JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SIGNIFICANT DEVELOPMENTS IN VISUAL CRYPTOGRAPHY

[1]Mrs. Uzma Khan,[2]Dr. Ankit Temurnikar,[3]Dr. Sunil Patidaar

[1]Research Scholar,[2]Assistant Professor,[3]Assistant Professor
[1]Department of Computer Science,
[1]Madhyanchal Professional University, Bhopal ,India

Abstract : Visual information protection uses visual cryptography as a cryptographic approach for data transfer security. Because of the encryption, decryption is a mechanical process. Several sharing images are created using the secret image. The photos that are shared are blurry or noisy, and they only produce the right image when they are combined in the right way. To ensure the secure transmission of information, this study includes multiple visual encryption and decryption methods. General Access Texture, halftone, Color, Progressive, Incremental Area, Advanced ViewEncryption, color-enhanced visual encryption, visual XOR and OR encryption, and visual encryption applications are covered in this visual encryption article. Applications like banking security, steganography, criminal records, intelligence communication, multilayered ID cards, and fingerprint records are covered in this article.The paper gives a summary of developments in VCS, where each technique addresses a different set of issues.

IndexTerms **- Visual Cryptography; encryption; decryption; extended visual cryptography.**

I. INTRODUCTION

Encryption is a research and practice method for secure communication in the presence of third parties identified as adversaries.It creates and evaluates the protocols that keep the public and other parties from seeing private messages. The study of cryptography is interdisciplinary and calls for expertise in a variety of fields, including physics, electrical engineering, computer science, communication, and mathematics. Secure data transfer without interference from outside parties is the main goal of cryptography. A cipher, which consists of two algorithms that provide encryption and later decryption for end users, performs a cryptographic operation. a cryptosystem having a list of components arranged in the following order: a finite number of plain texts, a finite number of possible cipher texts, a finite number of keys, and an encryption and decryption algorithm for each key. For both formal and functional operations, a key is necessary because ciphers without one are useless for the majority of applications because they can be easily cracked given the knowledge of the cipher that was used. The two main categories used to categories cryptosystems are symmetric and asymmetric systems. The system is symmetrical if the same key is used for both encryption and decryption. Variable keys are used in an asymmetric system to encrypt and decrypt messages. The publication [1] examined the developments in the area of visual cryptography with an emphasis on models, unresolved problems, applications, and a cryptographic approach.

The publication [2] provides an overview of the visual cryptography subject. The study examines upcoming technology in cryptography as well as the fundamental modeling involved. A relatively recent method of encryption called visual cryptography treats the information that needs to be encrypted as a visual representation. The visual information is encrypted, making it up to the person using sight reading to decrypt it. This study focuses on the most recent developments in safe transmission utilizing visual cryptography, including methods for visual encryption and decryption.

Before continuing with this article, it is important to refer to [3] to learn about the principles of cryptography in order to get the information required for visual cryptography. In the book, the potential for sharing many secrets is discussed, along with a virtual computer system (VCS) based on the reconstruction of encrypted images and decryption of images that incorporates probabilistic rebuilding or different logical operations for the combination of shared images.

In 1994 [4], a conceptualization of visual cryptography was made. In this research, a cryptographic method for decoding hidden images without performing cryptographic calculations is given. The implementation of the technique is simple and completely secure. The k out of n secret sharing problem is expanded into a visual variation in the paper, where n numbers of users are each given one transparency. By simply stacking the transparent image shares, any k of them can view the hidden image, but any k-1 of them does not learn everything there is to know about it.

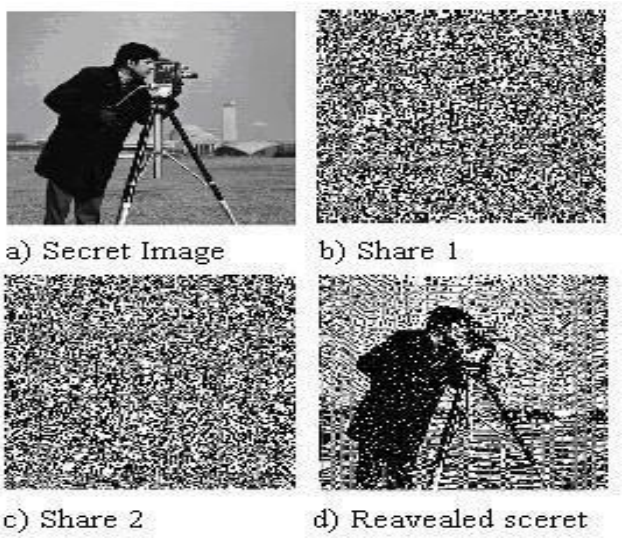

Fig.1.1: Sharing pictures with visual cryptography [52]

The study [5] provides a brief overview of the subject and investigates a number of frequently occurring problems in visual cryptography, including alignment, cheating, flipping, distortion, and thin lines. It reviews numerous VCSs, such as XOR-based and security-enhanced VCS, and demonstrates various ways to convey colored textutilizing visual cryptographic approaches.

