IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Secret sharing scheme Circular Visual Cryptography for Color Images - Survey

[1*]Sudhir Parmar, [2]Sheshang D Degadwala, [3]Nimit Modi

[1, 2, 3]Computer Engineering Department, Sigma Institute of Engineering, Vadodara, Gujarat, India

Available online at: www.ijcseonline.org

Accepted: 16/Nov/2018, Published: 30/Nov/2018

Abstract**—** Information Security ensures mathematical techniques and related aspects to provide for confidentiality, data security, entity authentication and data origin authentication. Visual cryptography is a new technique which provides information security using simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows visual information to be encrypted in such a way that their decryption can be performed by the Human Visual System (HVS), without any complex cryptographic algorithms. Circular Random Grids extends the functionality by hiding more data in circular grids to provide confidentiality and secrecy without risking suspicion of an intruder. The proposed scheme complies with the methodology of secret sharing scheme where secret information is divided into various shares in meaningless form and is further recovered on overlapping printed transparencies with the shared information on it. Each of them is then validated for authenticity. An attempt has been made to use circular rings to embed the secret information with certain angular rotation and validation of the individual cipher shared in order to avoid cheating. In this paper we are describe every methods of VCS and presented its comparative study using advantages and disadvantages.

Keywords**—** Visual cryptography, Random grid, Circular girds, Q'tron neural networks traditional visual cryptography, circular visual cryptography, hierarchical visual cryptography.

I. INTRODUCTION

The current trend in Information Technology is highly dependent on the communication among devices like high end Server & Commodity client machines, hand held devices, notepads and tablets, house hold gadgets and appliances including various other things (Internet of Things) [1]. In order to ensure that the data transfer over these networked devices are safe and secure, the Network Security services must abide by the authorization of access to the data over a network such as authenticating both the Information & User, maintaining confidentiality of the message that is transmitted over the communication channel, and also ensuring that Data Integrity is maintained throughout the sender & receiver's data. VC is a unique technique in the sense that the encrypted message can be decrypted directly by the human visual system (HVS). The shares are a random collection of noise. The decoding can be done visually by overlaying all the defined or defined threshold number of shares. An expert cryptanalyst even cannot decode the secret with lesser than the threshold values of shares. However, this technique suffers from the following drawbacks:-

i. Pixel Expansion resulting in an increased size of the encrypted shares thereby generating greater traffic.
ii. Only one secret image can be encrypted.
iii. Requirement of a complex codebook to generate the cipher text.

Section I contains the introduction of basic approach for weather forecasting. II contain the related works of basic literature papers. Section III contain the methodology and algorithms section IV explain the comparative study between different algorithms and at last conclusion and future scope.

II. RELATED WORK

Sandeep Gurung, Mrinaldeep Chakravorty, Abhi Agarwal, M K Ghose Visual cryptography is a new technique which provides information security using simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows visual information to be encrypted in such a way that their decryption can be performed by the Human Visual System (HVS), without any complex cryptographic algorithms. Circular Random Grids extends the functionality by hiding more data in circular grids to provide confidentiality and secrecy without risking suspicion of an intruder. The simple 2:2 secret sharing scheme is extended to hide more than one secret message. Thus a high data capacity is also achieved in the proposed scheme. Generation of circular random grids which correspond to the rectangular grids generated. The circular shares are rotated at multiple angles using one of the grids as a basis to hide more secret information. Both confidentiality and authentication can be achieved by this method of encryption. The project can be extended further to incorporate the encryption of gray scale and colored images rather than just binary images. [1]

Sandeep Gurung, Bijoy Chhetri, Mrinal Kanti Ghose , The proposed scheme complies with the methodology of secret sharing scheme where secret information is divided into various shares in meaningless form and is further recovered on overlapping printed transparencies with the shared information on it. Each of them is then validated for authenticity. An attempt has been made to use circular rings to embed the secret information with certain angular rotation and validation of the individual cipher shared in order to avoid cheating. Cryptography turns out to be the trusted brand in the computer science fraternity and Visual Cryptography, as one among this, is a methodology where the secret recovery is done with human visual system without having to perform complex calculations. This is consequently a proposed scheme which incorporates, multiple secret information being embedded in the shares, in a meaningless way. These shares can recover the secret by overlapping them together and the subsequent secrets are revealed by rotation of the shares to certain predefined angles. The proposed system also has the authentication of each individual shares which can be done to uphold the security criteria of Network transmission. [2]

