ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

Color Image Encryption by Random Circular Visual Cryptography

Varsha H. Borkhatariya
PG Scholar, Electronics & Communication Engineering Department, Sardar Vallabhbhai Patel Institute of Technology, Gujarat, India

Dr. Y. B. Shukla
Head of Department, Electronics & Communication Engineering Department, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India

Dr. S. R. Panchal
Assistance Professor, Electronics & Communication Engineering Department, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India

ABSTRACT

Information security is the most important part in the research and development area, government, industry, organization, etc. Recently, cybercrime or related hacking problem increase more and more. So high security is required to secure the information and/or image. Visual Cryptography Scheme (VCS) is a one of the technique to secure the information using simple algorithm while in some other security technique complex algorithm was used. VCS have a simple encryption algorithm which is secure information converting into the different shares and for the decryption process do not required any type of devices or any complex decryption algorithm. Decryption process is done using Human Visual Scheme (HVS). Circular Random Grid shares is better than the rectangular shares because functionality is increased by secure multiple information in circular random grid to provide the confidentiality. In the proposed scheme, secret sharing scheme is that secret information is divided into various meaning full and meaningless shares and is further recovered by superimposing processing and it is seen by HVS. In this Research we are describe every methods of VCS and presented its comparative study using advantages and disadvantages.

Key Words: Visual Cryptography Scheme (VCS), Random Grid, Secret Sharing Scheme, XOR operation, Circular Random Grid

1.1 INTRODUCTION

To get the improvement in existing system which provides high security against the hacker, proposed system will apply to secure the information. Now a day's cybercrime is at top position which is challenge for upcoming research. So, to provide the security to confidential data is a prime requirement.

In today's technology the war of protecting confidential data is going intense by an hour. Many techniques have been developed to overcome the cybercrime related problem such as Cryptography and image steganography. These are the good scheme where, the former needs special decryption device and the latter never reveals its presence.

Cryptography is a process of encryption and decryption both. Encryption means original text, information or images converted into cipher text or in unreadable form. Decryption process is the reverse of the encryption process. But in traditional cryptography, encryption and decryption process is done by the key. And key is either symmetric or asymmetric algorithm. So in cryptography technique chance to reduce the security [8].

Visual cryptography is a new technique and playing a virtual role as far as today's security needs are concerned. In Visual Cryptography Technique when there is a more pixel expansion then the visual quality of resultant image is degraded as well as it provide very large reconstructed image which is

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

undesired.

In visual cryptography secret image converted in to no. of shares form and these shares distributed into the no. of participants, this is the encryption process and decryption process is done by Human Visual System (HVS) even when noise is included in any reassemble image, no requirement of any type of devices and complex algorithm[1]. This technique is more secure than the cryptography technique.

More security level is increased by the Circular VCS Scheme. To secure Binary, Grey and Color Image with proposed Circular Random grid based Visual Cryptography. To Divide the image into (k, n) Share Scheme (i.e. 2, 4, 8, 16) Using Hierarchical Circular Visual Cryptography. To improve the PSNR and MSE value of for Recover data.

In (k, n) threshold model, generate the n no. of shares and distributed in the participants. If participants combine less than k or k-1 shares then cannot be extract secret image. If and only if combine all the participation or k shares then and then extract the original secret image. Otherwise not possible to extract the original secret image. So in the manner increases the security level of the secret images and /or information.

1.2 RELATED WORK

S. Gurung and M. Chakravorty [1], in this paper proposed system is, methodology to hide the multiple secret information in a pair of shares and use the QNN to improving the security of the secret information and General Access Structure (GAS) is used to hide the data. Methodology is Circular random Grid, multiple information is hiding using the circular random grid or circular share. To address the problem of angular rotation by circular random grid because circular grid rotate at various angle to hide the multiple information. And no pixel expansion problem is generated in this method. QNN is used to extract the original information form the circular shares even when information is not clearly visible and QNN network will not be tapped at any local minima. In this paper encrypt the multiple information into the circular shares and decrypt by the Human Visual System (HVS).

X. Wu and Z.-R. La [2], in this paper to address the pixel expansion problem and to provide the flexible sharing strategy. In proposed method pixel expansion for the different threshold is always 1, in other methods when the value of k and n is increase pixel expansion of method becomes larger. To address above problem RG-CBW-VCS algorithm is used for GAS and XOR operation is applied to the color pixel. Further extends the proposed system to realize the Generalized General Access Structure (GGAS), in GGAS allows the users to assign different probabilities to the different minimal qualified sets. These proposed system proved by using the different Lemmas and Theorems. Also prove the theoretical and experimental value of the security and contrast condition whether both values are nearby or not.