Additionally, it outlines some uses for visual cryptography, like as watermarking, numerous resolutions, and resolution variant VCS. The article [6] examines the security concerns and basic model methods of several cryptography algorithms. It is concluded that research should move further while concurrently addressing contrast and security.

The book [7] covers data communication, a variety of encryption methods, and visual cryptography. The size invariant and recursive cryptography discussed in the first chapter's examination of the mathematical underpinnings of conventional visual cryptography.The second chapter covers expanded visual cryptography, which includes dot-size variation visual cryptography, cheating visual immune systems, and half-tone. The third chapter, which is about dynamic visual cryptography, covers sharing across several screens and embedding shares in halftone images.The fourth chapter discusses image sharing using random masks and color visual cryptography. The chapter also covers determining the image's quality before sharing it. The topic of progressive visual cryptography is covered in chapter 5. The sixth chapter discusses picture hatching for security analysis and visual cryptography.Moire patterns, watermarking, and assessment criteria are the three main applications of visual cryptography that are covered in the seventh chapter.

Visual cryptography applications:

a) Protection utilizing VC:

Standards must be developed in order to give the schemes legal support, regardless of the visual encryption that is developed. Therefore, in accordance with the copyright protection article [8], a technique is provided for the protection of images against unauthorized reproduction utilizing visual cryptography. Additionally, noise cropping, lossy compression, and image sharpening are all resistant to image processing.

The paper [9] suggests using cryptographic watermarking to secure the copyright owner of the digital image. Since it is difficult to recognize and recover from the marked image without authorization, the watermark pattern does not have to be directly incorporated into the original image. The watermarked design is very transparent and durable.

b)Multilayered Id cards and fingerprints:

The application of visual cryptography in the security of multilayered identification cards and fingerprints is covered in the work [41]. For the purposes of their applications, visual cryptography techniques are somewhat changed. To broadcast one or more secrets, these applications function as secure communication systems.

a) BankingSecurity:

The design of a biometric personal identification system that complies with standards for ATM access, information security, and access control to sensitive areas is used to safeguard the assets and data of financial institutions. After [49], which provides a thorough description, security components, including biometric IDs, passwords, and PINs, must be provided to servers in encrypted form to prevent unauthorized access.

b) Crime:

The biometric digital library of offenders is used to protect data from unauthorized access. Data security is made possible by the use of VCS. The paper [42] discusses using visual cryptography to develop anti-phishing websites that incorporate the authentication procedure. The image is split into two using the k-n sharing technique after the paper utilizes captcha as a password. Only one share, containing watermark text for matching purposes, is sent to the user; the rest stays on the server. This solution for website authentication has been suggested in the study.

c) Intelligence communication:

Visual cryptography is used to protect government departments' intelligence communications from enemy interception.

d) Steganography:

Steganography is a way for encrypting data such that it cannot be seen by humans. To make it difficult for hackers to decrypt the transmission, the concealed data is encrypted into other less crucial data. The paper [43] had covered a number of visual cryptography applications. Visual cryptography is a significant area of study that is employed in multimedia, color imaging

systems, multimedia, data concealment, and image protection, among other similar topics. Visual cryptography is used in file formats, cybercrime, and other areas. The main uses of VCS are discussed in this paper.

The use of visual cryptography for financial documents was covered in the study [44]. In the competitive world, protecting financial information is crucial, but it can be challenging to discern digits precisely, making it an undesirable protection method. To get around the issue and produce a straightforward, orderly document that is comparable to the original, VCRYPT employs a threshold method. The straightforward sharing strategy to cut those charges makes this a flexible choice for sharing financial information over the Internet. VC also required enormous storage and effective transmission systems.

II. LITERATUREREVIEW

In 1994, Moni Naor and Adi Shamir invented visual cryptography for the first time [4]. The technique's objective is to encrypt images as they travel over networks.Numerous advancements have been made in the field of visual cryptography over the years. Different approaches for visual cryptography schemes address the drawbacks of existing visual cryptographic schemes (VCS). There have been several reviews of visual cryptography in the past; one such research is [7]. Numerous described approaches perform remarkably well, and many applications, including verification and authentication, benefit from the state-of-the-art methodologies. The following developments in visual cryptography were noted:

1. Improve contrast.
2. Scaling back sharing sizes.
3. Expand the selection of suitable photographs (binary, grey and color images).
4. Improvement of effectiveness.
5. Sharing numerous secrets.

The study [10] addresses the present issues and potential solutions in this sector as well as the most recent advancements in VCS since its inception. Investigations must be done into the routes and patterns for potential VC work with potential VC applications. A report on several visual cryptography techniques was submitted to the department of computer science at the University of Toronto by J Cai. The report gives readers an overview of the already-researched VCS technology [12]. One of the first techniques for visual cryptography involves turning a single secret image into a collection of arbitrary transparencies, which when manually overlapped expose the image.The secret is obtained by stacking the first share and rotating the second share at various angles. This method of sharing secrets results in a collection of X>=2 secrets that are divided into two circular shares.

