Encrypting Binary and Gray-scale Images Using RandomCircular Visual Cryptography

[1]Dr. Brijesh Kumar Bhardwaj, [2]Tanu Singh, [3]Kiran Gupta, [4]Hariom Pandey and [5]Anupam Tiwari

[1]Associate Professor MCA, [2,3,4,5]Research Scholar MCA

[1,2,3,4,5]Dr. Ram Manohar Lohia Avadh University Ayodhya U.P.

Email : [1]wwwbkb2012@gmail.com, [2]singhtanu8932@gmail.com, [3]9335kiran@gmail.com, [4]hariompandeyhari312@gmail.com, [5]anupamt158@gmail.com

ABSTRACT

Information security is the most important part in the research and development area, government, industry, organization, etc. Recently, cybercrime or related hacking problems have increased more and more. So, high security is required to secure the information and/or image. Visual Cryptography Scheme (VCS) is one of the techniques to secure information using a simple algorithm, while some other security techniques use complex algorithms. VCS has a simple encryption algorithm which secures information by converting it into different shares, and the decryption process does not require any type of devices or any complex decryption algorithm. The decryption process is done using the Human Visual Scheme (HVS). Circular Random Grid extends its functionality by securing more information in a circular grid to provide confidentiality. In the proposed scheme, the methodology of the secret sharing scheme is that secret information is divided into various shares in meaningless form and is further recovered by overlapping these various shares using HVS. In this research, we describe every method of VCS and present its comparative study using advantages and disadvantages.

KEYWORDS

Visual Cryptography Scheme (VCS); Random Grid; Secret Sharing Scheme; XOR operation; Circular Random Grid.

INTRODUCTION

To improve the existing system, which provides high security against hackers, the proposed system will be applied to secure information. Nowadays, cybercrime is at the top position, posing a significant challenge for upcoming research. Therefore, providing security for confidential data is a prime requirement. The main goal of network security policy is to ensure security and enable information to reach the correct receiver without any interference through several weak communication channels and unprotected links.

On networked devices, data transfer is more secure. Network security services must control access to data on the network, authenticate both the information and user, maintain the confidentiality of messages transmitted over the communication channel, and ensure data integrity between senders and receivers.

In today's technology, the battle to protect confidential data is intensifying by the hour. Many techniques, such as cryptography and image steganography, have been developed to address this challenge. Cryptography requires special decryption devices, while steganography conceals the presence of data.

Visual cryptography plays a crucial role in meeting today’s security needs. However, when there is significant pixel expansion, the visual quality of the resultant image degrades, resulting in a large, reconstructed image that is undesirable.

To increase the security level, the Circular VCS Scheme will be used. Secure binary, gray, and color images with the proposed random grid-based visual cryptography. The image will be divided into a (2, n) share scheme (i.e., 2, 4, 8, 16) using hierarchical circular visual cryptography. This approach aims to improve the PSNR and MSE values for recovered data.

RELATEDWORK

S. Gurung and M. Chakravorty [1], in their paper, propose a methodology to hide multiple secret information in a pair of shares using QNN to improve the security of the secret information. The General Access Structure (GAS) is used to hide the data. Their methodology involves a Circular Random Grid, where multiple pieces of information are hidden using a circular random grid or circular share. This addresses the problem of angular rotation, as the circular grid rotates at various angles to hide the multiple pieces of information without generating a pixel expansion problem. QNN is used to extract the original information from the circular shares even when the information is not clearly visible, ensuring the QNN network does not get trapped in any local minima. The paper encrypts multiple pieces of information into circular shares and decrypts them using the Human Visual System (HVS).

X. Wu and Z.-R. La [2], in their paper, address the pixel expansion problem and provide a flexible sharing strategy. Their proposed method maintains pixel expansion at 1 for different thresholds, whereas other methods see pixel expansion increase with the values of k and n. They use the RG-CBW-VCS algorithm for GAS and apply XOR operation to the color pixel. This system is further extended to realize the Generalized General Access Structure (GGAS), allowing users to assign different probabilities to different minimal qualified sets. The proposed system is validated using various lemmas and theorems, comparing theoretical and experimental values of security and contrast conditions.

X. Wu and C.-N. Yang [3], in their paper, propose a scheme combining CBW-VCS and Polynomial-based Secret Image Sharing (PSIS), including color share generation. Their paper outlines two decryption processes: stacking-to-see and lossless image reconstruction. XOR operation is used to improve visual quality. A grayscale secret image is converted into p-radix and binary images, then encrypted using (k, n) PSIS under mod p (with p = 19). Perfect recovery of the p-radix image is achieved using Lagrange polynomial interpolation, and binary image preview decryption is done by stacking. The proposed method slightly reduces the quality of the recovered image compared to conventional VCS.