X. Wu and C.-N. Yang [3], in this paper proposed scheme is the combination of the CBW-VCS and Polynomial based Secret Image Sharing (PSIS). Color share generation is also a proposed system. In this paper includes two decryption process: stacking-to-see and lossless image reconstruction. XOR operation is used to improve the visual quality. Gray-scale secret image is convert into the p-radix image and binary image and then encrypt p-radix image by (k, n) PSIS under mod p (in this paper author taking p = 19) operation. For the perfect recovery of the p-radix image is done by using Lagrange polynomial interpolation method and binary image preview decryption is done by stacking. Disadvantage of the proposed method (combination of CBW-VCS and PSIS) is to slightly reduce the quality of recovered image compared to the conventional VCS.

R. N. Chaturvedi et al. [5], in this paper proposed approach is to improve the quality, contrast level,

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

resize the recovered secret image and to reduce the noise which is present in the reconstructed image. In this paper MSE, PSNR and SSIM parameter is used to measure the performance of original image and reassembled image. In this paper two methods are used to resize the reconstructed image one is linear interpolation and second is preserve the column and row (1 out of n). Method 1 gives the average value of the MSE, PSNR and SSIM and method 2 gives the exact value of the parameter. In this paper get the ideal value of MSE, PSNR and SSIM for binary, gray and color images, MSE as"0", PSNR as "infinity", and SSIM as "1".

A. Mishra and A. Gupta [8], in his paper proposed system is (2, n, m) multi secret sharing scheme in this scheme n shares are generated to hide the m secret images and proposed algorithm is based on stacking of shares. Minimum two shares are required to decrypt one secret image i.e. m+1 or n shares are required to recover original secret image. Images are recover only when shares belongs to the qualified sets if shares belongs to forbidden sets then cannot be possible to reconstruct original image. Image reconstruction is done by superimposing these shares. In this paper to address the alignment problem at time of decryption by using XOR operation.

1.3 DIFFERENT METHODOLOGIES

A. CRYPTOGRAPHY SCHEME:

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, some common algorithms include:

Secret Key Cryptography (SKC): Here only one key is used for both encryption and decryption. This type of encryption is also referred to as symmetric encryption.

Public Key Cryptography (PKC): Here two keys are used. This type of encryption is also called asymmetric encryption. One key is the public key that anyone can access. The other key is the private key, and only the owner can access it.

Hash Functions: These are different from SKC and PKC. They use no key and are also called one-way encryption. Hash functions are mainly used to ensure that a file has remained unchanged.

Keys have had to become longer. For many years the limit was 40-bits, but today we are seeing up to 4096-bit key lengths in cryptography

B. VISUAL CRYPTOGRAPHY SCHEME (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

Theoretical Background: Traditional VCS, Random Grid VCS and XOR based VCS

1. TRADITIONAL VCS:

Visual cryptography 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.

The secret image (a) is encoded into (b) & (c) two shares and (d) is decoded by superimposing these two shares with 50% loss of contrast.

