ISSN:0975-9646

A Survey on Visual Cryptography Techniques and their Applications

Ms. Bhawna Shrivas
M. Tech Scholar
Mahakal Institute of Technology
Behind Air Strip, Dewas Road,
Ujjain(M.P.) -456664, India

Prof.Shweta Yadav
Reader
Mahakal Institute of Technology Behind Air Strip,
Dewas Road, Ujjain(M.P.) -456664, India

Abstract-Image cryptography is emerging field of the research. There are various techniques has been established for cryptography. The many encryption techniques have been used for hide the visual information (pictures, text, etc.) in images. The main idea of encryption is possibility of decryption by the human vision if the correct key image is used is known as visual cryptography. In this paper, different research has been discussed for Visual Cryptography.

Keywords: Visual Cryptography, Halftone, Dithering etc.

1. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in the way that decryption becomes a mechanical operation. Visual Cryptography utilizes two transparent images. One image contains random or noisy pixels and the other image contains the secret data. It is almost impossible to retrieve the secret information from encrypted images. Both transparent images and layers are required to reveal the information. The easiest way to implement a Visual Cryptography is to print the two layers onto one transparent sheet.

The advantage of visual cryptography scheme is that it eliminates computation problem during decryption process, and the secret image can be restored by stacking operation. This property makes the visual cryptography especially useful for the low computation method.

The visual cryptography scheme was introduced by Naor & Shamir 1994 [1]. It is a secret sharing scheme with good security for binary image. Another distinguished advantage of this is that it decodes directly during human vision.

There are different levels of visual cryptography techniques. In this paper we will discussed the work done on the

a. Binary images
b. Gray Images
c. Color Images .

The research work are described in the subsequent topics.

2. VISUAL CRYTOGRPHY FOR BINARY IMAGES

Naor and Shamir's [1] have proposed a (k, n) threshold visual cryptography scheme which encodes a given secret image into n shadow images (shares), where any k or more of them can visually recover the secret image system, but any k-1or fewer of them fail to recover the secret image. It exploits the human visual system to read the secret message from some overlapping shares function, thus overcoming the disadvantage of complex computation required in the traditional cryptography.

The basic model of visual cryptography scheme proposed by Naor and Shamir has been applied to many applications, they include information hiding, general access structures, visual authentication, and identification and so on. Unfortunately, these applications are all restricted o the use of binary images as input due to the nature of the model. This drastically decreases the applicability of visual cryptography because binary images are usually restricted to represent text-like messages.

In [2] Wu et al have proposed a visual cryptography schemes to share two secret images in two shares. In the hidden two secret binary images into two random Shares, for namely A and B, such that the first secret can be seen by stacking the two shares. In [3] S J Shyu et al authors have proposed the multiple secrets sharing in visual cryptography. This scheme encodes a set of $n \geq 2$ secrets into two circle. The n secrets can be obtained one by one by stacking the first share and the rotated second shares with n different rotation angles this system. To encode unlimited shapes of image and to remove the limitation of transparencies to be circular, offered reversible visual cryptography sytem. In this scheme two secret images which are encoded into two shares; one secret image appears with just stacking two shares and the other secret image appears with stack two shares after reversing one of them. Jen-Bang Feng et al [5] developed a visual secret sharing scheme for hiding multiple secret images into two shares.

In image data hiding schemes the secret image data is embedded into several images. For the embedded data can be extracted with some procedure process. On the other hand, visual cryptographic techniques break up a secret image into several shares so that only someone with all shares can decrypt the secret image by superposing all shares together. It is image data hiding schemes based on error diffusion have the feature of visual cryptography with respect to extracting of embedded data image. They embed secret image data into several halftone images without affecting their perceptual qualities and the embedded data can be restored with apparently high quality when the halftone images are overlaid without any special electronic calculation. In [18] authors have formulated an image data hiding scheme based on error diffusion and proposed a formulation for the scheme in the view of a stochastic analysis.

