Machine Learning and Cybernetics*. 2013, DOI: 10.1109/icmlc.2013.6890758.

[65] P. V. Chavan, M. Atique, and L. Malik, "Signature-based authentication using contrast- enhanced hierarchical visual cryptography," *2014 IEEE Students' Conference on Electrical, Electronics and Computer Science*. 2014, DOI: 10.1109/sceecs.2014.6804453.

[66] Y. Maeng, A. Mohaisen, M.-K. Lee, and D. Nyang, "Transaction authentication using complementary colors," *Computers & Security*, vol. 48. pp. 167–181, 2015, DOI: 10.1016/j.cose.2014.10.001.

[67] G. Soman and J. K. John, "Secure digital image sharing using diverse image media," *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*. 2015, DOI: 10.1109/icatcct.2015.7456867.

[68] A. Nandhinipreetha and N. Radha, "Multimodal biometric template authentication of finger vein and signature using visual cryptography," *2016 International Conference on Computer Communication and Informatics (ICCCI)*. 2016, DOI: 10.1109/iccci.2016.7479963.

[69] M. T. Arafin and G. Qu, "Secret Sharing and Multi-user Authentication," *Proceedings of the 26th edition on Great Lakes Symposium on VLSI - GLSVLSI '16*. 2016, DOI: 10.1145/2902961.2903039.

[70] G. D. Dalvi and D. G. Wakde, "Facial images authentication in visual cryptography using sterilization algorithm," *2017 2nd International Conference for Convergence in Technology (I2CT)*. 2017, DOI: 10.1109/i2ct.2017.8226269.

[71] V. A. Daisy, V. Annie Daisy, C. Vijesh Joe, and S. Shinly Swarna Sugi, "An image-based authentication technique using visual cryptography scheme," *2017 International Conference on Inventive Systems and Control (ICISC)*. 2017, DOI: 10.1109/icisc.2017.8068666.

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

[73] C. Xu, J. Zhou, and G. Xiao, "A multisignature scheme for the general access structure," *Proceedings. 2005 International Conference on Communications, Circuits and Systems, 2005.* DOI: 10.1109/icccas.2005.1493368.

[74] H. Zhang, X. Wang, W. Cao, and Y. Huang, "Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding," *Journal of Computers*, vol. 3, no. 12. 2008, DOI: 10.4304/jcp.3.12.68-75.

[75] Y. Wei, P. Zhong, and G. Xiong, "A Multi-Stage Secret Sharing Scheme with General Access Structures," *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*. 2008, DOI: 10.1109/wicom.2008.2939.

[76] S.-Z. Ye, G.-X. Yao, and Q.-L. Guan, "A Multiple Secrets Sharing Scheme with General Access Structure," *2009 International Symposium on Intelligent Ubiquitous Computing and Education*. 2009, DOI: 10.1109/iuce.2009.65.

[77] K.-H. Lee and P.-L. Chiu, "An Extended Visual Cryptography Algorithm for General Access Structures," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1. pp. 219– 229, 2012,

DOI: 10.1109/tifs.2011.2167611.

[78] S. J. Shyu, "Visual Cryptograms of Random Grids for General Access Structures," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 3. pp. 414–424, 2013, DOI: 10.1109/tcsvt.2012.2204940.

[79] Y.-H. Chen, C.-S. Chan, P.-Y. Hsu, and W.-L. Huang, "Tagged visual cryptography with access control," *2014 IEEE International Conference on Multimedia and Expo Workshops (ICMEW)*. 2014, DOI: 10.1109/icmew.2014.6890648.

[80] S. K. Mishra and K. Biswaranjan, "Extended visual cryptography for general access structures using random grids," *2015 International Conference on Advances in Computing, Communications, and Informatics (ICACCI)*. 2015, DOI: 10.1109/icacci.2015.7275899.