R. N. Chaturvedi et al. [5], propose an approach to improve the quality, contrast level, resize the recovered secret image, and reduce noise in the reconstructed image. They use MSE, PSNR, and SSIM parameters to measure the performance of the original and reassembled images. Two methods are used to resize the reconstructed image: linear interpolation and preserving the column and row (1 out of n). Method 1 provides average values for MSE, PSNR, and SSIM, while method 2 gives exact parameter values. Ideal values for binary, gray, and color images are MSE = 0, PSNR = infinity, and SSIM = 1.

A. Mishra and A. Gupta [8], propose a (2, n, m) multi-secret sharing scheme, where n shares are generated to hide m secret images. The proposed algorithm is based on stacking shares, requiring a minimum of two shares to decrypt one secret image, and m+1 or n shares to recover the original secret image. Images are recovered only when shares belong to qualified sets; if shares belong to forbidden sets, reconstruction is impossible. Image reconstruction is done by superimposing these shares, and the alignment problem during decryption is addressed using the XOR operation.

DIFFERENTMETHODOLOGIES

A. CRYPTOGRAPHYSCHEME

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. There are various types of algorithms for encryption, including:

Secret Key Cryptography (SKC): This type of encryption, also referred to as symmetric encryption, uses a single key for both encryption and decryption.

Public Key Cryptography (PKC): Also known as asymmetric encryption, this type uses two keys: a public key that anyone can access and a private key that only the owner can access.

Hash Functions: Unlike SKC and PKC, hash functions use no key and are also called one-way encryption. They are primarily used to ensure that a file has remained unchanged.

Keys have had to become longer over the years. While the limit was once 40 bits, today's cryptographic key lengths can be up to 4096 bits.

B. VISUALCRYPTOGRAPHYSCHEME (VCS)

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted using an encoding system that can be decrypted by eyes. It does not require a computer for the decoding. Types of VCS: (2, 2) VCS, (K, N) VCS, (N, N) VCS.

Traditional VCS, Random Grid VCS, and XOR-based VCS.Traditional VCS is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system.

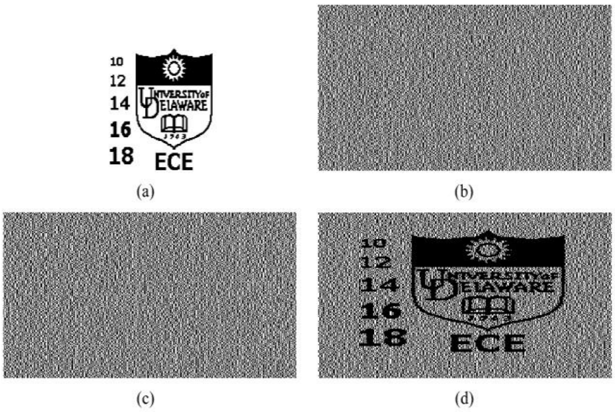

Fig.1. Exampleofatwo-Outof-Two VCS

Random Grid VCS is a random grid that encrypts secret information into 2D arrays of transparent and opaque pixels. The scheme is simple and does not involve any increase in pixel size. Whatever problems are present in Traditional VCS, the same problems are present in Random Grid VCS.

C. Circular Visual Cryptography Scheme

Quantum Neural Network (QNN) is a modified network of the Hopfield neural network, and QNN gives multiple output levels. QNN is based on the local minima escaping capabilities. In general, each Q'tron is self-connected with negative connection strength to provide means for negative feedback. QNN can extract the original information even when it is not clearly visible to the human eye.

Circular Random Grid is a method where two circular shares are required to hide multiple images. One image is hidden in these two circular shares, and then any one circular share rotates at various angles to hide more than two secret images. No pixel expansion problem is generated in Circular Random Grid VCS. It hides multiple pieces of information, and no complex codebook is required. With this methodology, both confidentiality and authentication can be achieved.

PROPOSEDSYSTEM

Proposed system for three types of Images: Proposed system for Binary Image, for Gray Scale Image, for the Color Image. In the proposed system the general approach is to convert the any image into the circular grid and then generate a circular share of that circular grid using circular random grid method after this encryption process starts the decryption process.

The decryption process is to combine the circular shares and getting the original image. In this proposed system first Gary scale image (Decimal, range: 0 - 255) convert into the binary image (Decimal to Binary) then system read this binary image and resize it then generate a grid i.e. square Gary scale image into circular form. Apply the Random grid Circular Visual Cryptography (RCVCS) on the binary image to generate the shares (S1 Grid and S2 Grid).