From the oldest VCS technology to the most recent, the advancements in VCS are described below. Several forms of visual cryptography include:

i. Gray Scale VCS

A grey scale is a picture intensity scaling in which each pixel's value serves as a sample, therefore containing just information about intensity. White is the lightest color imaginable, whereas black, the darkest shade imaginable, represents the absolute absence of visible or reflected light. Secret photos in grayscale format are used in this cryptography approach.

The study [14] covers the fundamentals of a grey scale VCS, as well as the reconstruction/decryption of the shared image and the introduction of a VCS threshold. The increase of pixels enhances the reconstruction quality. In the past, the human visual system has directly done the decoding of grayscale images, but this system could only handle binary images.

The study [15] introduces a novel concept known as g grey levels, which span from 0 to g-1 for improved clarity in black and white imaging. The contrasts in the reconstructed image are likewise recognized by the grey scale VCS, but it does so by simulating the contrasts in multiple grey scales.The article also suggested binary secret imaging, which enables users to conduct actions in reverse.

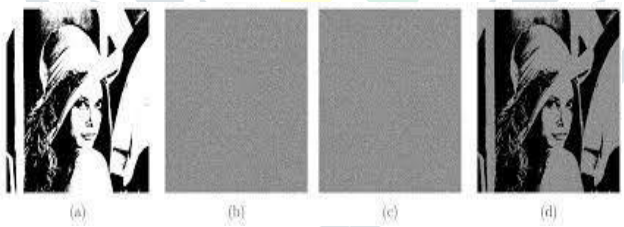

Fig.2.1:VCS sharingimage throughgrayscale [53]
(a) image(original)
(b) share image1
(c) share image2
(d) image decrypted

ii. VCS GeneralAccessStructure

Only participants in a qualified group can decode information using VCS for General Access Structures (GAS), which separates information into a subset of the restricted and prohibited group of participants.This section discusses various GAS-based VCS types. GAS VCS examines the VCS's organizational structure and demonstrates the restrictions on the size of the shares allotted to scheme members. The proposed method demonstrates a state-of-the-art strategy to achieve k out of n VCS thresholds.[39] provides a new method that is superior to the method proposed by M.Naor & A.Shamir for running k of n VCS.

A diagram explaining the encryption and decryption of images is available here.

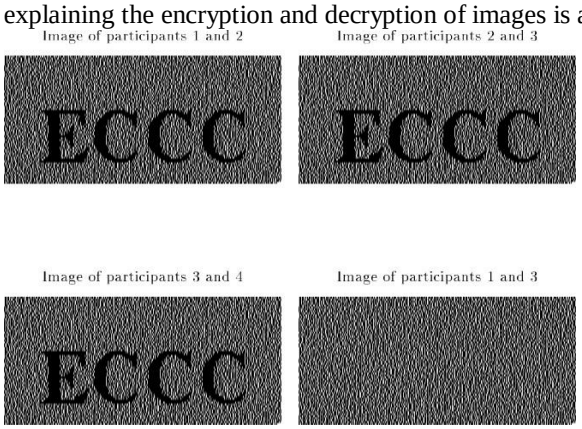

Figure 2.2: visual cryptography explained diagrammatically [39]

iii. Halftone VCS

The halftone VCS referenced in [16]. Half toning, which mutes colors to reduce pixel size, is a concept that is introduced. If the grey levels are reduced by two, the resulting image doesn't have enough spatial resolution to show the details. Dithering is the process of creating colors where none exist. It's done through the random pixel layout. The Floyd Steinberg dithering technique is a way to adjust the color. A single pixel quantization error is propagated to the neighboring pixel during the dithering process for later correction. When the original pixel values are halfway between the closest available colors, the dither effect creates a checkerboard pattern.For example, 50% of the gray data can be split into a black and white checkerboard pattern. The number of quantization errors must be accurate enough to avoid rounding errors affecting the results for optimal dithering.

The proposed method uses the idea of blue noise dithering to transform a binary latent image into regular images with significant visual information in n halftones. Using halftoning techniques, a halftone encoded secret image is created that captures a meaningful image, the pixel size is expanded, resulting in a larger image area in visual encoding. The stocks are halftone and the secret image is embedded as binary value stocks.Error diffusion has the benefit of being simple and having outstanding image quality in halftone sharing. Halftone VCS also uses Floyd and Jarvis dithering methods addressed in [17] include the reconstructed image's contrast and similar image quality.

Fig2.3:HalftoneVCS Image sharing[16]
i. Image (sent) ii.Image (received)

The original image is on the left of the top image and the encrypted image is on the right. The contrast between the original image and the decoded image is just the opposite. Graphics that follows explains why the colors of the pixels in the image have .