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

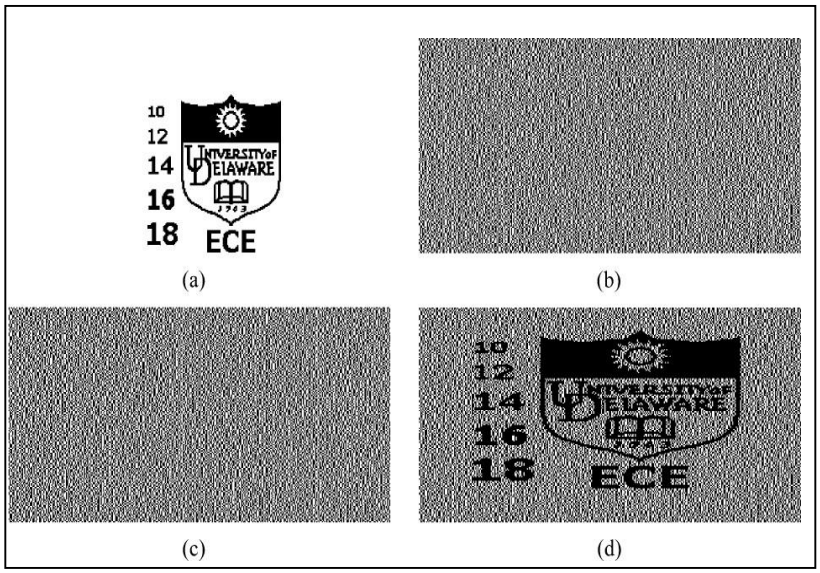

Figure 1: Example of a two-Out of-Two VCS

2. RANDOM GRID VCS:

A random grid encrypts the secret information into 2D arrays of transparent and opaque pixels. The scheme is simple and does not involve any increase in pixel size. Whatever problem is present Traditional VCS same problem is present in random grid VCS.

C. CIRCULAR VISUAL CRYPTOGRAPHY SCHEME:

1. QNN

Quantum neural network (QNN) is a modified network of the Hopfield neural network and QNN gives multiple outputs 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. To extract the original information with the help of the QNN even when the information is not clearly visible to the human eye.

2. CIRCULAR RANDOM GRID VCS

In this method there are two circular shares are required to hide the multiple images. One image is hide in these two circular shares and then any one circular share rotate at various angle and hide more than two secret images. No pixel expansion problem is generate in circular random grid VCS, hide the multiple information and no complex codebook is required. With the help of this methodology, both confidentiality and authentication can be achieve.

1.4 PROPOSED SYSTEM WORK

Proposed system is for three types of Images such as Binary Image, Grey Scale Image and Color Image.

In proposed system general approach is to convert the any image into the circular grid and then generates a circular shares of that circular grid image using circular random grid method after the

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

completion of encryption process starts the decryption process. In decryption process combines the circular shares and generates the original image.

1.4.1 PROPOSED SYSTEM FOR BINARY IMAGES

In this proposed system first read the binary image (INDIA) then after resize the binary image after completion of resize after the resize generate grid i.e. square to circular form. The Random grid Circular Visual Cryptography (RCVCS) apply on circular binary image to generate the shares (S1 Grid and S2 Grid). This whole process is encryption process, to encrypt the binary image after this encryption process start the decryption process, in decryption process combine these two shares and get the original binary image.

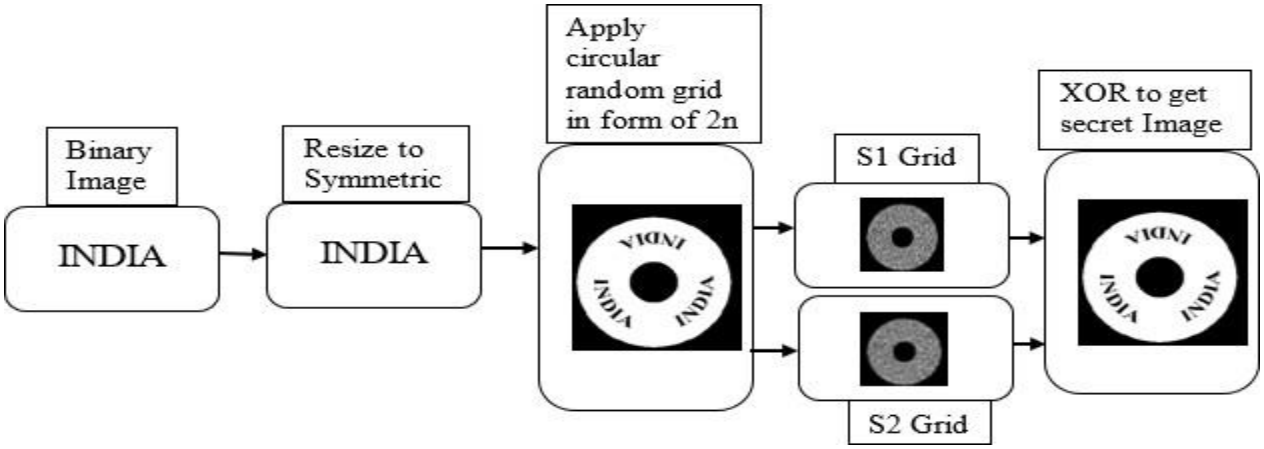

Figure 2: Block Diagram for Binary Image

1.4.1.1 COMPARISON OF EXISTING SYSTEM AND PROPOSED SYSTEM

In this section present the compareson result of existing system and proposed system. This compareson is based on the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Time. PSNR and MSE value of existing system is low compared to the proposed system. In existing system OR operation is used for reconstruct the secret image and in proposed system XOR operation is used for reassemble the secret image. PSNR is mostly used to measure the quality between the original secret image and reassembled secret image. Higher PSNR gives a better quality of the reassembled image. MSE represent the cumulative squared error between the original image and reconstructed image. Lower MSE means lesser error in reassembled image. Ideal value of PSNR and MSE is 'infinitive' and '0' respectively. In proposed system get the ideal or near to the ideal value PSNR and MSE using the Random grid Circular Visual Cryptography Scheme (RCVCS). And take a less time compared to the QNN algorithm or existing system.