[81] S. J. Shyu and M. C. Chen, "Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 9. pp. 1557–1561, 2015, DOI: 10.1109/tcsvt.2015.2389372.

[82] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, "Progressive Visual Secret Sharing for General Access Structure with Multiple Decryptions," *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*. 2016, DOI: 10.1109/itme.2016.0156.

[83] X. Jia, D. Wang, D. Nie, and C. Zhang, "Collaborative Visual Cryptography Schemes," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 5. pp. 1056–1070, 2018, DOI: 10.1109/tcsvt.2016.2631404.

[84] K. Meng, F. Miao, Y. Yu, and C. Lu, "A Universal Secret Sharing Scheme with General Access Structure Based on CRT," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. 2018, DOI: 10.1109/trustcom/bigdatase.2018.00031.

[85] V. J. Katz, *The Mathematics of Egypt, Mesopotamia, China, India, and Islam: A Sourcebook*. Princeton University Press, 2007.

[86] X. Wu and Z.-R. Lai, "Random grid-based color visual cryptography scheme for black and white secret images with general access structures," *Signal Processing: Image Communication*, vol. 75. pp. 100–110, 2019, DOI: 10.1016/j.image.2019.03.017.

[87] A. Jain and S. Soni, "Visual cryptography and image processing based approach for secure transactions in the banking sector," *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)*. 2017, DOI: 10.1109/tel-net.2017.8343545.

[88] S. J. Shyu, "XOR-Based Visual Cryptographic Schemes With Monotonously Increasing and Flawless Reconstruction Properties," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 9. pp. 2397–2401, 2018, DOI: 10.1109/tcsvt.2017.2707923.

[89] M. A. Salama, M. F. M. Mursi, and M. Aly, "Safeguarding images over the insecure channel using master key visual cryptography," *Ain Shams Engineering Journal*, vol. 9, no. 4. pp. 3001–3013, 2018, DOI: 10.1016/j.asej.2018.03.002.

[90] D. Yang, I. Doh, and K. Chae, "Secure medical image-sharing mechanism based on visual cryptography in EHR system," *2018 20th International Conference on Advanced Communication Technology (ICACT)*. 2018, DOI: 10.23919/icact.2018.8323795.

[91] C.-C. Lin and W.-H. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, no. 3. pp. 405–414, 2004, DOI: 10.1016/s0164- 1212(03)00239-5.

[92] G. Abboud, J. Marean, and R. V. Yampolskiy, "Steganography and Visual Cryptography in Computer Forensics," *2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*. 2010, DOI: 10.1109/sadfe.2010.14.

[93] L. Rudraksha and M. N. Giri Prasad, "Advanced Robust Data Hiding Using Visual Cryptography," *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. 2019, DOI: 10.1109/icecct.2019.8868240.

[94] D. van der Linden, D. van der Linden, A. Rashid, E. Williams, and B. Warinschi, "Safe cryptography for all," *Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment - SEAD '18*. 2018, DOI: 10.1145/3194707.3194709.

[95] W. Liu, Y. Xu, M. Zhang, J. Chen, and C.-N. Yang, "A Novel Quantum Visual Secret Sharing Scheme," *IEEE Access*, vol. 7. pp. 114374–114384, 2019, DOI: 10.1109/access.2019.2931073.

[96] C. Zihan, C. Peng, and C. Fangfang, "Research on the Application of Visual Cryptography in Cultural and Creative Artworks," *2019 IEEE 19th International Conference on Communication Technology (ICCT)*. 2019, DOI: 10.1109/icct46805.2019.8947239.

[97] R. Du, E. Lee, and A. Varshney, "Tracking-Tolerant Visual Cryptography," *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. 2019, DOI: 10.1109/vr.2019.8797924.

[98] S.-S. Lee, Y.-J. Huang, and J.-C. Lin, "WEB-VC: Visual Cryptography for Web Image," *2019 IEEE*

International Conference on Image Processing (ICIP). 2019, DOI: 10.1109/icip.2019.8803455.