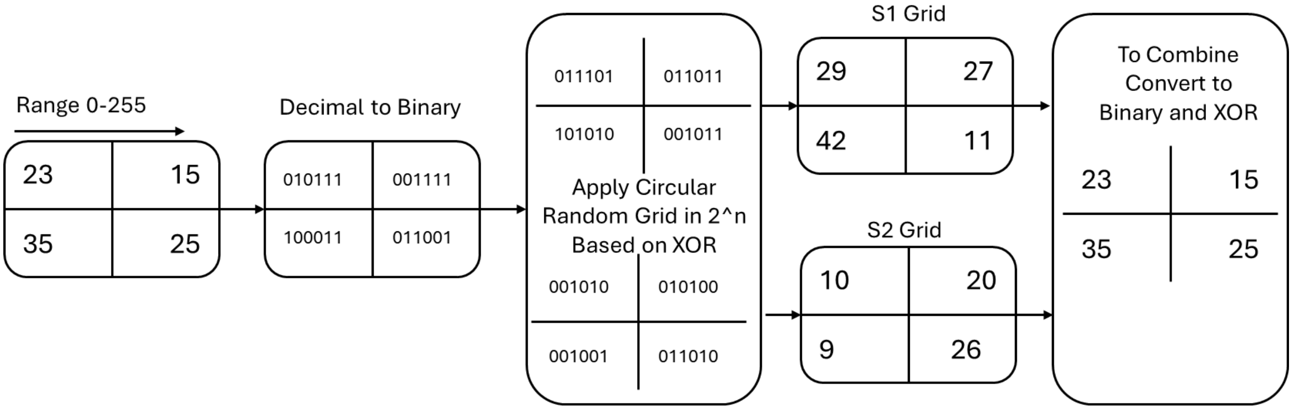

Fig.2. BlockDiagramoftheProposedSystemforGaryscaleImage

After applying this algorithm generates two or more shares. This whole process is encryption process. After completion of encryption process start the decryption process, in decryption process combine these two shares and get the original Gary scale image. Here, XOR gate is used for the pixel expansion purpose.

In the proposed system shares is generated in form of 2^n (i.e. 2, 4, 8…). Pixel expansion process is helpful to secure the image or information. Pixel expansion using OR gate image detection problem is present but Pixel expansion using XOR gate any image can’t detected by un-authentication user.