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

Parameter	Existing System		Proposed System		Decryption
Algorithm	QNN		RCVCS-Binary, Gray and Color		In existing system only 2 and 4 shares was generated but using proposed algorithm generate 2^n shares (2, 4, 8, 16). Existing system is available only for the binary image but proposed system is available for binary, Gray and color images.
Methods	OR-Random Grid		XOR-Circular Random Grid		If use OR operation it may be possible to extract secret image after share generation but to address above problem XOR operation is used for share generation.
No. of Shares	2	4	2	4	Get the higher PSNR and lower MSE in proposed system compared to the existing system. Ideal value of PSNR and MSE is 'infinitive' and '0' respectively.
PSNR	54.6148	54.5842	Infinity	97.6732	
MSE	0.2247	0.22629	0	$1.1111e^{-05}$	
Time	0.01019	0.05123	0.23439	0.10276	

1.4.2 PROPOSED SYSTEM FOR GREY SCALE IMAGES

In this proposed system first Grey 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 Grey 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).

After applying this algorithm generates two or more shares. This whole process is encryption process after completion of encryption process starts the decryption process, in decryption process combine these two shares and get the original Grey scale image.

Here, XOR gate is used for pixel expansion process. In the proposed system, shares generation is in form of 2^n (i.e. 2, 4, 8…). Pixel expansion process is useful to secure the image or information. If OR gate is used for pixel expansion then secret image cannot be hide properly but this problem is solved by using XOR gate and secret image cannot be detected by any unauthenticated person.

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

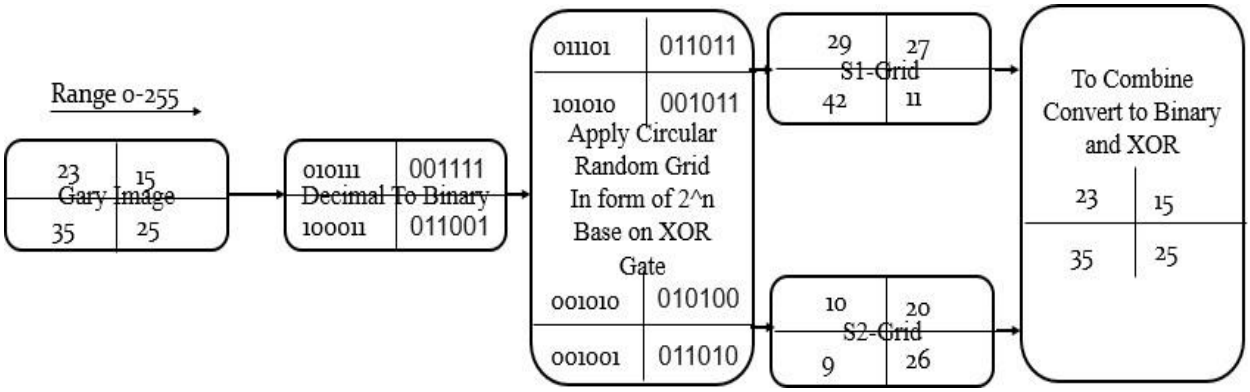

Figure 3: Block Diagram for Grey scale Image

1.4.3 PROPOSED SYSTEM FOR COLOR IMAGES

In this proposed system first extract the R, G and B component from the colour image. This component acts as binary image then system read this binary image and resize it then generate a grid i.e. square colour 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). Two grid for the R component, two grid for the G component and two grid for the R component.

After share generation process combine one grid R1 of R component, one grid G1 of G component and one grid B1 of B component and getting one common gird S11. Repeat same process for another grid and getting another new grid S22. This whole process is encryption process after completion of encryption process start the decryption process, in decryption process again extract the component and combine the grid shares and get the original colour image.