Tzung-Her Chen, Kuang-Che Li, Visual secret sharing (VSS) can encode a secret image into several share images where the original secret can be reconstructed and recognized by sight by stacking all share images. This paper proposes a novel RG-based VSS scheme that encodes multiple secret images at a time. The scheme encrypts multiple secret images into two circular cipher-grids and decrypts the images by stacking two circular cipher-grids to obtain the first secret and gradually rotating one circular cipher-grid at a fixed degree (based on the quantity of the secret images encrypted) to disclose other secrets. Compared with conventional VC-based VSS, the proposed scheme has no pixel expansion, a higher capacity for secret sharing, and no need for a complex VC codebook to be redesigned. This paper proposes a novel RG-based VSS scheme with the capability of encrypting multiple secret images at once into only two circular cipher-grids. To decrypt all secrets, decoders stack the two circular cipher-grids to disclose the first secret and then gradually rotate one circular cipher-grid at a fixed degree to reveal the second. Theoretical analysis demonstrates the accuracy and security of the proposed method. [3]

Sandeep Gurung and Mrinaldeep Chakravorty, Visual cryptography, an example of a secret sharing scheme encrypts the secret digital information into a number of shares wherein the decryption is performed by overlaying the shares generated and by utilizing the HVS (Human Visual System). General access structures efficiently hides the data by defining an access structure of qualified sets which only can produce the hidden information. Since no transmission is noise free, quantum neural network is used to extract the original information even when the information is not clearly visible to the human eye. The paper proposes a methodology to conceal multiple secret in a pair of shares and the Q'tron network to improve the security of information systems. The systems generate circular random grids without pixel expansion to conceal the angular orientation and also hides compound secret information. The mechanism achieves confidentiality of data and authentication of the end users. The ideology can be upgraded to incorporate encryption of grayscale and colored images. Codebook needless: Traditional approaches fulfill the access schemes of visual cryptography using codebooks. For complex access schemes, a codebook is hardly to be found and/or not existent. Generality: The approach is very general and, hence, can be used to fulfill any access scheme for visual cryptography. [4]

Shyong Jian Shyu binary or color secret image shared by a set of n participants with a strong access structure, we devise two effective algorithms to produce a set of VCRG so that the members in each qualified set can reconstruct the secret image by superimposing their shares, while those in any forbidden set cannot. Our algorithms do not require any extra pixel expansion, which is indispensable and grows exponentially as n increases in conventional visual cryptographic schemes. The feasibility, light contrasts, flexibility, and limitations of our algorithms are explored from both theoretical and empirical points of view. The approach of VCRG relieves the concern of pixel expansion, yet its reconstruction ability is not flawless as VCS (which flawlessly reconstructs each white and each black pixels without any misperception from the visual sense) due to the reason that a quite small white region might be mis reconstructed as black. Therefore, it is not appropriate to deal with those secret images whose critical information is characterized by very small white regions.[5]

III. Methodology

A. *Random Grid :*

The concept of Random Grid based VC was introduced by Kafri & Karen[7] where a reference grid is generated with each pixel in the grid chosen randomly such that the number of transparent pixels (white) is probabilistically equal to that of opaque pixels (black) and also ensured that the size of secret image and the grid are same. Every pixel is either transparent or opaque.

Transmission of light through these chosen pixels is random. Opaque pixels block out light whereas transparent pixels allow light to pass through. The number of white pixels is approximately equal to the number of black pixels making its average light transmission as half. This scheme of encrypting the images is in a way similar to one-time pad techniques, which adds to its security.This idea was proposed with three different algorithms for generation of shares using Random Grid as a reference Grid as shown in Fig 1.

B. Multi Information Hiding

The problem with random grids is that it is only possible to encrypt a single image. However this concept was extended to encrypting two images by Chen et al [5] in which the two different hidden images were obtained by stacking the shares on top of each other and then rotating the grids. For this, the user was required to possess both the grids as well as the knowledge about the angle of rotation for which the images would be obtained. The limitation in this scheme was that the angle of rotation to obtain the second secret image could either be 90, 180 or 270 degrees as the grids were rectangular in shape; also the idea included pixel expansion to implement the scheme. Since there were only three available options, an intruder could easily decrypt the information simply by using Brute- Force technique. However, the geometric configuration of the shares can be exploited to increase the amount of information being hidden by exploring the spatial domain with share representation in a Circular, Cylindrical, Cubical or Spherical orientation.

C. Circuler VCS

The innovation and idea of multiple secret hiding also started with the method of hiding secrets recursively. In recursive hiding of secrets, several additional messages can be hidden in one of the shares of the original secret image, thereby, making reduced network load during information transmission. Also proposed an idea of hiding multiple secrets using recursive hiding in Circular Share.

The basic idea behind recursive threshold VC such that a bit of share conveys to (n-1)/n bit of secret which is sufficient to reveal the secrets while superimposing.

