A Study on Modeling and Constraints of Visual Cryptography

Sakshi Mehta
Department od computer science
BRCM college of engineering
Bahal,India

Basant Sah
Assistant Professor , Department of Computer science
BRCM college of engineering
Bahal,India

Dr V K Jha
Associate Professor , Department of Computer science
BIT , Mesra Ranchi
India

Abstract— Today, information is communicated in different forms. Image data communication is one such desired data form. Biometric authentication, graphical passwords has improved, the need to secure this Visual data. Visual cryptography is one such encoding technique defined specifically for Image data. In this paper, the modeling of visual cryptography method is presented as well as associated features are explored. The paper defines the basic process method of visual cryptography along with relative constraints. The paper explores the associated constraints, matrices and methods.

Keywords : Visual Cryptography, Visual, Encoding, Decoding

I. INTRODUCTION

Visual cryptography is one of the extension method which provides the image encoding under share content method. This image content sharing method is provided to generate the multiple shares on an image or pixel with the inclusion of specific binary patterns to provide effective image encoding. A share specific transparency analysis is here provided to identify the share of each participant. The visual information sharing is here divided based on the number of participants and applied to partial pixel contents. This partial pixel content processing also improves the computational power of visual cryptography method along with model processing respective to the number of defined shares. Some of the common encoding process based on two shares is shown in figure 1. Cryptography method for secure communication. On the sender side, the key based encoding is performed and on the receiver side, the key based decoding is performed. The basic encoding and decoding process is shown in figure 1. The method is based on the multiple splits applied over the image. These splits are based on defined or the random patterns. The information accession and stacking between these multiple shares is applied to generate the result information. The information can be revealed so that the perfect reconstruction to the secret image can be done to generate the result image. The figure is showing the split adaptive method along with relative share specification. The figure is share showing the encoded and the decrypted image pixel for half tone images along with the color specification. The block specific pixel color specific encoding method is shown here in the figure

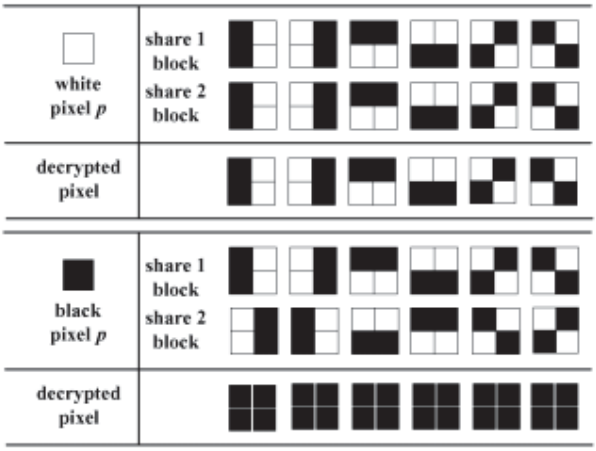

Figure 1 : Share Specific Visual Cryptography[8]

In case of visual cryptography, two or more shares are defined based on the individual and authentication specification. The information capturing along with secret image processing is applied to generate the stacked shares. The logical operations can be employed on these partial bit parts to generate the reconstructed secret image. The constraints or the conditions can be applied while setting up the features of cryptographic image. These conditions or constraints are

- The number of shares must be defined to apply the sharing and to perform the recovery along with qualified share specification.
- The size of qualified set of shares are required to defined to apply the effective encoding and modeling the cryptographic method.
- The method uses the visual or the error information of the image to generate the encoded image.
- The pixel size of generated qualified result image must be defined and restricted.
- The meaningful information from the image must be preserved.
- The share preserved encoding is defined by the method to provide the effective information gain and to provide the reliable result image.
- The key specific encoding can be applied to improve the encoding result.

In this paper, an exploration to the visual cryptography is provided. The paper defines different constraints, features and types of visual cryptography. In this section, the basic concept of visual cryptography is provided along with characterization of cryptography method. Different associated constraints are also defined. In section II, the exploration of visual cryptography methods proposed by different researchers is discussed. In section III, different methods of visual cryptography are explored. In section IV, the conclusion of work is presented.