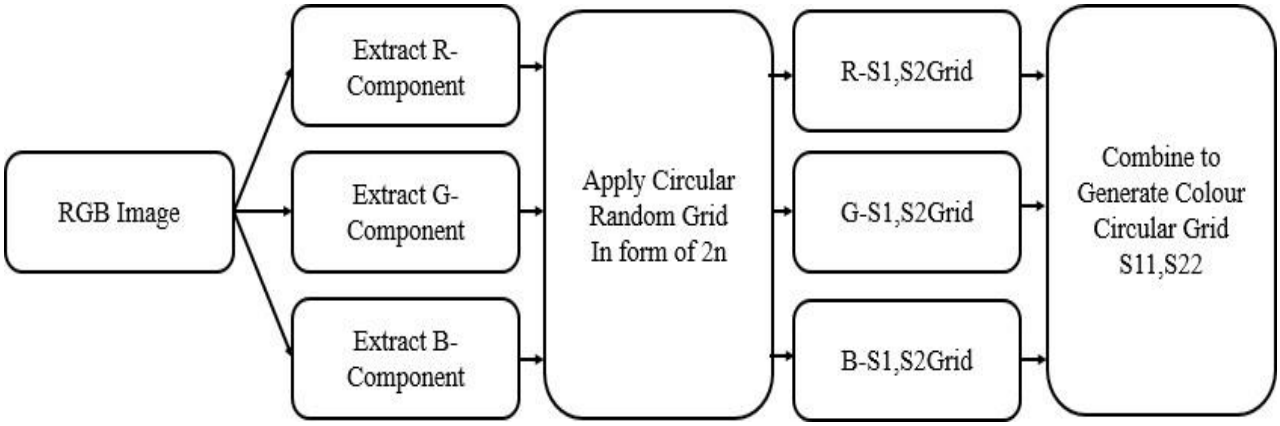

Figure 4: Block Diagram for Color Image

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

1.5 RESULTS ANALYSIS

Result of the Random grid Circular Visual Cryptography algorithm for binary image. Value of the PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Value). Reconstructed image is depends on the PSNR. PSNR value is high, quality of the reconstructed image is also high.