Step 1: Read Binary data row-col MxN matrix

Step 2: Make Column MN matrix

Step 3: Make Circular Mask

Step 4: Fill with Binary Column matrix

Step 5: Apply VCS

Step 6: Generate Shares

Step 7: Combine Shares using EXOR

The circular grids are gradually rotated to reveal the multiple pixels. The multiple secret sharing is also incorporated in the scheme proposed by H C Wu et al [20] and Shyu et al [17], where, circular share with multiple information hiding is done with pixel expansion and later improvised by T.H Chen et al [12, 13] with the usage of random grid. In the progression of such research activities various schemes were proposed to enable (2,n) [15] (k,n) [21], (n,n) [8,13]. All of these mentioned proposals incorporate random grid implementation. Another proposal by Jeane Chen et al [22] used fixed angle segmentation with inner ring & outer ring of the circular representation to hold two secrets. As the limitation of VC always lie on the fact that the quality of recovered image is not 100% satisfactory, the human visual system always fails to obtain the contrast as good as the original secret image.

IV. COMPARATIVE STUDY

Table I. Comparison between Classification Extraction Method

Method	Advantages	Limitation
Simple VCS	Works with binary data. Easy to implement	Not works for grey or colour data. Even combination is possible ex: 2,4 or 8.
Random Grid VCS	No codebook design is required, modularity. Fast computation.	Pixel Exaptation Present so more Space require. Original image n secrete image size different
Circular Random Grid VCS	Works Without pixel expansion. Codebook require for pattern. Progressive is possible to hide in cover.	Complex Calculation

V. CONCLUSION AND FUTURE SCOPE

After review different types of Visual cryptography approaches we can conclude that future research presents the first ever attempt for security of image using circular approach. In that we can use propose visual approach with CVS scheme. Also work for binary, grey and Color images.

REFERENCES

[1] Sandeep Gurung and Mrinaldeep “ChakravortMultiple Information Hiding in General Access Structure Visual Cryptography Using Q’tron Neural Network”. Springer-2018[1]

[2] Abhishek Mishra & Ashutosh Gupta “ Multi secret sharing scheme using iterative Method”. 12 Apr 2018 Elsevier[2]

[3] Bibhas Chandra Das, Md Kutubuddin Saradr, Avishek Adhikari “Efficient Constructions for t-(k; n)-Randon Grid Visual Cryptographic Schemes”. 2017 IEEE[3]

[4] Tzung-Her Chen , Kuang-Che Li “Multi-image encryption by circular random grids”. 2009 Elsevier[4]

[5] Sandeep Gurung, Mrinaldeep Chakravorty, Abhi Agarwal, M K "Multiple Information Hiding using Circular Random Grids".2015Elsevier[5]

[6] Sandeep Gurung, Bijoy Chhetri, Mrinal Kanti Ghose "A Novel approach for Circular Random Grid with Share Authentication". 2015 IEEE[6]

[7] S. D. Degadwala and S. Gaur "Metadata of the chapter that will be visualized in SpringerLink". Springer-2018[7]

[8] Shyong Jian Shyu " Visual Cryptograms of Random Grids for General Access Structures". 2012 IEEE[8]

[9] Sandeep Gurung,Gaurav Ojha,M K Ghose " Multiple Image Encryption using Random Circular Grids and Recursive Image Hiding". May 2013 IJETAE[9]

[10] Sandeep Gurung, Mrinaldeep Chakravorty, Abhi Agarwal, M K Ghose "Multiple Information Hiding using CircularRandomGrids".2015Elsevier[10]

Authors Profile

Mr. Sudhir Parmar have completed my bachelor from Parul institute in computer & science in 2016. His area of interest in image processing. Working on image privacy and security algorithms. Pursuing master in computer engineering from sigma institute of engineering, bakrol, Vadodara. Area of interest in Visual cryptography.

Dr. Sheshang D. Degadwala Completed Ph.D. in Computer Engineering from Madhav University, Abu Road, Sirohi, Rajasthan, India in year 2018. He is currently working as Head of Computer Engineering Department in, Sigma Institute of Engineering, Vadodara, India since 2012. He has published more than 58 research papers in reputed international journals and 3 in National conferences including Thomson Reuters and conferences including IEEE, Springer and it's also available online. His main research work focuses on Image Processing, Information Security and Data Mining. He has 6 years of teaching experience and 6 years of Research Experience.

Mr. Nimit Modi, Assistant Professor Department of Computer Engineering ,Sigma Institute of Engineering,Vadodara,Gujarat B.E in Computer Engineering 2010 M. E in Computer Engineering -2013 Published 6 research paper in IJSRSET journals and conference Area of interest :Mobile ad-hoc network and wireless communication, cloud computing.