Major Developments in Visual Cryptography

Surajit Goon

Abstract: ***Visual cryptography is a cryptographic mechanism that gets applied in visual information protection for secured transfer of data. The encryption makes the decryption a mechanical operation.The secret image gets converted into several share images. The share images are distorted/ noisy images which will give the correct image only when placed in the right combination. This paper reviews various visual encryption and decryption mechanism with the safe transmission of information from the literature. This paper about visual cryptography discusses, general access structure, halftone, colour, progressive, region incrementing, extended visual cryptography, colour extended visual cryptography, XOR and OR visual cryptography and the applications of visual cryptography. The applications discussed here are banking security, steganography, crime records, intelligence communication, multilayered Id cards and fingerprint records. The paper provides an overview of advances in VCS where each technique overcomes the problem(s) faced in the other manner.***

Keywords: Visual Cryptography; encryption; decryption; extended visual cryptography.

I. INTRODUCTION

Where third parties are present who identified as adversaries, cryptography is a practice and research method for secure communication. It builds and analyses the protocols that prevent third parties/public from reading private messages. The study of cryptography is inter-disciplinary requiring knowledge on mathematics, computer science, communication, electrical engineering, physics etc. The primary purpose of cryptography is secured data transmission without intersected by third parties. A cryptography operation is performed by a cypher that is a pair of algorithms generating encryption and then decryption for end users. A cryptosystem with the list of items in the order of the finite number of plain text, finite possible ciphertext, limited possible keys and encryption and decryption algorithm which corresponds to each key. A key is essential for both formal and functional operations as cyphers without this can be broken trivially only with the knowledge of the cypher used and are therefore counterproductive for most applications. The cryptosystems get primarily classified as symmetric and asymmetric systems. If both encryption and decryption are using the same key, then the system is symmetrical in nature. An asymmetric system uses variable keys for encryption and decryption of the message. The paper [1] has reviewed the progress in the field of visual cryptography focusing on models, open issues, applications and perspective of cryptography.

The paper [2] gives an introduction to the field of visual cryptography. The paper reviews the basic modelling involved and emerging technologies in cryptography. Visual cryptography is a comparatively new technique wherein the information that requires encryption, is considered a visual image. The visual information is encrypted so that decryption becomes the task of the person to decrypt through sight reading. This paper mainly deals with visual encryption and decryption methods and the latest technology involved in secured transmission using visual cryptography.

For gaining the necessary knowledge in visual cryptography, it is essential to refer [3] for getting the knowledge on fundamentals of cryptography before proceeding further in this article. The book describes the potential for sharing many secrets, VCS based on the reconstruction of encrypted image and decryption of images which includes probabilistic rebuilding or different logical operation for the combination of shared images.

The conceptualisation of visual cryptography was based given in 1994 [4]. In this paper, a cryptographic scheme gets presented for decoding concealed images without cryptographic calculations. The scheme is perfectly secure at the same time easy for implementing. The paper extends it into a visual variant of the *k* out of *n* secret sharing problem, in which n numbers of users are provided one transparency each. Any *k* of them can see the secret image by simply stacking the transparent images shares, but any *k*−1 of them gain no complete information about it

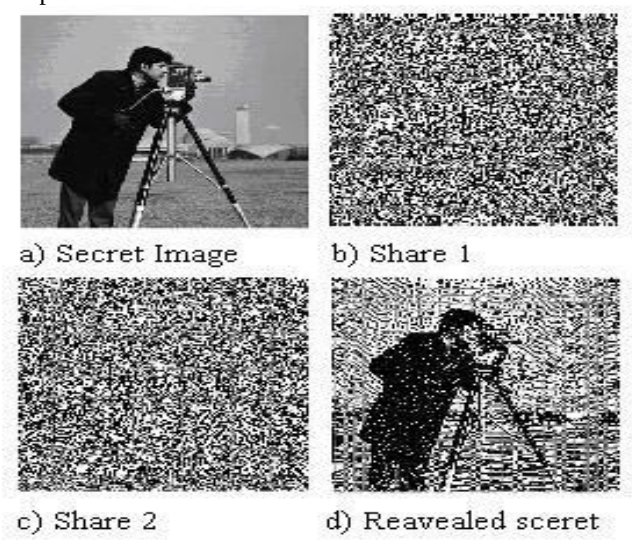


Fig.1.1: Image sharing through visual cryptography [52]

The paper [5] introduces the field briefly, examines numerous prevalent issues in visual cryptography, with the issues like alignment, cheating, flipping, distortion, and thin line. It reviews various types of VCSs like XOR-based and security enriched VCS; shows different methods for presenting colour content using visual cryptographic techniques;

Revised Manuscript Received on December 15, 2019
***** Correspondence Author
Mr. Surajit Goon, Ph.D. Scholar, Brainware University, Kolkata, India.

It also describes some applications of visual cryptography asresolution variant VCS, watermarking and multiple-resolution VCS. The paper [6] reviews the basic models' schemes and security issues of various cryptographic techniques. It concludes that research should progress in solving contrast and security simultaneously.