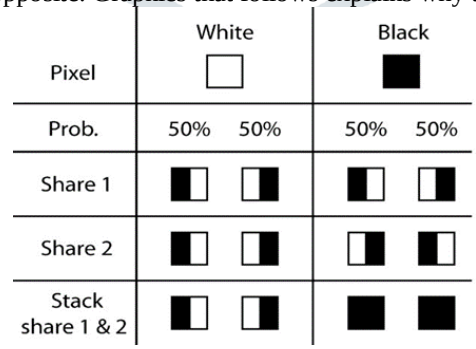

Fig2.4:halftone VCS Working [6]

The mentioned image in question shows that this method cannot provide a copy of the shared image.

iv. ColorVCS

An article [48] developed a visual color encoding where the encoding process uses the XOR operation. Binary images are created from monochrome photos to create binary encoded images;these binary images are encrypted using a binary image known as Share-1. Exclusive OR is used to individually encode the binary keyframe and the three halftones of the dark image. The shares are first encrypted on the source side, after that the result of the binary image is halftone backwards and merge to get the original image.

Cyan, magenta, and yellow are the three colors that make up the above image. The original color image of the encrypted image can be obtained by arranging the three images in the correct order.To reduce the aspect ratio, each image is halftone.

v. ProgressiveVCS

In terms of decoding, progressive visual coding (PVC) differs from traditional visual coding. The visibility and contrast of the hidden image decoded in the PVC steadily increases with the number of shares stacked.Progressive Color VCS is an additional variant of Progressive VCS.[25] The use of progressive color VCS, which applies to both color and grayscale images. The encryption can be recovered using one of three alternative description types, a better version of stacking to decrypt a raster image.

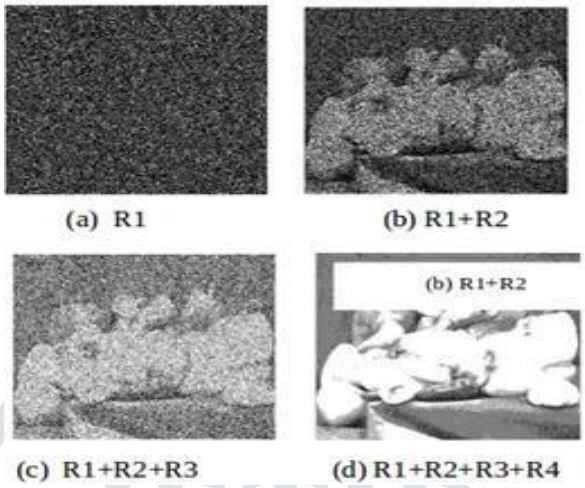

Fig2.6: Images in grayscale of the color red that are being constructed gradually [52]

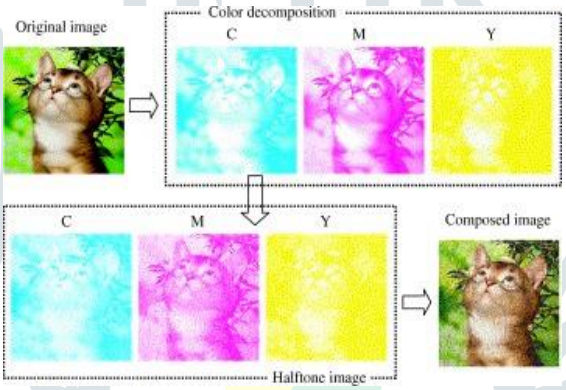

Fig:the Green image in grayscale [52]

Green and blue images are likewise created in grey scale, same to images in red.

Fig: Reconstructed Image[52]

Another paper discusses progressive VCS that can be used to decrypt secret images. With a progressive VCS, a small portion of the image would give an idea of the secret image, and as the number of shares stacked increases, the details and hidden information would gradually become visible. The report states that the pixel enhancement is of fairly poor quality compared to other pixel enhancement methods.[26] The study proposed a completely new and radical spread of PVC, a strategy for creating shares that aren't many pixels in size. No one can reveal secrets with a share. Unlike (n-1)/n, overlapping division is better than traditional methods.

vi. RegionincrementingVCS

Visual encryption with regional increment enables secrets of different sensitivity levels to be transmitted in a single image. Depending on the level of secrecy, this technique divides the image into multiple regions and then applies different encoding rules to each region. Many studies included RIVC. The content is divided into different regions associated with n hidden layers and encoded in n+1 shares with the properties detailed below in the VCS region-boosting study [21], which the RIVC-Ann layers scheme.Not all shares can have secrets.

(i) I Secrets at any level of t-1 can be revealed using any t share.
(ii) Users are unaware of the quantity and location of undiscovered secrets.
(iii) When all n+1 shares are available, all of S's hidden information is made public.
(iv) Visual inspection reveals secrets without the need to measure properly stacked shares.