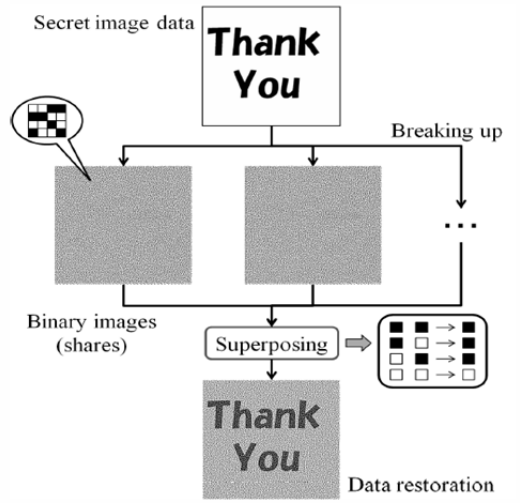
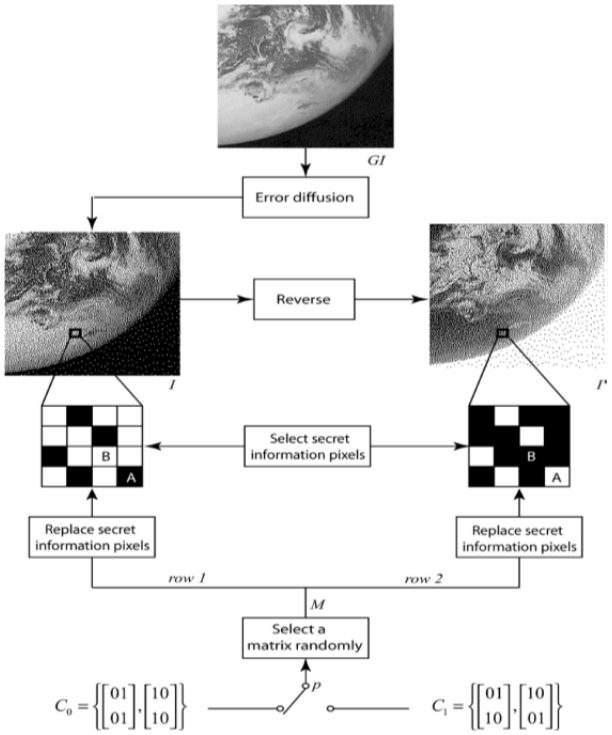


Figure 1: Typical flow chart of visual cryptography scheme [18]

Visual cryptography encodes a secret binary image into shares of random binary patterns. The shares are xeroxed onto transparencies, if the secret image can be visually decoded by superimposing a qualified subset of transparencies, no secret information can be obtained from the superposition of a forbidden subset process. The binary patterns of the shares, they have no visual meaning and hinder the objectives of visual cryptography. In [17] authors have proposed a novel technique named halftone visual cryptography. Based on the blue-noise dithering principles, their proposed method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information. Their simulation shows that the visual quality of the obtained halftone shares is observably better than that attained by any available visual cryptography method known to date.



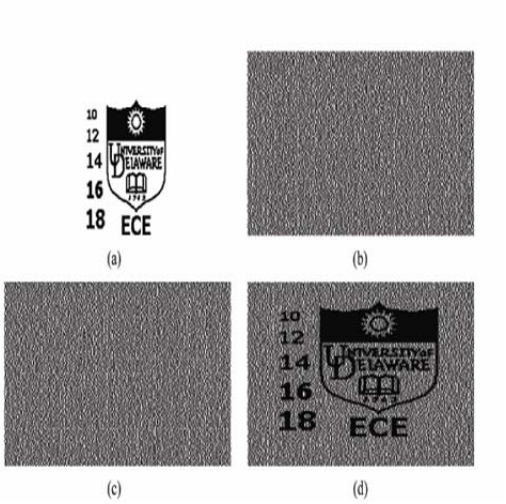


Figure 2: Visual cryptography scheme proposed by Zhi Zhou et al [17]

3. VISUAL CRYTOGRPHY FOR GRAY IMAGES

In [6] Conventional visual cryptography methods divide a secret digital image into n pieces and distribute them to n participants. This paper proposes a novel approach to visual cryptography for binary images that includes the capabilities of watermarking and verification. The proposed method allows an n×n watermark image to be embedded into an n×n secret image to construct two shadows and then to be used to verify the accuracy of the reconstructed image. The checking to determine the reliability of all shadows before they are used to recover the secret image prevents a participant from incidentally or deliberately providing invalid data.