The book [7] discusses the visual cryptography, various cryptographic schemes and sharing of data. The first chapter deals with traditional visual cryptography which includes size invariant and recursive cryptography and analyses the mathematical background. The second chapter deals with extended visual cryptography which includes half-tone, cheating visual immune schemes and dot-size variant visual cryptography. The third chapter deals with dynamic visual cryptography which discusses multiple screen sharing and embedding shares in the halftone image. The fourth chapter deals with colour visual cryptography and image sharing using random masks. The chapter also deals with evaluating the quality of the image shared. The fifth chapter deals with progressive visual cryptography. The sixth chapter deals with image hatching for visual cryptography and security analysis. The seventh chapter discusses three main applications of visual cryptography they are moire patterns, watermarking and criteria for evaluation purposes.

Uses of Visual Cryptography:

a) Protection using VC:

Whatever the visual encryption created; there is a necessity for the creation of standards for providing legal backing of the schemes. So as per the copyright protection paper [8] provides the scheme for the protection of images from illegal copying by using visual cryptography. Additionally, image processing is made resistant to lossy compression, cropping noise and sharpening images.

The paper [9] proposes a cryptographic watermarking approach to secure the digital image's copyright owner. The watermark pattern does not need to be inserted directly into the original image as it makes it difficult to unlawfully identify and recover from the marked image. The watermarked pattern has great transparency and robustness.

b) Multilayered Id cards and fingerprints:

The paper [41] discusses the use of visual cryptography in multilayered Id Cards and fingerprint security. The techniques of visual cryptography are slightly modified to suit the purpose of their applications. These applications are secured communication system that is used to broadcast one or more secrets.

c) Banking Security:

Design of a biometric system for personal identification that meets the access control criteria for protected areas, ATM access, computer security etc. are used for data and money protection of banking systems. [49] gives a detailed explanation for Security features like biometric identifiers, passwords, PINs are to be communicated in encrypted form to the servers to prevent illegal access a detailed explanation is given in [49].

d) Crime:

The digital library of criminals' biometrics is to keep data safe from unauthorised accesses. The application of VCS enables the safety of the data. The paper [42] Discusses designing anti-phishing websites through visual cryptography by including the authentication process. The paper uses captcha as a password, and then the image is split into two using k-n sharing algorithm. The user receives only one share which contains watermark text for matching purpose other part remains with the server. The paper has proposed this method for website authentication.

e) Intelligence communication:

Intelligence communication between government departments without getting intercepted by the enemies uses visual cryptography.

f) Steganography:

The method of hiding data within another data called as steganography. The hidden data encrypted into another not so important data for making it difficult for the hackers to decode the message. The paper [43] had discussed various applications of visual cryptography. Visual Cryptography is large field of research used in data hiding, image protecting, colour imaging systems, multimedia and other fields of this kind. Visual Cryptography also finds in cybercrime, file formats etc. This paper describes the most important applications of VCS.

The paper [44] had discussed the use of visual cryptography to financial documents. Securing financial records are essential in the competitive world it is often difficult to distinguish digits accurately, making it an unattractive protection technique. VCRYPT uses a threshold technique to overcome the problem and generate a simple, clean, similar document to the original. VC also required huge storage, efficient transmission techniques, so the simple sharing technique to reduce those costs make this a variable alternative for sharing financial documents over the Internet.

II. LITERATURE REVIEW

The origin of visual cryptography is in 1994 developed by Moni Naor and Adi Shamir [4]. The objective of the method is to encrypt the images while transferring through the networks. Over the years various developments have occurred in the field of visual cryptography. Different visual cryptographic schemes designs overcome the shortcomings of the other visual cryptographic schemes(VCS). Various reviews conducted in the past regarding visual cryptography, one such study is [7] Many of the schemes presented work exceptionally well and the current state of the art techniques are beneficial for many applications, such as verification and authentication. The following trends identified within visual cryptography:

1. Contrast improvement.
2. Reducing the size of shares.
3. Increase the range of appropriate images (binary, grey and colour images).
4. Efficiency enhancement.
5. Multiple secret sharing.

The paper [10] summarizes the recent developments in VCS since its beginning and describes the current problems and possible solutions in this field. The paths and patterns for potential VC work with possible VC applications shall also be investigated. A report submitted in the department of computer science from the University of Toronto by J Cai has surveyed various visual cryptography schemes. The report provides the readers with an overview of VCS technology which is already studied [12]. One of the earliest methods of visual cryptography is creating one secret image into into a set of random transparencies which reveals the image when superimposed manually. The sharing of secrets is in such a way that it creates a set of X>=2 secrets into two circle shares; such that none of any particular share leaks the secret and secret is obtained by stacking the first share and rotating second at different angles [13].

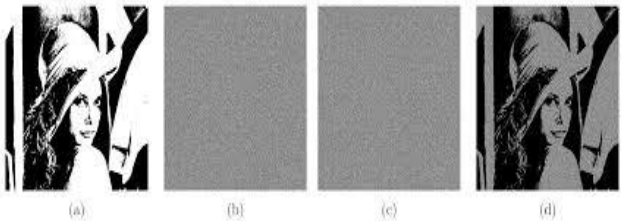
The improvements in VCS are made and are explained below from the most ancient VCS technology to the latest. Different types of visual cryptography are,

i. Gray Scale VCS

A grey scale is an image intensity scaling in which a sample is the value of each pixel, i.e. it only carries information about intensity. Black is the darkest possible shade, which is the total absence of visible or reflected light, and white is the lightest possible shade. This scheme of cryptography technique uses the secret images in the grey scale format.