1.5.1 RESULTS OF THE PROPOSED SYSTEM FOR BINARY IMAGE

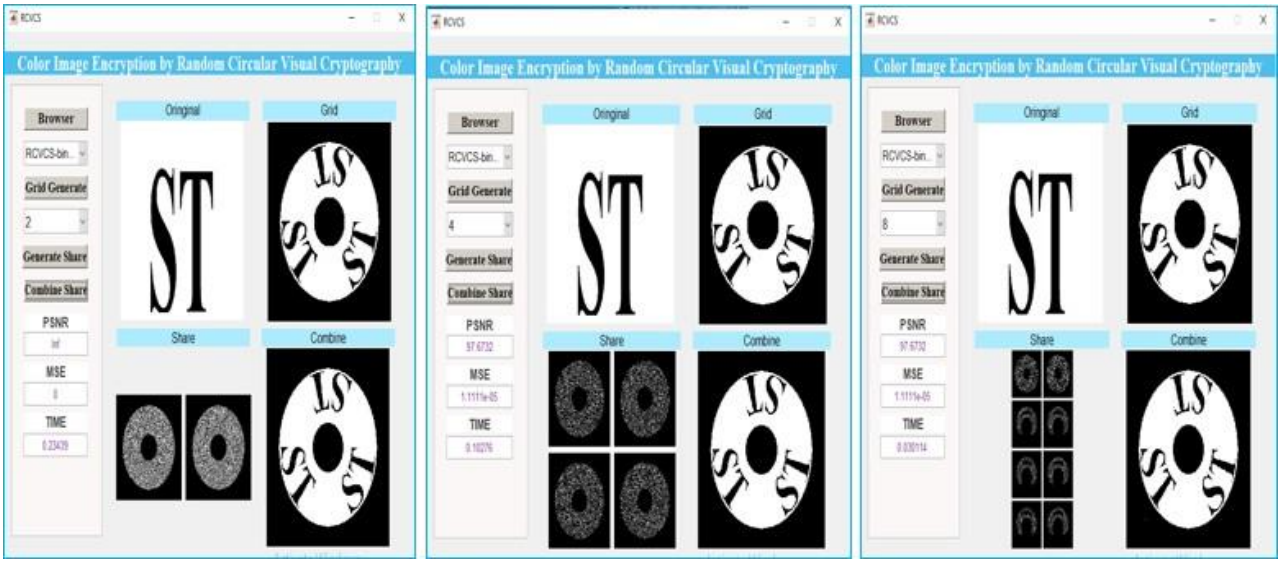

Figure 5: Results of Binary Image

1.5.2 RESULTS OF THE COMPARISON OF EXISTING SYSTEM AND PROPOSED SYSTEM

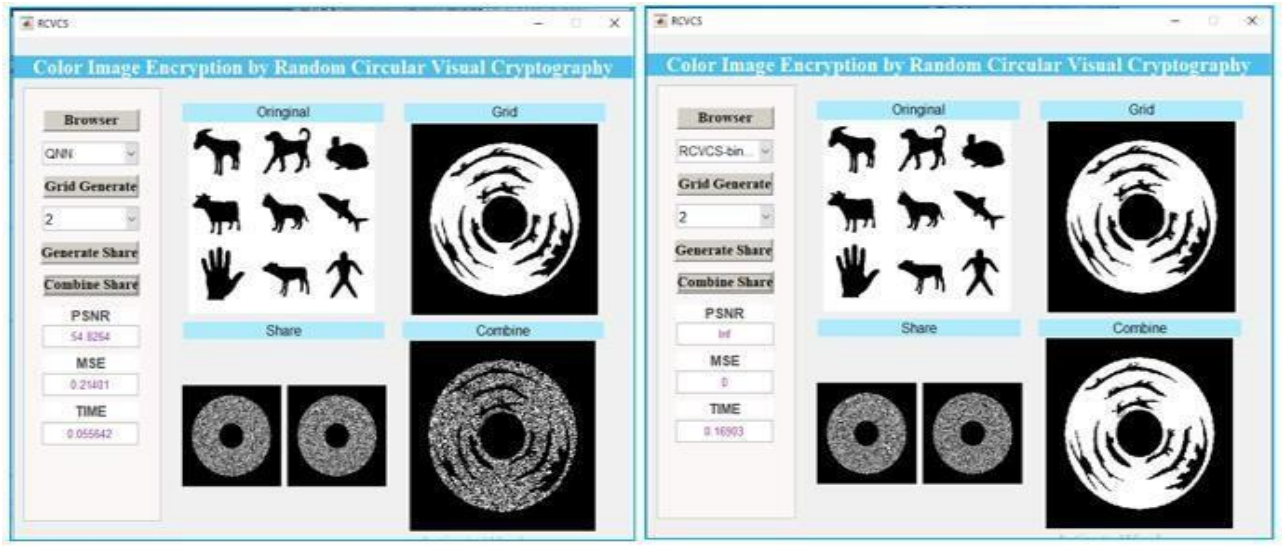

Figure 6: Results of Comparison of the Existing System and Proposed System

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

1.5.3 RESULTS OF THE PROPOSED SYSTEM FOR GREY SCALE IMAGE

Figure 7: Results of Grey Scale Image

1.5.4 RESULTS OF THRE PROPOSED SYSTEM FOR COLOR IMAGE

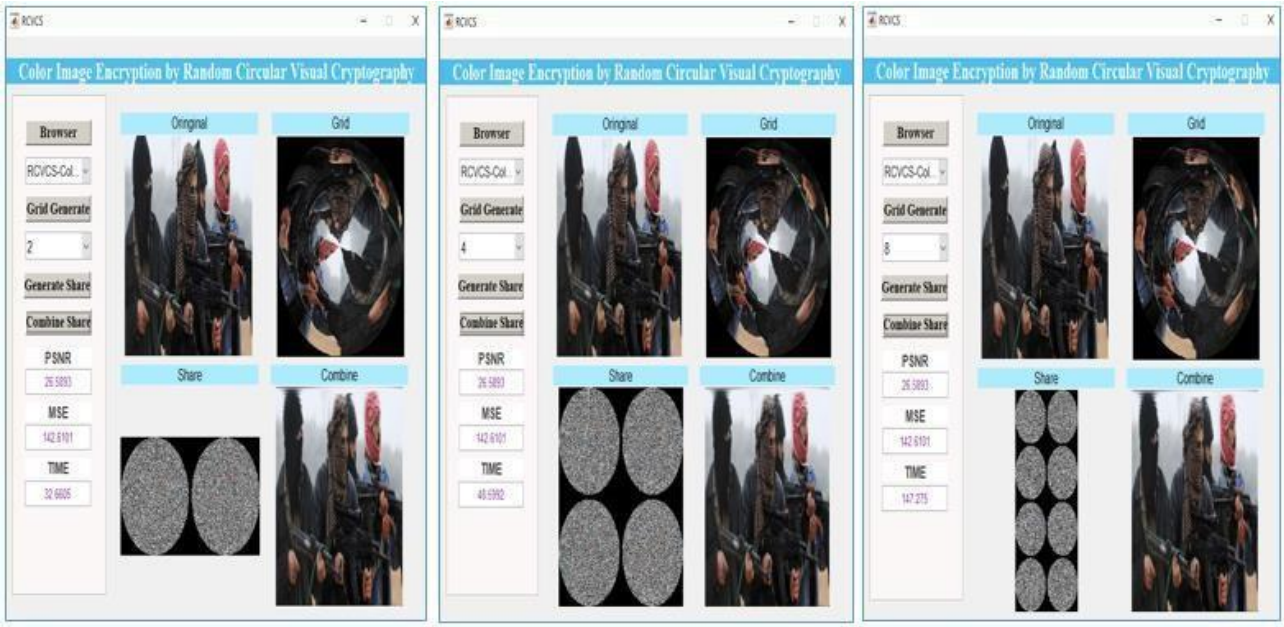

Figure 8: Results of Color Image

1.6 CONCLUSION

In existing system only 2 and 4 no. of shares generation is possible, so this is one of the main reason to reduced security level and this system is only for the binary system. To address this problem, in

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

proposed system shares generation is in form of 2^n, so more no. of shares will be generated and increase security level and it is applied on the binary, gray scale and color images.

Proposed system gives the batter results than the existing system. For binary image, proposed system gives higher PSNR value (PSNR = infinity) and lower MSE value (MSE = 0).

REFERENCES

[1] S. Gurung and M. Chakravorty, "Multiple Information Hiding in General Access Structure Visual CryptographyUsing 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 Visual Cryptography Scheme 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] B. Yan, Y. Xiang and G. Hua, "Improving the visual quality of size-invariant visual cryptography for grayscale images: An Analysis-by-Synthesis (Abs) Approach", IEEE Transaction on Image Processing, Vol. 28, no. 2, pp. 896 – 911, 2019.

[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] 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.

[7] 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.