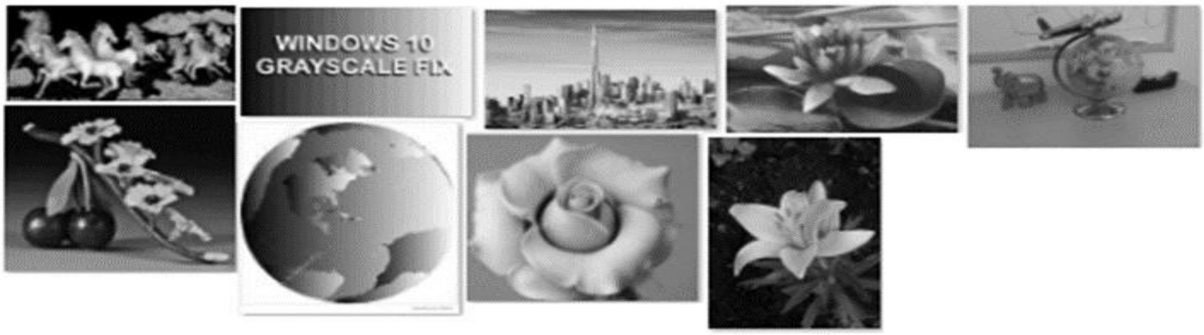

Fig.3. DatasetoftheGrayImage

RESULTSANDANALYSIS

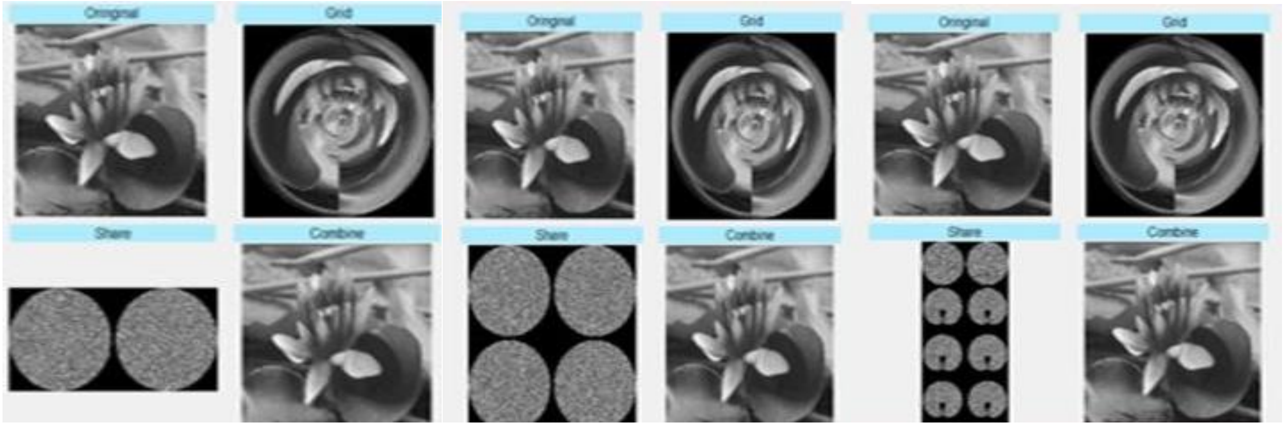

Fig.4. 2,4,8 -ShareGenerationgray

CONCLUSION

As From the Results Conclude that proposed system can generates 2^n shares combination for binary image while existing system work with only 2 and 4 share combination. In Existing system data disclose when 2 or more shares combine. The proposed system gives the higher value of PSNR and MSE as compared to the existing system. XOR operation gives a better result than the OR operation. In proposed system getting a better result than the existing system. So, in future proposed share generation will apply on color image, the security of the system will increase. And Improve PSNR and MSE parameters.

REFERENCES

[1]S. Gurung and M. Chakravorty, "Multiple Information Hiding in General Access Structure Visual Cryptography Using Q'tron Neural Network", Advances in Intelligent Systems and Computing, Vol. 706, pp. 385 – 394, 2018.

[2] X. Wu and Z.-R. Lai, "Random Grid based Color VCS for Black and White Secret Images with General Access Structure", Signal Processing: Image communication, Vol. 75, pp. 100-110, 2019.

[3] X. Wu and C.-N. Yang, "A Combination of Color-Black-and-White Visual Cryptography and Polynomial based Secret Image Sharing", Journal of Visual Communication and Image Representation, Vol. 61, pp. 74 – 84, 2019.

[4] Z. Fu, Y. Cheng and B. Yu, "Perfect Recovery of XOR-based Visual Cryptography Scheme", Information Engineering University, Vol. 78, no. 2, pp. 2367 – 2384, 2018.

[5]R. N. Chaturvedi, S. D. Thepade and S. N. Ahirrao, "Quality Enhancement of Visual Cryptography for Secret Sharing of Binary, Gary and Color Images", IEEE Conference on Computing Communication Control and Automation, 2019.

[6] B. Yan, Y. Xiang and G. Hua, "Improving the visual quality of size invariant visual cryptography for grayscale images, IEEE Transaction on Image Processing, Vol. 28, no. 2, pp. 896 – 911, 2019.

[7] Z. Fu, Y. Cheng, S. Liu and B. Yu, "A New Two-Novel Information Protection Scheme based on Visual Cryptography QR Code with Multiple Decryption", Journal of Measurement, Vol. 141, pp. 267 – 276,2019.

[8] A. Mishra and A. Gupta," Multi secret sharing scheme using iterative method", Information and Optimization Sciences, Vol. 39, pp. 631 – 64,2018.

[9]S. Sridhar & G. F. Sudha," Circular meaningful shares based (k, n) two in one image secret sharing scheme for multiple secret images", Electronics & Communication Engineering, Vol. 77, pp. 28601 – 28632,2018.

[10]S. Gurung, A. Agarwal, M. Chakravorty, M. K Ghose," Multiple Information Hiding using Circular Random Grids", Intelligent Computing, Communication & Convergence, Vol. 48, pp. 65 –

72, 2015.

[11] S. Gurung, B. Chhetri, M. K. Ghose." A Novel approach for Circular Random Grid with Share Authentication", Advances in Computing, Communications and Informatics, IEEE conference, 2015.

[12] T - H. Chen, K. – C. Li," Multi-image encrypt -ion by circular random
grids", Computer Science and Information Engineering, Vol. 189, pp.
255 – 265, 2012.

[13]S. D. Degadwala and S. Gaur,"4 -Share VCS Based Image watermarkingfor Dual RST Attacks", Computational Vision and Biomechanics, Vol.28, pp. 902 – 912, 2018.

[14] T. W. Yue, S. Chieng,"The semipublic encryption Visual Cryptography Using Q'tron Neural Network", Journal of Network and Computer Application, Vol. 30, pp. 24 – 41, 2007.

[15] X. Wu, W, Sun, "Random grid- based visual secret sharing for general access structure with cheat-preventing ability", Journal of System and Software, Vol. 85, pp. 1119 – 1134, 2012.