The paper [14] discusses the basics of a grey scale VCS, and reconstruction/decryption of the image shared and introduced a threshold for VCS. The reconstruction quality improves through pixel expansion. The grayscale VCS has done the decoding process directly by human visual system previously it was restricted to processing binary images, but here different shades of grey are considered.

In the paper [15] a new concept called g grey levels is introduced which ranges from 0 to g-1 for better clarity in black and white imaging. The grey scale VCS is also developed to identify the contrasts of the reconstructed image but reproduces in the form of different scales of grey. The paper also proposed binary secret imaging which allows participants to perform reversing operations.



(a) Original image
(b) image share 1
(c) image share 2
(d) decrypted image

Fig.2.1: Image sharing through grayscale VCS [53]

ii. General Access Structure VCS

A VCS for General Access Structures (GAS) splits the Information into a subset of restricted and forbidden set of participants, wherein only the participants belonging to the qualified set can reveal the information encoded. Different types of VCS based on GAS addressed in this section.

GAS VCS analyzes the structure of VCS and shows the limitations on the size of the shares allocated to all the scheme's participants. The proposed method shows a novel technique for realising k out of n threshold VCS. [39] Provides a novel method for realising k out of n VCS which is better than the method proposed by *M.Naor & A. Shamir.*

Given below is the diagrammatical explanation for the image encryption and decoding process.

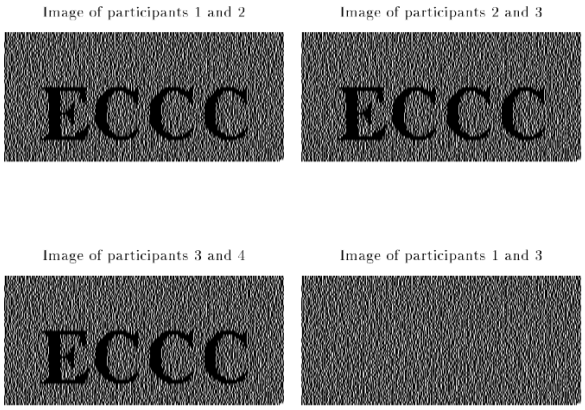


Figure 2.2: a diagrammatical explanation for visual cryptography [39]

iii. Halftone VCS

. The halftone VCS discussed in [16]. It introduces the concept of Halftone where the colours are toned down to reduce the pixel sizing. If the grey levels are reduced by two, the image that appears does not have a much spatial resolution to describe the details. Dithering is the process of creating illusions of the colour that are not present. The random pixel arrangement does it. The Floyd Steinberg dithering is a method for colour correction. The dithering gets performed through error diffusion which means that it pushes the quantisation error of a pixel into the neighbouring pixel to deal with it later. The dithered effect is creating a check board pattern when the original pixel values are exactly halfway between the nearest available colours. For example, as a black-and-white check board pattern, 50% grey data could be dithered. For optimum dithering the quantification error count should be precise enough to prevent rounding errors affecting the results.

The concept of blue noise dithering used for the proposed method use the void and cluster algorithm to transform a hidden binary image into common images with substantial visual information in n halftone. It expands the pixel size hence the area of the image gets enlarged in the visual cryptography by the addition of halftoning techniques, a secret image encoded into halftone shares taking meaningful visual information. The hidden image gets embedded as binary valued shares while the shares get halftoned. The advantage of error diffusion is that that it has low complexity and halftone shares have excellent image quality. Other dithering techniques used for Halftone VCS are Floyd, Jarvis. Shared image quality and the contrast of the reconstructed image discussed in [17].

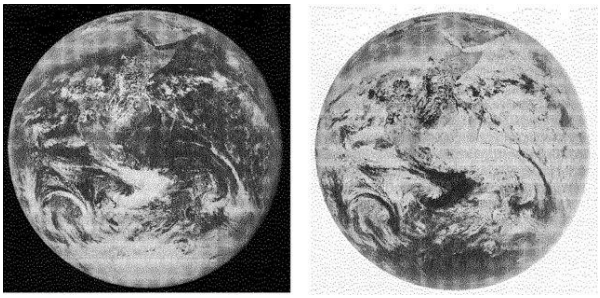


Fig 2.3: Image sharing through Halftone VCS [16]
i. Sent image ii. Received image

The above figure represents the original image on the left and complimentary Halftone VC scheme decrypted image. The decrypted image contrast is precisely opposite to the original. Why the image pixel colours have changed is explained below through a diagram.

Pixel	White		Black	
Prob.	50%	50%	50%	50%
Share 1				
Share 2				
Stack share 1 & 2				

Fig 2.4: Working of halftone VCS [6]

From the above image, it shows that this method is incapable of giving the replica of the shared image.

iv. Color VCS

The paper [48] has created a colour visual cryptography where the encryption performed through an XOR operation. Monochromatic images get converted to binary images. Such binary images are encrypted using a binary image, which is called as share-1 to get binary cypher images. Binary key image and three half-tones of the dark colour image encrypted separately using Exclusive OR process. The shares are decrypted in the source side, then the retrieved binary image are halftoned in reverse and then combined to get the original image.