A novel method that enhances region incrementing VCS is called region in region incrementing. A new layer of secrecy enhancement is included in the suggested method for region incrementing VCS. This method was proposed in the paper [22], and it has the advantage of providing a bigger area to conceal the hidden image than the non-overlapping parts in Region Incrementing VCS.

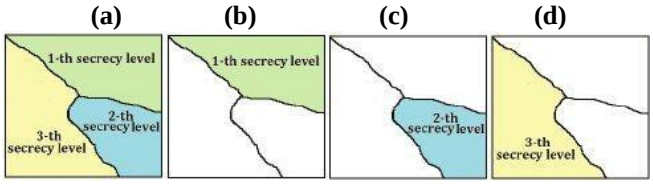

Fig:Apartition of three secrecylevel regionsforthe(2,4)-RIVCS:

(a) Decomposition of secrecy levels into three levels (b) the region that is visible when two shadows are piled. (c) The area that is made visible by stacking three shadows. (d) The area made visible by piling four shadows.[22]

ExtendedVisualcryptography

Although the Enhanced Visual Cryptography Scheme (EVCS) and traditional VCS are comparable, this method has major advantages. Another type of steganography is EVCS. This section explains recent research inthis area of encryption. In article [27], digital watermarking is used to generate a large number of shares. Hidden shares are marked with multiple cover photos before publishing. One cover image at a time, taken from shared resources, is stacked to gradually reveal the hidden image. By pulling out the shared images, the images reveal themselves little by little. This technique has advantages of good security and high contrast of the reconstructed image. To improve the quality of the released photos and restore an image similar to the original secret halftone image, the raster image method. The treatment is suggested in the study [28]. The work suggested a compromise between the contrast of the image recovered on each slide and the contrast of the image [29].

With this method, hackers cannot derive any secret image information from individual cover images. As a result, scientists have developed a method for visually encoding color images. The paper [18], which uses the halftone technique, includes a code table and a secret code table to achieve two main divisions at the same time, discussing image sharing without attracting the attention of hackers. The article also examines hiding a secret image in two or more images named Shares that have a purpose and are of no interest to hackers. This approach uses the halftoning technique to hide the secret scrambling table over the scrambling table used to create the shares. When stacking high bets, the secret isunlocked. Chaotic random number is a technique used by [19] where encryption is done by sifting, dividing and chaotic randomization. Random composition was previously used in [20] where it was used to parse a VSS scheme based on any threshold grid to improve visual quality and examine differences between related methods. According to Paper [23], decrypting the image does not require great computer or cryptographic skills but the image could not be accessed. According to the article, the benefits of the black and white VCS can be preserved by using the human visual system to decode the scrambled images without the need for computation and maintaining backwards compatibility with previous discoveries. The following explanations of several expanded visual cryptography types:

(a) Colorextendedvisualcryptography

Article [30] covers the topic of embedding secret messages in shared color raster images. The purpose of this article is to demonstrate the advantages of visual color encoding over other encoding techniques.Because color contributions have different color structures, previous methods in the literature have shown good results for black and white or grayscale VC schemes, but are insufficient for direct application to color contributions.Some of the VC approaches are unsatisfactory as they deliver significant portions that are nonsensical or of poor visual quality, raising suspicions of encryption. To get a color visual encoding method that produces a significant percentage of colors with good visual quality, study introduces visual information pixel synchronization (VIP) and error diffusion. VIP Sync preserves pixel position while transferring visual information from the original color images. Channels and error diffusion produce contributions pleasing to the human eye. Comparing this method to the previous methods, it is clear that the new approach works better than the previous strategies.

(b) EmbeddedExtendedVisualcryptography

Using more than one secret image and inputs, the approach presented in [50] defines and presents different indicators for the contribution to visual quality, namely MAX ERROR, PSNR and Mean Square value. These values are specified between each segment. By stacking or overlaying a subset of contributions, this approach ensures that the hidden image is revealed.This study analyzes the results using various visual quality metrics, including PSNR, MSE, and MAX ERROR, and uses multiple input images and hidden segments to generate these values. Half toning also calculated using the matrix size defined by the user in this study.

vii. XORandORandotherVCS

This section covers many VCSs that use XOR, OR, etc. with different types of methods and operations. Article [31] deals with XOR-based visual encryption using the XOR technique for decoding to increase color contrast. In this thesis, the relationship between OR- and XOR-based VCS is investigated. The paper also found that the basic matrices of (k,n)-OVCS can be applied to (k,n)-XVCS by increasing the contrast by 2(k-1) times. The other plans are those listed in [32]. The encryption method uses sub-pixel imaging. Sub-pixels have the same color as the main pixel.Considering the pixel expansion, there was an improvement over

previously established optimal designs. Excellent resolution, contrast and color properties are found in VCS based on polarization. This isdescribed by the XOR method. A study [33] examines the visual secret sharing threshold system associated with XOR-based VC schemes. The resolution of the scheme is much higher than OR-based VC schemes.Even k-of-n schemes for XOR are fundamentally different from odd k-of-n strategies.