4. VISUAL CRYTOGRPHY FOR COLOR IMAGES

Gopi et. al [7} have proposed a new cryptography scheme for securing color image based on visual cryptography scheme. In a color image to be protected and a binary image used as key to encrypt and decrypt are taken as input data. A secret color image which needs to be communicated is decomposed into three monochromatic images based on YCbCr color space system. Then these monochromatic images are converted into binary image data, and finally the obtained binary images are encrypted using binary key image, in a called as share-l to obtain binary cipher images. To encrypt Exclusive OR operation is done between binary key image and three half-tones of secret color image separately. For the binary images are combined to obtain share-second (2). In decryption the shares are decrypted, for the recovered binary images are inverse half toned and combined to get secret color image. According to authors this scheme is more efficient than existing schemes.

In [8], a verifiable visual cryptography scheme is proposed to verify whether the share is authorized, in which authors have introduced a Third Trusted Party (TTP) whose action is guaranteed. It is scheme solves the participants distrusting in the center so as to improve the security of visual cryptography schemes. In [9] a simulation result shows that the visual quality of the obtained halftone share are observably better. In [10] a novel (2, m + 1) visual

cryptographic technique has been proposed image data, where m number of secret images has been encrypted based on a randomly generated master as a common share for all secrets which is decodable with any of the shares in conjunction with master share out of m + 1 generated shares. The instead of generating new pixels for share except the master share, in hamming weight of the blocks of the secret images has been modified using random function to generate shares corresponding to the secrets.

In [11], authors introduces the concept of visual information pixel (VIP) synchronization and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality. The visual information pixel (VIP) synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes. For the Comparisons with previous approaches show the superior performance of the new method.

5. Applications Of Visual Crytogrphy Technique

As science and technology progresses and as more and more personal data is digitized, this is even more of an emphasis required on data security today than there has ever been. In protecting this data in a safe and secure way which does not impede the access of an authorized authority is an immensely difficult and very interesting problem. The attempts have been made to solve this problem within the cryptographic community.

Visual cryptography allows effective and efficient secret sharing between a number of trusted parties. With many cryptographic schemes, for trust is the most difficult part. In the visual cryptography provides a very powerful technique by which one secret can be distributed into two or more shares. The shares are xeroxed onto transparencies and then superimposed exactly together; in original secret can be discovered without computer participation.

Many applications based on visual cryptography has been developed. In [13] authors have applied visual cryptography for copyright protection. A multiparty scheme is presented for co-owners of digital image. Many novel algorithms have been proposed in the fields of steganography and visual cryptography with the goals of improving security, reliability, and efficiency George et.al [14] have compares the two methodologies and proposed a possible algorithm which combines the use of both steganography and visual cryptography.

Young et al. [15] have proposed a intellectual property protection scheme for digital images based on visual cryptography and statistical property. The result of comparing two pixels that are selected randomly from the host image determines the content of the master share. Then, the master share and the watermark are used to generate the ownership share according to the encryption rules of visual cryptography. Their method does not need to alter the original image and can identify the ownership without restoring to the original image. Besides, their method allows multiple watermarks to be registered for a single host image without causing any damage to other hidden watermarks. Moreover, it is also possible for this scheme to cast a larger watermark into a smaller host im

The importance of utilizing biometrics to establish personal authenticity and to detect imposters is growing concern in the present scenario of global. The visual cryptographic methods can be used to detracts the suapicious looking peoples. In [16] authors have proposed secure tongue biometric authentication system using visual cryptography.

6. Conclusion

An extensive survey of different visual cryptographic techniques and their applications is presented in this paper. Many types of visual cryptography are examined from the very first type of traditional visual cryptography right up to the latest developments in it. Traditional VC specifically deals with sharing a single binary secret between a number of participants. Extended VC attempts to take this a step further.

Acknowledgments

Authors are thankful to the Head of Department of Mahakal Institute of Technology (MIT), Ujjain, India for his kind support and useful technical discussion during the course of this work, Thanks are also due to friends and colleagues of our department for their cooperation, fruitful technical discussion and guidance.