II. EXISTING WORK

Cryptography is the way to secure the information transmitted by applying the encoding technique over it. The data in different media forms can be secured by using a different cryptography method. For encoding the image data by preserving the image contents, the visual cryptography method can be applied. In this section, different algorithmic approaches and advancements proposed by different earlier researchers are defined. Ramya et. al.[6] has provided a study on different methods and measures of visual cryptography. Author identified various application domains, including the capacha processing, printing information processing, etc. The bit expasion method, image format and other key constraints were also discussed by the author.

Visual cryptography basically works on different binary patterns and different qualified sets of transformation to generate the secret image. Different researchers used different image information, features and patterns generate the encoded image. One such encoded approach was proposed by Zhou et. al.[1] by utilizing the principle of noise dither. Author has used the cluster algorithm to utilize the selective image share to utilize the binary information. The image structure is utilized here with specification of qualified subsets and relatively joined these subset to generate the encoded image. An extensive improvement to the visual cryptography was provided by Desiha et. al.[2] by applying the effective dithering on halftone biometric images. The gemerated the location

specific data patterns on halftone images and generated the dithering matrix for image encoding. Alex et. al[3] has provided the meaningful sharing of image along with generation on encoding segments including the noise, color information etc. The error filters are also implied on image to improve the featured strength of image. The random share was created for the half tone image and processed the neighbor pixels to generate the encoded image. The weighted proposed method has improved the strength of cryptographic method and provided the qualified encoding of image. The visual information processing was provided for reducing the error diffusion for halftone shares. Malik et. al.[4] has captured the visual information of written text, notes and pictures. The cryptography method was implied respective to sheer size and quality of reconstructed images. The real time processing on image features is provided for generation of encoded featured blocks. The domain specific processing was provided by the author for generating the encoded secret image.

Yanyan et. al.[5] has processed the overlapped information share along with verifiable visual cryptography scheme to improve the trust vector for image encoding. The distrust vector image was observed for improving the security vector for visual information constraints and to process the bit segmented information. The sub pixel processing was suggested by the author to generate the encoded image. Chavan et. al.[7] has provided a descriptive work on hierarchical visual cryptography method at different levels. Author observed the cryptograpy trends and generated the data segmented in extensive random form. The expansion ratio based observation is here implied for image encoding by merging the data segments. The share specific expansion ratio was procssed to improve the encoding measure. Kang et. al.[8] has used the error diffusion approach to apply visual cryptography on color images. Author defined a work on data synchronization and error diffusion to share the sensitive information secretly. The shared information is also preserved through the color channels and provided the performance adaptive communication. The contrast feature analysis is here provided to keep the content information and to provide the secret communication through meaniningful random patterns. Aksari et. al.[9] has provided a work to avoid the pixel expansion for half tone images and provided the safe and reliable communication in an open environment. The extensive size and the share information analysis was provided to recover the secure image. A series of processing methods are applied under the visual cryptography scheme to cover the meaningful image contents. The sub pixel based content information processing was provided to improve the carry capability of image. The interesting content preserved cryptography method is employed to share the visual contents effectively.