The study [34] discusses adaptive VC and XOR-based VC algorithms with area enlargement for commonly available structures. This article examines the effectiveness of visual encryption techniques.To solve the problem of poor image quality without blurring in the VC, two XOR-based VCs are presented in [35]. To get the most out of VCS, advanced features are recommended in addition to the XOR-based VCS features.This study uses two algorithms, with the first being used to create a sophisticated release strategy using GAS without compromising utility. The second approach restores security levels based on qualified sentences, not quality in adaptive security.The size-independent method introduced another type of visual secret-sharing method, the VCS. In this scheme, the secret image is encoded infractions larger than the original images and fractionsare then decrypted on the stack without doing any cryptographic work. Such a method for encoding a black and white image into identically sized parts of a secret image is discussed in [36]. Suggested schemeconstructed image contrasts with a traditional chart. Contrast VCS is another form of VCS, also used to encode and decode data, but differs from other schemes in that it attempts to minimize pixel expansion while maximizing visual contrast.In the paper [37], contrast enhancement was discussed and k-on-n thresholding techniques were used to analyze image contrast. The article uses k=2.Another type of VCS, called Multi-Secret VCS, is proposed in [38] and examines the situation where more than one picture needs to be encrypted. Security and contrast issues are addressed together in the study.[39] Visual analysis of the encryption scheme components and demonstration of the scheme sizes assigned to participants. It provides a new way to display visual threshold encryption methods for kouts of n.The proposed construction for k out of n visual encryption methods exceeds the expected one in terms of pixel expansion.

III. ANALYSIS OF THE PERFORMANCE OF CERTAIN CRYPTOGRAPHIC SCHEMS

In the above situations which are very important for data security, this method is only used for data encryption because the performance of visual encryption is reliable. The performance of cryptographic systems is analyzed in [45].The results of the analysis show that while RC4 and Triple DES have low and medium encryption rates, respectively, and the rest of symmetric key encryption have high encryption rates, asymmetric key encryption has high encryption rates.The study [34] analyzes how the power of XOR-based encryption was exploited and presents two variants, including XOR-based VC for GAS and XOR-based VC Zone Adaptive Amplification. Research leads to further conclusions using the Generic Access Framework (GAS)Implemented in XOR-based VC technology for GAS, which is a complex subdivision technique.There was a way to provide an algorithm classified by visual encryption standards while also understanding the process of implementation and to be able to evaluate algorithm process and provide data for image reconstruction.

An excellent description of visual encryption techniques can be found in publication [46].The analysis shows how visual encryption has evolved and how new techniques have improved the quality of image transmission. It has proven particularly useful for data encryption in the field of image processing.

In addition, visual encryption can be used for a variety of everyday purposes and proved its usefulness as a means of implementing network and data security. Another overview [11] lists many of the contributions from authors who have helped visual cryptography reach important milestones. Calculation based on image size, pixel extension, number of hidden images and sharing types, visual encryption increases security with biometric authentication. Iris is one such authentication method used as reported in [47] where researchers used different strategies to secure the raw biometric data and the template in the databasein conversation. The proposed method is to use visual encryption to securely store the iris pattern in the database. The iris needs to be mapped to authentication, but in this case the iris authentication speed is slow.

Manual image comparisons are used to compare visual encryption methods and image restoration techniques. The example image in Fig.shows the difference between the images for comparison.XOR,grayscaleand half-tone images.

IV.CONCLUSION

This paper examined the benefits and drawbacks of the various cryptographic technologies. Each technique is chosen in accordance with the necessary requirements for the parameters used. The paper also discusses a comparative analysis of all forms of visual cryptography and their benefits. Future research directions will benefit from the insights provided by this work. Visual cryptography can only prevent data flow interception; it cannot prevent data snooping. Snooping has direct access to the nodes' data. However, encryption only takes place when data is being transmitted. Therefore, the protection of nodes could be increased using visual cryptography.

REFERENCES

1. D'Arco, Paolo, Roberto De Prisco, and Yvo Desmedt. "Private visualshare-homomorphic computation and randomness reduction in visualcryptography." In International Conference on Information TheoreticSecurity,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,Issue3,2488-2491,2014
3. CimatoS,YangC.N,"VisualCryptographyandsecretimagesharing",CRCpress 1stEdition,2017.
4. Naor,M.,A.Shamir."Visualcryptography.AdvancesinCryptologyEUROCRYPT'94 Lecture Notes in Computer Science." InWorkshopontheTheoryandApplicationofCryptographicTechniques,May9C12,pp.1-12.1995.
5. Liu, F., Yan, W. Q. "Visual Cryptography for Image Processing andSecurity" Vol.2.NewYork:Springer,2014
6. Chandramathi S, Ramesh Kumar R, Suresh R, Harish S "An overviewofvisualcryptography"InternationalJournalofComputationalIntelligenceTechniques,Vol1Issue1, pp32-37,2010.
7. Weir,J.P.Visualcryptographyand itsapplications. Bookboon, 2012.