[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] A. Mishra, Dr. T. Arjariya**, "**Visual Cryptography Techniques-A survey & Comparison", International Journal of Scientific & Engineering Research, Vol. 7, no. 2, pp. 582 – 587, ISSN: 2229-5518, 2016.

[11] 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.

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

[12] 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.

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

[14] 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

[15] Mr. Rohith S, Mr. Vinay G, "A novel Two Stage Binary Image Security System Using (2, 2) Visual Cryptography Scheme", International Journal of Computational Engineering Research, Vol. 2, no. 3, pp. 642 – 646, ISSN: 2250-3005 2012.

[16] F. Baby, Arun R., Dr. S. S. Babu, "Visual Cryptography Schemes for Security (An Overview of Different Types of Visual Cryptography Schemes)", International Journal of Computer Engineering, p-ISSN: 2278 – 8727, pp. 15 – 18, 2016

[17] Soheila Omer AL F. M. Koko et al., "Comparison of Various Encryption Algorithm and Techniques for improving Secured data Communication", International Journal of Computer Engineering, Vol. 17, no. 1, e-ISSN: 2278 – 0661, pp. 62 – 69, 2015

[18] B. C. Das, Md K. Sardar et al., "Efficient Construction for t-(k, n)*- Random Grid Visual Cryptography Scheme", Department of Pure Mathematics, 2017.

[19] T.-W. Yue, S. Chiang, "The Semipublic Encryption for Visual Cryptography using Q'tron neural networks", Journal of Network and Computer Application, Vol. 30, pp. 24 – 41, 2005.

[20] J. Weir, W. Yan, "Visual Cryptography and Its Application", Ventus Publication, ISBN 978-87-403-0126-7, 2012, https://bookboon.com/en/visual-cryptography-and-its-applications-ebook.

[21] "Visual Cryptography", Pallavi Khandekar, ppt.

[22] "Visual Cryptography", Ecaterina Moraru (Valică), ppt., http://students.info.uaic.ro/~evalica/

[23] "Visual Cryptography", S. M. Zargar, ppt.