Monoth et. al.[10] has defined a work on contrast information processing for additional pattern generation for improving the visual cryptography method. The information processing analysis of different parameters is provided here to reconstruct the image effectively. The noise information contents were used by the author to generate the secret image by preserving the computational complexity. The pixel pattern analysis was provided to keep the effective image contents and to keep the visual cryptography under pattern preserving method. Anbarasi et. al.[11] has provided a work of visual featured analysis with k share analysis is provided to save the information from intruders. The secret image analysis with the featured behavior analysis was provided to keep the preserved information. The secret image processing at multiple shares is provided to keep the stacked information. The rotation robust cryptography is provided in this work. Babu et. Al. [12] has provided a work on secret information processing by keeping the computation information contents for natural images. The visual information was preserved and the final resultant image was generated by applying the pseudo random pixel reversal method. The pixel difference analysis was provided here to keep the secret contents and by reducing the pixel expansion extensively. Tharayil et. al.[13] has provided a work on visual content encryption using a complex cryptographic formulation to generate the multiple shares. The distributed information processing and the vitality of the information content was used to generate the relative information share. The encryption technique here used is based on inter-pixel exchange applied to the secondary image. The block content analysis with the error filtration was provided to generate the encoded information image. The hybrid data scanning and error diffusion was provided to reduce the collective impurities from the image. The method improved the content recovery by applying the six share method. Cimato et. al.[14] has defined a work on color specific optimization method for encoding the image based on visual contents. The pixel expansion along with the threshold approach was applied to generate the symmetry properties of the image. The cannonial information processing was applied to encode the image by using the subpixel division method. The pixel merges with base matrix was applied to generate the color preserved encoded image. Wang et. al.[15] has applied the error diffusion method to identify the share interference analysis under the quality and contrast measures. The feathered phenomenon was applied to generate the structured image and provided the cross interference analysis to generate the encoded visual image.

III. VISUAL CRYPTOGRAPHY METHODS AND MODELING

Visual cryptography is applied on different images and on different application forms for encoding the image information. It can be applied on different image formats with block specific shares. The encoding in stacked format can be applied to generate the encoded structure. The visual cryptography method based on the matrices

can be applied for generating the image. The visual cryptography is a structure specific method which can be applied to observe the structural information. This structural information is defined as the cryptography matrices.

A) Matrices

The cryptogrpahy scheme can be applied on image pixel with specification of binary contents. The sub pixel specification based shared information processing is defined to process each share. The requirement specification based matrix analysis is applied based on the pattern specification. The matrices level estimation and analysis is applied with different parameter specification to generate the relative encoded share. The parameters associated with two shares called S0 and S1 are listed here under

- The method is defined with specification of vector V respective to n rows and k shares
- The logical operations are applied on these share to apply the relative switching and merging so that the encoding will be performed.
- The matrices must be defined to restrict each share in the limited size and by applying the column driven permutation.
- The weight specific analysis can be applied to preserve the information contents and to avoid the information loss.
- The specific or the random patterns can be applied over the image to generate the relative differnces to achieve the pixel expansion.

B) Boolean Based Visual Cryptography

The visual cryptography on a secret image can be applied by dividing the image in two different shares to represent each participant. Each of the participants is allocated by the specific m pixels or the share of each pixel with bit specification. The share binary images called S1 and S2 can be generated from the image. The color specific information processing with random pixel processing can be applied to generate the shared encoded image. Here the share specific encoded image using the subpixel processing is shown here in figure 2.

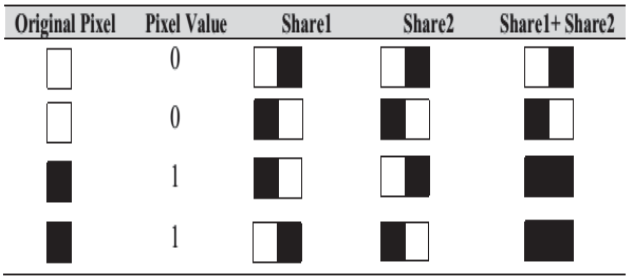

Figure 2 : Boolean Based Visual Cryptography

The figure here sharing two differnt shares called S1 and S2 based on the random pixel selection with equal number of black and white pixels. The recoved secret image can be composed using the sub pixel expansion. The difference and contrast specific encoding image can be generated from the image. The share specific encoding with random switch of pixel can be applied to generate the encoded image.