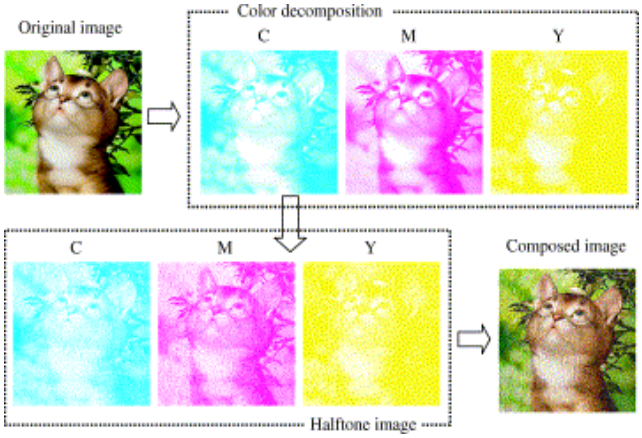


Fig.2.5: Color Visual cryptography [51]

The above image have got split into three shares namely cyan, magenta and yellow. When all the three images when stacked in the correct order, it gives the original colour image from the encrypted image. All the shares get halftoned for reducing the size.

v. Progressive VCS

Progressive Visual Cryptography (PVC) is different from regular VC concerning decoding. In PVC, with the amount of stacked shares, visibility and contrast of the decoded hidden image is gradually increased. Another variant of progressive VCS is the progressive colour VCS. [25] Discusses progressive colour VCS which can be used both in colour and grayscale images. Three different types of descriptions enable the recovery of the traditional visual cryptography. An enhanced stacking technique to decrypt into a halftone image.

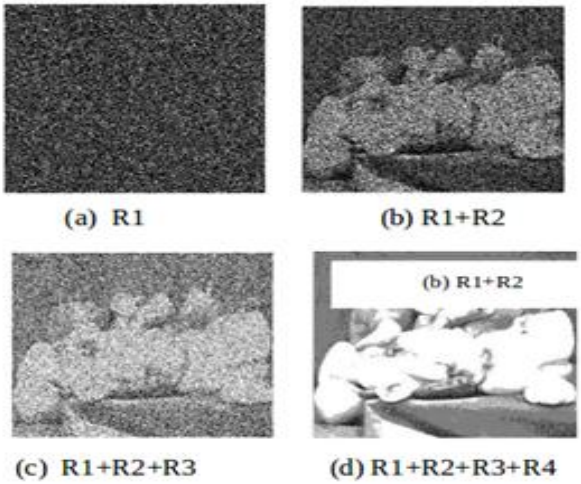


Fig 2.6: Greyscale images of red which is under progressive construction [52]

Similar to red colour, green colour image and blue colour image also get developed in grey scales

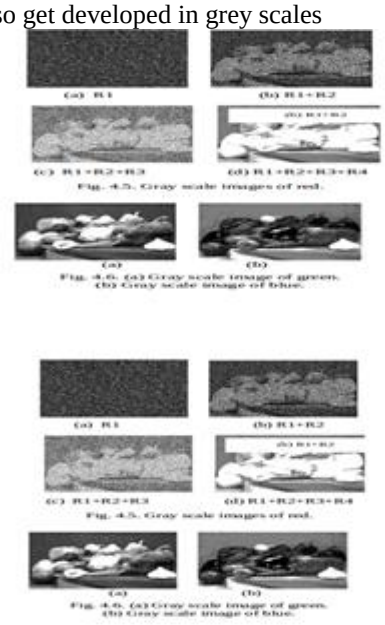


Fig 2.8 Greyscale image of blue [52]

Fig 2.7: the Greyscale image of green[52]

Fig 2.9 Reconstructed Image [52]

Another paper presents on progressive VCS which can be utilised to decode the secret image where a few pieces of the image would provide an overview of the secret image and by increasing the number of stacked shares, the specifics of the hidden information would be slowly exposed. The paper then compares it with the pixel expansion methods and claims that the pixel expansion is relatively poor quality. [26] The paper suggested a new radical VC distribution of PVC for the development of pixel-unexpanded shares. No one can obtain any hidden information with just a single share. Superimposition of shares rise the contrast to (n-1)/n which is better than traditional ways.

vi. Region incrementing VCS

Region Incrementing Visual cryptography for sharing visual secrets of multiple secrecy levels in a single image. In this scheme, different regions made of a single image, based on the secrecy level, and different encoding rules get applied to these regions. Various research discussed RIVC. [21] has examined region incrementing VCS in which proposed an n-level RIVC scheme, the content is divided into several regions associated with n hidden levels and encoded into n+1 shares with the features given below,

(i) each share cannot obtain the secrets.

(ii) any t shares can be used to reveal t-1 levels of secrets.

(iii) the number and location of not-yet-revealed secrets are unknown to users.

(iv) all secret information in S gets revealed when all of the n+1 shares are available.

(v) secrets are known by visual inspection without the measurement of correctly stacked shares.