8. Lou, Der-Chyuan, Hao-Kuan Tso, and Jiang-Lung Liu. "A copyrightprotectionschemefordigitalimagesusingvisualcryptographytechnique."ComputerStandards&InterfacesVol.29,no.1pp .125-131,2007.
9. Hwang, Ren-Junn. "Adigitalimagecopyrightprotectionschemebasedonvisualcryptography." Vol. 3,no. 2,pp97-106,2000.
10. Weir, Jonathan, and WeiQi Yan. "A comprehensive study of visualcryptography."Transactionsondatahidingandmultimediasecurity V,Springer, Berlin,Heidelberg,vol. 5pp.70-105 2010.
11. Revenkar, Pravin S., Anisa Anjum, and W. Z. Gandhare. "Survey ofvisualcryptographyschemes."InternationalJournalofSecurityandItsApplications Vol4,no.2pp49-56,2010.
12. Cai J. A short survey on visual cryptography schemes. Department ofComputerScience,UniversityofToronto.2004.
13. Shyu,ShyongJian,Shih-YuHuang,Yeuan-KuenLee,Ran-ZanWang,andKunChen."Sharingmultiplesecretsinvisualcryptography." Pattern Recognition Vol. 40, no. 12 pp.3633-3651,2007
14. Blundo, Carlo, Annalisa De Bonis, and Alfredo De Santis. "Improvedschemes for visual cryptography." Designs, Codes and CryptographyVol.24,no.3pp.255-278,2001.
15. Blundo,Carlo,AlfredoDeSantis,andMoniNaor."Visualcryptography for grey level images." Information Processing Letters2000Vol.75,no.6255-259,2000.
16. Zhou Zhi, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftonevisualcryptography."IEEEtransactionsonimageprocessing15,no.8,2441-2453,2006.
17. Wang, Zhongmin, Gonzalo R. Arce, and Giovanni Di Crescenzo."Halftone visual cryptography via error diffusion." IEEE transactionsoninformationforensics andsecurity4,no.3,pp383-396,2009.
18. Wu, Hsien-Chu, Hao-Cheng Wang, and Rui-Wen Yu. "Color visualcryptographyschemeusingmeaningfulshares."IEEEEighthInternationalConferenceonIntelligentSystemsDesignandApplications, ISDA'08,vol.3,pp.173-178, 2008.
19. Krishna,Murali,andM.JayaRam."ChaoticBasedEnhancedKeylessColor Image Visual Cryptography System." Journal of Innovation inComputerScienceandEngineering Vol.6,no.1pp.26-28,2016.
20. Yan, Xuehu, Xin Liu, and Ching-Nung Yang. "An enhanced thresholdvisual secret sharing based on random grids." Journal of Real-TimeImageProcessing14,no.1pp.61-73,2018
21. Wang, Ran-Zan. "Region incrementing visual cryptography." IEEESignalProcessingLetters 16,no.8pp.659-662,2009.
22. Yang,Ching-Nung,Yi-ChinLin,andChih-ChengWu."Region-in-Region incrementing visual cryptography scheme." In TheInternational Workshop on Digital Forensics and Watermarking 2012,pp. 449-463.Springer,Berlin,Heidelberg, 2013.
23. Hou, Young-Chang. "Visual cryptography for color images." Patternrecognition36,no.7(2003):1619-1629.
24. Jin, Duo, Weiqi Yan, and Mohan S. Kankanhalli. "Progressive colorvisualcryptography."Journalof ElectronicImaging14,no.3 (2005): 033019.
25. Hou,Young-Chang,andZen-YuQuan."Progressivevisualcryptography with unexpanded shares." IEEE transactions on circuitsandsystems forvideotechnology21,no.11(2011):1760-1764.
26. Jithi, P. V., and Anitha T. Nair. "Progressive Visual Cryptographywithwatermarkingformeaningfulshares."InAutomation,Computing,Communication,ControlandCompressedSensing(iMac4s),2013InternationalMulti-Conferenceon,pp.394-401.IEEE,2013.
27. Askari,Nazanin,HowardM.Heys,andC.R.Moloney."Anextendedvisualcryptographyschemewithoutpixelexpansionforhalftoneimages."InElectricalandComputerEngineering(CCECE),201326thAnnualIEEECanadianConferenceon,pp.1-6.IEEE, 2013.
28. Ateniese, Giuseppe, Carlo Blundo, Alfredo De Santis, and Douglas R.Stinson. "Extended capabilities for visual cryptography." TheoreticalComputerScience250,no.1-2(2001):143-161.
29. Kang, InKoo, Gonzalo R. Arce, and Heung-Kyu Lee. "Color extendedvisualcryptographyusingerrordiffusion."IEEETransactionsonimageprocessing20,no.1(2011):132-145.
30. Yang,Ching-Nung,andDao-ShunWang."PropertyanalysisofXOR-based visual cryptography." IEEE transactions on circuits andsystemsforvideotechnology24,no.2(2014):189-197.
31. Blundo, Carlo, Annalisa De Bonis, and Alfredo De Santis. "Improvedschemes for visual cryptography." Designs, Codes and Cryptography24,no.3(2001):255-278.
32. Tuyls, Pim, Henk DL Hollmann, Jack H. Van Lint, and L. M. G. M.Tolhuizen."XOR-basedvisualcryptographyschemes."Designs,Codes andCryptography37,no.1(2005):169-186.
33. Soman N, Baby S "XOR based Visual cryptography". InternationalJournaloncyberneticsandinformatics(IJCI)5,no.2(2016):253-264
34. Wu, Xiaotian, and Wei Sun. "Extended capabilities for XOR-basedvisual cryptography." IEEE Transactions on Information Forensics andSecurity9,no.10(2014): 1592-1605.
35. Ito, Ryo, Hidenori Kuwakado, and Hatsukazu Tanaka. "Image sizeinvariantvisualcryptography."IEICEtransactionsonfundamentalsofelectronics, communications and computer sciences 82, no. 10 (1999):2172-2177.
36. Blundo, Carlo, Alfredo De Santis, and Douglas R. Stinson. "On thecontrast in visual cryptography schemes." Journal of Cryptology 12,no.4(1999):261-289.
37. Yang, Ching-Nung, and Ting-Hao Chung. "A general multi-secretvisualcryptographyscheme."OpticsCommunications283,no.24(2010):4949-4962.
38. Ateniese, Giuseppe, Carlo Blundo, Alfredo De Santis, and Douglas R.Stinson."Visualcryptographyforgeneralaccessstructures."InformationandComputation129,no.2(1996):86-106.
39. Bludno,C.,DeSantis,A.,Stinson,D.R.,andVaccaro,U.(1995),Graph decomposition and secret sharing schemes,J.Cryptol.8,39-64.