C) Squared Pixel Expansion Method

The pixel expansion in the secret image not only increase the image size but also increases the chances of distortion. To avoid such horizontal and vertical distortion, the segmented sub pixel group based encoding can be applied. The sub pixel layout based sharing is here applied to generate the size specific sharing. The reconstructed image can be generated by avoiding the distortion. The change specific analysis can be applied on the origional image to generate the specific encoded image. The share speific encoded image can be obtained by keeping the size of share indentically same. The matrix level computation can be applied to generate the single share to generate the result encoded share.

IV. CONCLUSION

In this paper, a study to the visual cryptography methods and characterization is provided. The paper discusses the based method and constraints of visual cryptography. The paper has identified the associated matrics and defined the common methods of visual cryptography.

REFERENCES

[1] Zhi Zhou, G. R. Arce and G. Di Crescenzo, "Halftone visual cryptography," in IEEE Transactions on Image Processing, vol. 15, no. 8, pp. 2441-2453, Aug. 2006.

[2] M. Desiha and V. K. Kaliappan, "Enhanced efficient halftoning technique used in embedded extended visual cryptography strategy for effective processing," Computer Communication and Informatics (ICCCI), 2015 International Conference on, Coimbatore, 2015, pp. 1-5.

[3] N. S. Alex and L. J. Anbarasi, "Enhanced image secret sharing via error diffusion in halftone visual cryptography," Electronics Computer Technology (ICECT), 2011 3rd International Conference on, Kanyakumari, 2011, pp. 393-397.

[4] Jaya, S. Malik, A. Aggarwal and A. Sardana, "Novel authentication system using visual cryptography," Information and Communication Technologies (WICT), 2011 World Congress on, Mumbai, 2011, pp. 1181-1186.

[5] H. Yanyan, C. Xiaoni, Y. Dong and H. Wencai, "VVCS: Verifiable Visual Cryptography Scheme," Computational Intelligence and Security (CIS), 2011 Seventh International Conference on, Hainan, 2011, pp. 974-977

[6] J. Ramya and B. Parvathavarthini, "An extensive review on visual cryptography schemes," Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on, Kanyakumari, 2014, pp. 223-228.

[7] P. V. Chavan and M. Atique, "Design of hierarchical visual cryptography," 2012 Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, 2012, pp. 1-3

[8] I. Kang, G. R. Arce and H. K. Lee, "Color Extended Visual Cryptography Using Error Diffusion," in IEEE Transactions on Image Processing, vol. 20, no. 1, pp. 132-145, Jan. 2011.

[9] N. Askari, H. M. Heys and C. R. Moloney, "An extended visual cryptography scheme without pixel expansion for halftone images," Electrical and Computer Engineering (CCECE), 2013 26th Annual IEEE Canadian Conference on, Regina, SK, 2013, pp. 1-6.

[10] T. Monoth and B. A. P., "Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns," Cyberworlds (CW), 2010 International Conference on, Singapore, 2010, pp. 171-178

[11] L. J. Anbarasi, M. J. Vincent and G. S. A. Mala, "A novel visual secret sharing scheme for multiple secrets via error diffusion in halftone visual cryptography," Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, Chennai, Tamil Nadu, 2011, pp. 129-13

[12] R. Babu, M. Sridhar and B. R. Babu, "Information hiding in gray scale images using pseudo-randomized visual cryptography algorithm for visual information security," Information Systems and Computer Networks (ISCON), 2013 International Conference on, Mathura, 2013, pp. 195-199

[13] J. J. Tharayil, E. S. K. Kumar and N. S. Alex, "Visual cryptography using hybrid halftoning and inter-pixel exchanging," Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on, Bhopal, 2012, pp. 1-5

[14] S. Cimato, R. De Prisco and A. De Santis, "Contrast optimal colored visual cryptography schemes," Information Theory Workshop, 2003. Proceedings. 2003 IEEE, 2003, pp. 139-142

[15] Z. Wang, G. R. Arce and G. Di Crescenzo, "Halftone Visual Cryptography Via Error Diffusion," in IEEE Transactions on Information Forensics and Security, vol. 4, no. , pp. 383-396, Sept. 2009