A novel method called Region in Region Incrementing VCS enhances region incrementing VCS. The proposed method is including a new layer of secrecy enhancement for region incrementing VCS. The advantage of this method is the recommended method has more area to hide the secret image than the non-overlapping regions in Region Incrementing VCS. The paper [22] proposed this method.

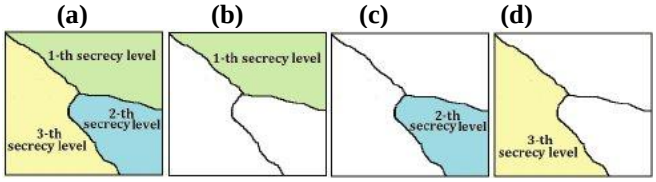


Fig 2.10 A partition of three secrecy level regions for the (2, 4)-RIVCS:
(a) three levels of secrecy-level decomposition (b) the area exposed when two shadows are stacked (c) the region revealed by stacking three shadows (d) the region revealed by stacking four shadows. [22]

vii. Extended Visual cryptography

Extended Visual Cryptography Scheme (EVCS) is similar to the traditional VCS, but this technique has significant shares. Another method of steganography is EVCS. Recent research in this domain of cryptography gets explained in this section. In the paper [27] digital watermarking technique is used in order to generate large number of shares. Before being published, the hidden shares are watermarked with different cover images. The cover images that get extracted from the shares are stacked one by one, slowly exposing the secret image. The revelation of images is gradually done by extraction from the shares. High security, high contrast of the recovered image are advantages of this scheme.

The paper [28] proposes a method for halftone image processing to improve the quality of shared images and recover the image similar to the original halftone secret image. The paper [29] proposes a trade-off between the contrast of the restored image on each transparency and the contrast of the image.

This scheme ensures that hackers cannot discern any hints from individual cover images about the secret image. Hence the researchers have made some technique for the colour image visual cryptography. The paper [18] Discusses the image sharing without arousing the attention of hackers utilising the halftone technique, cover the coding table and secret coding table to generate two significant shares together. The paper also discusses hiding the secret image into two or more images called shares which are meaningful hence does not create curiosity for hackers. The scheme utilises halftone technique, cover the coding table with the secret coding table for generating shares. The secret gets decrypted by stacking the significant shares. [19] has utilised a method called chaotic, random number, where the encryption is done based on sieving, division, chaotic random based shuffle share. The random numbering is previously used in [20] where an arbitrary threshold grid based VSS scheme aiming at improving the visual quality gets analysed and the differences between related approaches discussed. Paper [23] has claimed that it neither needs cryptographic knowledge nor needs complex computation to decrypt, but at the same time, hackers cannot access the image. The paper has proposed that advantages of black and white VCS get retained by exploiting the human visual system to decrypt the secret images without computation and also backward compatibility with previous results.

Different types of extended visual cryptography explained below,

(a) Colour extended visual cryptography

The paper [30] discusses encrypting secret messages into colour halftone image shares. The paper aims for proving the superiority of colour extended visual cryptography over the other methods of encryption. Past methods in the literature show good results for VC schemes in black and white or grey scale, but nevertheless, they are not enough to be applied directly to colour shares because of different colour structures.

Some of the methods available for VC are unsatisfactory in terms of either generating meaningless shares or significant shares of poor visual quality resulting in suspicion of encryption. The paper presents the visual information pixel (VIP) synchronisation and error diffusion to attain a colour visual cryptography encryption method which produces significant colour shares with high visual quality. VIP synchronisation retains the pixels position carries visual information of original images throughout the colour channels & error diffusion generates shares that are pleasant to human eyes. Comparing this method with previous approaches show that the performance of the new method is better than previous plans.

(b)Embedded Extended Visual cryptography

This method proposed in [50] defines and shows the different visual quality shares metrics and that are MAX ERROR VALUE, PSNR VALUE and MEAN SQUARE value by taking more than one secret and input image and these values are calculated between each segment. This scheme ensures that the hidden image can be visually observed by stacking or overlaying the subset of shares.

This paper analyses the results using different visual quality shares' metrics like PSNR, MSE, MAX ERROR by taking more than one secret and input image and these values are calculated between each segment and a here also a user-defined matrix dimension is also defined to compute halftoning.

viii. XOR and OR and other VCS

Various VCS that uses XOR, OR, etc. with different types of approaches and operations gets discussed in this section. The paper [31] Discusses XOR based visual cryptography where XOR operation used for decoding to improve the contrast in the colours. The paper examines the relation between XOR based VCS and OR-based VCS. Also, the article proves that base matrices of (k,n) -OVCS can be used in (k,n)-XVCS, resulting in enhancement of contrast by 2^(k-1) times. The other schemes are as pointed out in [32]. The scheme is method encryption uses sub pixels for imaging. The sub pixels display same colour of its pixel. There is an improvement from the previously known best constructions considering the pixel expansion. VCS based on the polarisation of light has excellent resolution, contrast and colour properties. XOR operation describes it. The paper [33] investigates threshold visual secrets-sharing system associated with XOR based VC schemes. The scheme has much better resolution than OR-based VC schemes. XOR-based k-out-of-n schemes for even k are fundamentally different from those of odd k.