References

[1] M.Naor, A. Shamir, “Visual cryptography,”Advances in Cryptology-EUROCRYPT’94, LNCS, vol.950,pp.1-10,1995.

[2] C.C. Wu, L.H. Chen, “A Study On Visual Cryptography”, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[3] S.J.Shyu, S.Y.Huanga, Y.K.Lee, R.Z.Wang, and K.Chen, “Sharing multiple secrets in visual cryptography”, Pattern Recognition, Vol.40, Issue 12, pp.3633-3651,2007.

[4] Wen-Pinn Fang, “Visual Cryptography In Reversible Style”, IEEE Proceedingon the Third International Conference on Intelligent Information Hidingand Multimedia Signal Processing (IIHMSP2007), Kaohsiung, Taiwan, R.O.C,2007

[5] Jen-Bang Feng, Hsien-ChuWu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, “Visual Secret Sharing For Multiple Secrets”, Pattern Recognition 41, pp.3572–3581, 2008.

[6] Zhi-hui Wang, Chin-Chen Chang, Huynh Ngoc Tu, “Sharing a Secret Image in Binary Images with Verification” Journal of Information Hiding and Multimedia Signal Processing Volume 2, Number 1, January 2011

[7] Gopi Krishnan S and Loganathan D,”Color Image Cryptography Scheme Based on Visual Cryptography “,Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011)

[8] Han Yanyan, Cheng Xiaoni, Yao Dong, He Wencai,” VVCS: Verifiable Visual Cryptography Scheme”, 2011 Seventh International Conference on Computational Intelligence and Security

[9] Nitty Sarah Alex, L. Jani Anbarasi,” Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography”

[10] J. K. Mandal, Subhankar Ghatak, “A Novel Technique for Secret Communication through Optimal Shares using Visual Cryptography (SCOSVC)”, 2011 International Symposium on Electronic System Design

[11] InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee, ” Color Extended Visual Cryptography Using Error Diffusion”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 1, JANUARY 2011

[12] Young-Chang Hou , Zen-Yu Quan “Progressive Visual Cryptography with Unexpanded Shares”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 21, NO. 11, NOVEMBER 2011

[13] Shen Ying," Visual Cryptography based Multiparty Copyright Protect Scheme", 978-1-4244-5848-6/10/ ©2010 IEEE
[14] George Abboud, Jeffrey Marean, Roman V. Yampolskiy," 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering", 978-0-7695-4052-8/10 © 2010 IEEE DOI 10.1109/SADFE.2010.14
[15] Young-Chang Hou, Pei-Hsiu Huang," IMAGE PROTECTION BASED ON VISUAL CRYPTOGRAPHY AND STATISTICAL PROPERTY", 2011 IEEE Statistical Signal Processing workshop (SSP)
[16] Sowmya Suryadevara, Rohaila Naaz, Shweta, Shuchita Kapoor, Anand Sharma," Visual Cryptography Improvises the Security of Tongue as a Biometric in Banking System", International Conference on Computer & Communication Technology (ICCCT)-2011, 978-1-4577-1386-611@2011 IEEE
[17] Zhi Zhou, Member,Gonzalo R. Arce, Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST 2006
[18] Masakazu Higuchi, Shuji Kawasaki, Jonah Gamba, Atsushi Koike, Hitomi Murakami "A Fundamental Conception to Formulate Image Data Hiding Scheme Based on Error Diffusion from Stochastic Viewpoint", INTERNATIONAL JOURNAL OF APPLIED MATHEMATICS AND INFORMATICS, Issue 1, Volume 6, 2012.

AUTHORS PROFILE

Ms. Bhawna Shrivas is a M. Tech Scholar in Mahakal Institute of Technology, behind Air Strip, Dewas Road, Ujjain(M.P.) -456664, India. Her research interest are in the area of visual cryptography and encryption algorithms for data securing and transmission.

Prof Shweta Yadav is a reader in Mahakal Institute of Technology, behind Air Strip, Dewas Road, Ujjain(M.P.) -456664, India. Her research interest are in the area of cryptography and encryption algorithms for internet security.