40. Yengisetty, Subba Rao V., and Bimal K. Roy. "Applications of visualcryptography."InternationalJournalofParallel,EmergentandDistributedSystems 26,no.5(2011):429-442.
41. ManasiAshokraoDeshmukh,R.V.Deshpande“Anti-phishingwebsiteusingvisualcryptography”InternationalJournalofInnovativeResearchinComputerandCommunicationEngineering,5no.7,(2017):13385-13393
42. Pandey,Anjney,andSubhranilSom."Applicationsandusageofvisualcryptography: A review." In Reliability, Infocom Technologies andOptimization(TrendsandFutureDirections)(ICRITO),20165thInternationalConferenceon,pp.375-381. IEEE,2016.
43. Hawkes, L., Alec Yasinsac, and C. Cline. "An application of visualcryptographytofinancialdocuments."FloridaStateUniversity,Florida (2000):1-7.
44. Jeeva, A. L., Dr V. Palanisamy, and K. Kanagaram. "Comparativeanalysis of performance efficiency and security measures of someencryption algorithms." International Journal of Engineering ResearchandApplications (IJERA)2,no.3(2012):3033-3037.
45. Walden,Disa."ABenchmarkingassessmentofknownvisualcryptographyalgorithms." (2012).
46. Revenkar, P. S., Anisa Anjum, and W. Z. Gandhare. "Secure irisauthenticationusingvisualcryptography."arXivpreprintarXiv:1004.1748(2010).
47. Krishnan, Gopi S., and D. Loganathan. "Color image cryptographyschemebasedonvisualcryptography."InSignalProcessing,Communication,ComputingandNetworkingTechnologies(ICSCCN), 2011 International Conference on, pp.404-407. IEEE,2011.
48. ChandrasekhaRa,andJagadeesha“SecureBankingApplicationsusingvisualcryptographyagainstfakewebsiteauthenticitytheft.” InternationalJournalofadvancedcomputerengineeringandcommunication technology,2no.2(2013):1-5.
49. Navjot Kaur & Dr Rajiv Mahajan "An enhanced embedded, extendedvisualcryptographyscheme"InternationalJournalofSoftware&HardwareResearchinEngineering,2no.5,(2014):120-122.
50. Isha Padiya, Vinod Manure, Ashok Vidhate Visual “secret sharingscheme using encrypting multiple images” International Journal ofadvancedresearchinElectrical,ElectronicsandInstrumentationEngineering4no.1,(2015):132-137
51. Fersne,Athira“ProgressivevisualCryptographyschemewithoutpixelexpansionforcolourimages”Internationaljournalofadvancedresearch in computer and communication engineering 4 no 6 (2015):186-191