The paper [34] addresses VC algorithms based on XOR for general access structure and adaptive region incrementing XOR based VC. This paper reviews the visual cryptography schemes and their performance. Two XORs-based VC is proposed in [35] to solve the problem of low visual quality without darkening the background in VC. In addition to XOR based VCS capabilities, an extended ability is proposed to extract the maximum from the VCS. The paper uses two algorithms here; the first algorithm is used to implement complex sharing strategy using GAS without affecting the merits. The use of the second algorithm is for adaptive security is where the security levels get recovered following the qualified sets instead of the quality.

Size invariant VCS is another type of visual secret sharing scheme proposed; the secret image gets encoded into shares, where the shares size is larger than that of the original image, and the shares get decoded by stacking without performing the cryptographic computation. The paper [36] discusses one such scheme to encode the black and white image to same size shares of the secret image. The reconstructed image of the proposed scheme gets compared with the conventional scheme. On contrast VCS is another type of VCS scheme is also used to encode and decode data, the difference between this and other schemes is that it goes for the minimum pixel expansion and contrast of the image gets optimised. The paper [37] discusses contrast optimisation, and the contrast of the image get analysed in k out of n threshold schemes. Here the paper takes the value of k=2.

Multi-secret VCS is another type of VCS in [38] is proposed and discusses the condition when more than one image is to be encrypted. The paper addresses the security and contrast issues together. [39] Study of the composition of the visual cryptography schemes and proof of the size of the schemes allocated to the scheme's participants. It offers a novel technique to render k out of n threshold visual cryptography schemes. The proposed construction for k out of n visual cryptography schemes is better in terms of expansion of pixels than the expected one.

III. PERFORMANCE ANALYSIS OF VARIOUS CRYPTOGRAPHIC SCHEMES

Only because the performance of visual cryptography is reliable, the methodology gets used in the encryption of data in the above said examples, which are extremely critical of the data security. The performance of cryptographic schemes gets analysed in [45]. The analysis results show that asymmetric key encryption has high encryption ratio, while Triple DES has average encryption ratio and RC4 has low encryption ratio, and the remaining symmetric key encryption has high encryption ratio.

The paper [34] analyses the performance of XOR-based cryptography has been exploited and two variants of XOR-based cryptography gets introduced namely XOR-based VC for GAS and adaptive region incrementing XOR based VC. The paper further concludes that complicated sharing strategy by using General Access Structure (GAS) implemented in XOR based VC for GAS. [46] Proposed a method to give the algorithm that is ranked as per the visual cryptography standards and the capabilities to understand the implementation method to evaluate the algorithm development and provide image reconstruction information. The paper presents a good discussion on visual cryptography algorithms.

The review shows that visual cryptography has been useful in data encryption especially in the field of image processing and has evolved and has improved the image transfer quality by innovative methods.

It has also shown through the applications, the use of visual cryptography can get applied in our daily basis for various requirements which proves that visual cryptography is a reliable method of implementation of network and data security. Another review is presented in [11] which tabulates various authors contributions which have created milestones in the field of visual cryptography. The tabulation created considering the image format, pixel expansion, the number of secret images and types of shares generated.

Biometric authentications give the security enhancement of visual cryptography. One such authentication used is Iris mentioned in [47] where different approaches adopted by researchers to secure the raw biometric data and template in the database discussed in this paper. The method proposed is to store iris template securely in the database using visual cryptography. Iris should get matched for authentication, but the problem with this system is the iris authentication speed is slow.

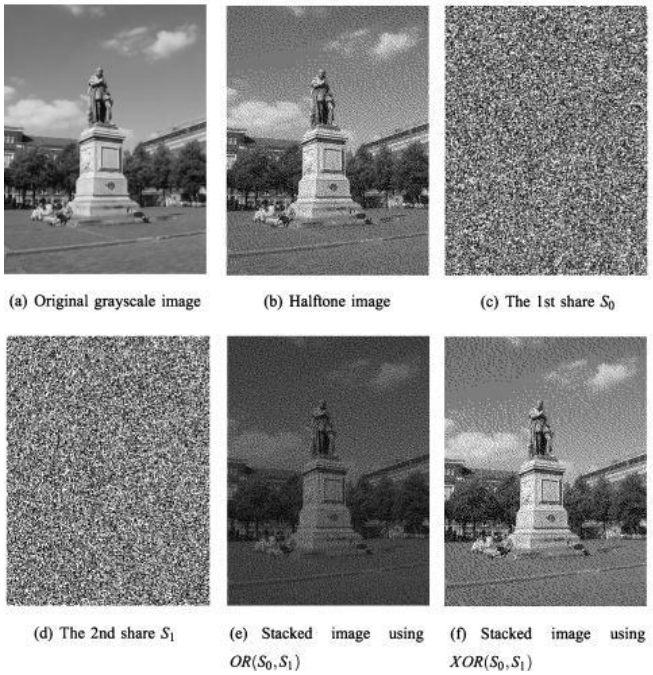


Fig. 3.1 Comparison of Greyscale cryptography with Half-tone, OR and XOR [25]

The comparisons of visual cryptography techniques and image recovery get carried out through manually comparing images. A sample image that gets shown in Fig 3.1 shows the difference in the images for comparison. The comparison is between XOR, grayscale and Halftone images.