[99] R. Maurya, A. K. Kannojiya, and B. Rajitha, "An Extended Visual Cryptography Technique for Medical Image Security," *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. 2020, DOI: 10.1109/icimia48430.2020.9074910.

[100] S. S. Rane, K. A. Phansalkar, M. Y. Shinde, and A. Kazi, "Avoiding Phishing Attack on Online Voting System Using Visual Cryptography," *2020 International Conference on Computer Communication and Informatics (ICCCI)*. 2020, DOI: 10.1109/iccci48352.2020.9104071.

Table 1. Results achieved by previous schemes

S. No	AUTHOR & YEAR	RESULTS ACHIEVED BY THESE SCHEMES				
1	Kezheng et al. 2008 S. and	**VISUAL QUALITY OF SECRET IMAGE** ✓		✓	✓	**SECUTIY DURING DATA TRANSFER** **MAINTAINING THE SIZE OF SECRET IMAGE**
2	Loganathan 2011					
3	Han et al. 2013	✓	✓			
4	Mukherjee and Ganguly 2015	✓	✓			
5	Ansari and Shaikh 2016	✓	✓			
6	K. and P. 2015		✓			
7	Shankar and Eswaran 2016		✓			
8	Patel and Srivastava 2016	✓	✓	✓		
9	Ravella and Chavan 2017	✓	✓			
10	Dhiman and Kasana 2018	✓	✓	✓		
11	Chaturvedi et al. 2018	✓				
12	Bhatia et al. 2018	✓	✓			
13	Wu and Yang					
14	Tripathi et al.					

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

2020 ✓ ✓

2020 ✓

2014

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

Table 2. Algorithms, Techniques, and traits of reviewed Schemes.

S.NO.	AUTHOR NAME & Year	ALGORITHMS & TECHNIQUES USED	METRICS
1	Suryadevara et al. 2011	1. 3D database 2. k-out-of-n visual cryptography scheme	Iris
2	Swathi and Madhavi Kumari 2017	1. Watermarking Algorithm 2. Visual Cryptography technique	Iris
3	Judith et al. 2016	1. Asymmetric Algorithm 2. Visual Cryptography	Face and Iris
4	Suganya et al. 2017	1. Permutation algorithm 2. Inverse permutation algorithm 3. Visual Cryptography	Finger Print
5	Madankar et al. 2018	1. Scramble private image 2. Visual cryptography	Face
6	Toli and Preneel 2018	1. Crypto-biometrics for privacy-preserving 2. Pseudo - identities 3. Visual cryptography	Fingerprint
7	Gupta and Sharma 2016	1. 2 x 2 visual cryptography 2. Steganographic 3. QR Code. 4. Two’s complement algorithm of Steganography.	Fingerprint
8	Chutake, Vinay, et al. 2014	1. Minutia Extraction 2. Visual cryptography 3. Matching	Iris
9	Meshram, S.P., & Longadge, R. 2014	1. Random Grid Algorithm Keren's three algorithms	fingerprint and iris templates
10	Rajanwar, Shubhangi et al. 2014	1. Gray Scaling Algorithm	

	2. Floyd Steinberg Error Diffusion 3. Simple Block Replacement (SBR) Algorithm 4. Pattern Match Algorithm Biometric Image		
	Anusree and Binu 2014 Watermarking algorithm Halftoning technique Fingerprint and face	1. Error-diffusion algorithm	
12	Sarika, M.P. 2017 2. Scrambled Image	1. Image decomposition	
13	Rajanwar, Shubhangi et al. 2014 1. Floyd Steinberg Error Diffusion Algorithm 2. Halftone Algorithm 3. Balanced Block Replacement 4. Rescaling algorithm Biometric		
14	Esai Puvanesh, S. et. al 2018 1. Face detection algorithm 2. Visual cryptography	Iris