IV. CONCLUSION

This paper discussed the various technologies in cryptography and addressed their setbacks and advantages. Each technique gets determined according to the required specification concerning the parameters used. Also, the paper presents the study of comparative analysis of all types of visual cryptography with advantages. This research study serves as a beneficial knowledge for future research direction. The visual cryptography can only protect from the interception of data flow but does not protect data from snooping. Snooping can access data directly on to the nodes. But the encryption is done while transmitting data only. So, the visual cryptography could get extended to the protection of nodes.

REFERENCES

1. D'Arco, Paolo, Roberto De Prisco, and Yvo Desmedt. "Private visual share-homomorphic computation and randomness reduction in visual cryptography." In International Conference on Information Theoretic Security, Springer, Cham, pp. 95-113, 2016.
2. Sandhya .N, Jyothi R. "A brief introduction to visual cryptography". International Journal of engineering research and Technology (IJERT) Vol. 3, Issue 3, 2488-2491, 2014
3. Cimato S, Yang C.N, "Visual Cryptography and secret image sharing", CRC press 1st Edition, 2017.
4. Naor, M., A. Shamir. "Visual cryptography. Advances in CryptologyEUROCRYPT'94 Lecture Notes in Computer Science." In Workshop on the Theory and Application of Cryptographic Techniques, May 9C12, pp. 1-12. 1995.
5. Liu, F., Yan, W. Q. "Visual Cryptography for Image Processing and Security" Vol. 2. New York: Springer, 2014
6. Chandramathi S, Ramesh Kumar R, Suresh R, Harish S "An overview of visual cryptography" International Journal of Computational Intelligence Techniques, Vol 1 Issue 1, pp32-37, 2010.
7. Weir, J. P. Visual cryptography and its applications. Bookboon, 2012.
8. Lou, Der-Chyuan, Hao-Kuan Tso, and Jiang-Lung Liu. "A copyright protection scheme for digital images using visual cryptography technique." Computer Standards & Interfaces Vol. 29, no. 1 pp.125-131, 2007.
9. Hwang, Ren-Junn. "A digital image copyright protection scheme based on visual cryptography." 淡江理工學刊 Vol. 3, no. 2, pp 97-106, 2000.
10. Weir, Jonathan, and WeiQi Yan. "A comprehensive study of visual cryptography." Transactions on data hiding and multimedia security V, Springer, Berlin, Heidelberg, vol. 5 pp. 70-105 2010.
11. Revenkar, Pravin S., Anisa Anjum, and W. Z. Gandhare. "Survey of visual cryptography schemes." International Journal of Security and Its Applications Vol 4, no. 2 pp49-56, 2010.
12. Cai J. A short survey on visual cryptography schemes. Department of Computer Science, University of Toronto. 2004.
13. Shyu, Shyong Jian, Shih-Yu Huang, Yeuan-Kuen Lee, Ran-Zan Wang, and Kun Chen. "Sharing multiple secrets in visual cryptography." Pattern Recognition Vol. 40, no. 12 pp.3633-3651, 2007
14. Blundo, Carlo, Annalisa De Bonis, and Alfredo De Santis. "Improved schemes for visual cryptography." Designs, Codes and Cryptography Vol. 24, no. 3 pp. 255-278, 2001.
15. Blundo, Carlo, Alfredo De Santis, and Moni Naor. "Visual cryptography for grey level images." Information Processing Letters 2000 Vol. 75, no. 6 255-259, 2000.
16. Zhou Zhi, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography." IEEE transactions on image processing 15, no. 8, 2441-2453, 2006.
17. Wang, Zhongmin, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography via error diffusion." IEEE transactions on information forensics and security 4, no. 3, pp383-396, 2009.
18. Wu, Hsien-Chu, Hao-Cheng Wang, and Rui-Wen Yu. "Color visual cryptography scheme using meaningful shares." IEEE Eighth International Conference on Intelligent Systems Design and Applications, ISDA'08, vol. 3, pp. 173-178, 2008.
19. Krishna, Murali, and M. Jaya Ram. "Chaotic Based Enhanced Keyless Color Image Visual Cryptography System." Journal of Innovation in Computer Science and Engineering Vol. 6, no. 1 pp. 26-28, 2016.
20. Yan, Xuehu, Xin Liu, and Ching-Nung Yang. "An enhanced threshold visual secret sharing based on random grids." Journal of Real-Time Image Processing 14, no. 1 pp.61-73, 2018
21. Wang, Ran-Zan. "Region incrementing visual cryptography." IEEE Signal Processing Letters 16, no. 8 pp. 659-662, 2009.
22. Yang, Ching-Nung, Yi-Chin Lin, and Chih-Cheng Wu. "Region-in-Region incrementing visual cryptography scheme." In The International Workshop on Digital Forensics and Watermarking 2012, pp. 449-463. Springer, Berlin, Heidelberg, 2013.
23. Hou, Young-Chang. "Visual cryptography for color images." Pattern recognition 36, no. 7 (2003): 1619-1629.
24. Jin, Duo, Weiqi Yan, and Mohan S. Kankanhalli. "Progressive color visual cryptography." Journal of Electronic Imaging 14, no. 3 (2005): 033019.

25. Hou, Young-Chang, and Zen-Yu Quan. "Progressive visual cryptography with unexpanded shares." IEEE transactions on circuits and systems for video technology 21, no. 11 (2011): 1760-1764.
26. Jithi, P. V., and Anitha T. Nair. "Progressive Visual Cryptography with watermarking for meaningful shares." In Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on, pp. 394-401. IEEE, 2013.
27. Askari, Nazanin, Howard M. Heys, and C. R. Moloney. "An extended visual cryptography scheme without pixel expansion for halftone images." In Electrical and Computer Engineering (CCECE), 2013 26th Annual IEEE Canadian Conference on, pp. 1-6. IEEE, 2013.
28. Ateniese, Giuseppe, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. "Extended capabilities for visual cryptography." Theoretical Computer Science 250, no. 1-2 (2001): 143-161.
29. Kang, InKoo, Gonzalo R. Arce, and Heung-Kyu Lee. "Color extended visual cryptography using error diffusion." IEEE Transactions on image processing 20, no. 1 (2011): 132-145.
30. Yang, Ching-Nung, and Dao-Shun Wang. "Property analysis of XOR-based visual cryptography." IEEE transactions on circuits and systems for video technology 24, no. 2 (2014): 189-197.
31. Blundo, Carlo, Annalisa De Bonis, and Alfredo De Santis. "Improved schemes for visual cryptography." Designs, Codes and Cryptography 24, no. 3 (2001): 255-278.
32. Tuyls, Pim, Henk DL Hollmann, Jack H. Van Lint, and L. M. G. M. Tolhuizen. "XOR-based visual cryptography schemes." Designs, Codes and Cryptography 37, no. 1 (2005): 169-186.
33. Soman N, Baby S "XOR based Visual cryptography". International Journal on cybernetics and informatics (IJCI) 5, no. 2 (2016): 253-264
34. Wu, Xiaotian, and Wei Sun. "Extended capabilities for XOR-based visual cryptography." IEEE Transactions on Information Forensics and Security 9, no. 10 (2014): 1592-1605.
35. Ito, Ryo, Hidenori Kuwakado, and Hatsukazu Tanaka. "Image size invariant visual cryptography." IEICE transactions on fundamentals of electronics, communications and computer sciences 82, no. 10 (1999): 2172-2177.
36. Blundo, Carlo, Alfredo De Santis, and Douglas R. Stinson. "On the contrast in visual cryptography schemes." Journal of Cryptology 12, no. 4 (1999): 261-289.
37. Yang, Ching-Nung, and Ting-Hao Chung. "A general multi-secret visual cryptography scheme." Optics Communications283, no. 24 (2010): 4949-4962.
38. Ateniese, Giuseppe, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. "Visual cryptography for general access structures." Information and Computation 129, no. 2 (1996): 86-106.
39. Bludno, C., De Santis, A., Stinson, D. R., and Vaccaro, U. (1995),Graph decomposition and secret sharing schemes,J.Cryptol.8, 39-64.
40. Yengisetty, Subba Rao V., and Bimal K. Roy. "Applications of visual cryptography." International Journal of Parallel, Emergent and Distributed Systems 26, no. 5 (2011): 429-442.
41. Manasi Ashokrao Deshmukh, R.V. Deshpande "Anti-phishing website using visual cryptography" International Journal of Innovative Research in Computer and Communication Engineering, 5 no. 7,(2017): 13385-13393
42. Pandey, Anjney, and Subhranil Som. "Applications and usage of visual cryptography: A review." In Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), 2016 5th International Conference on, pp. 375-381. IEEE, 2016.
43. Hawkes, L., Alec Yasinsac, and C. Cline. "An application of visual cryptography to financial documents." Florida State University, Florida (2000): 1-7.
44. Jeeva, A. L., Dr V. Palanisamy, and K. Kanagaram. "Comparative analysis of performance efficiency and security measures of some encryption algorithms." International Journal of Engineering Research and Applications (IJERA) 2, no. 3 (2012): 3033-3037.
45. Walden, Disa. "A Benchmarking assessment of known visual cryptography algorithms." (2012).
46. Revenkar, P. S., Anisa Anjum, and W. Z. Gandhare. "Secure iris authentication using visual cryptography." arXiv preprint arXiv:1004.1748 (2010).
47. Krishnan, Gopi S., and D. Loganathan. "Color image cryptography scheme based on visual cryptography." In Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on, pp. 404-407. IEEE, 2011.
48. Chandrasekhara, and Jagadeesha "Secure Banking Applications using visual cryptography against fake website authenticity theft." International Journal of advanced computer engineering and communication technology, 2 no. 2 (2013):1-5.
49. Navjot Kaur & Dr Rajiv Mahajan "An enhanced embedded, extended visual cryptography scheme" International Journal of Software & Hardware Research in Engineering, 2 no. 5, (2014): 120-122.
50. Isha Padiya, Vinod Manure, Ashok Vidhate Visual "secret sharing scheme using encrypting multiple images" International Journal of advanced research in Electrical, Electronics and Instrumentation Engineering 4 no. 1, (2015): 132-137
51. Fersne, Athira "Progressive visual Cryptography scheme without pixel expansion for colour images" International journal of advanced research in computer and communication engineering 4 no 6 (2015): 186-191