International Journal of Engineering Technology and Applied Science

(ISSN: 2395 3853), Vol. 5 Issue 6 June 2019

"A Modified Reverse Data Hiding Method to Improve Security Privacy Preserving In Encrypted Gray Scale Images Utilizing Visual Cryptography"

[1]Ranjana Rathore, [2]Mr. Gagan Sharma

[1]M. Tech Scholar, [2]Assistant Professor

Department of Computer Science & Engineering, RKDF University

ranjanajadon@yahoo.co.in

Abstract- ***Visual Cryptography is a sort of cryptography technique that does not requires exceptionally complex estimation in procedure. VC assumes a significant job in sharing of advanced information over the web and broadly utilizes by every one of the clients. Turning around procedures are broadly use in visual cryptography for parallel mystery pictures, Gray scale pictures. When Revering procedures are apply on Gray scale picture with turning around strategies, differentiate is much lower. Thusly, it is increasingly alluring to improve the differentiation in the dark scale picture recreation. Nonetheless, when grayscale pictures are included, one can't exploit this switching activity so effectively.***

In this examination paper we are exhibiting an altered switch information concealing strategy to improve security safeguarding in encoded dim scale pictures utilizing visual cryptography. Proposed MRDHVC strategies right off the bat performs least pixel development strategy with bit pivot method which gives better encoded picture and make hacking progressively troublesome. In second steps MRDVHC strategy uses changed sigmoid capacity in spatial area for complexity improvement in the subsequent mystery picture. The subsequent picture has an a lot higher coherence and demonstrates exceedingly successful in managing poor difference pictures. Proposed and existing strategies both are mimicked by utilizing MATLAB test system and different examination parameters are determined, for example, PSNR, direct co connection measure, standardize cross co connection measure and so on. A trial result plainly demonstrates that proposed strategy performs exceptional over existing technique.

Keywords- *Visual Cryptography, MRDHVC (Modified reversal data hiding Visual cryptography, Pixel reversal, Sigmoid function, Image processing*

1. INTRODUCTION

Cryptography refers to the study of mathematical techniques and related aspects of information security like data confidentiality, data integrity and of data authentication. In the process of Visual Cryptography a secret image is encrypted into shares which refuse to divulge information about the original secret image. Decryption is through a separate decryption algorithm. A basic model for Visual Cryptography for natural images was proposed by Naor and Shamir, where the resultant image is twice the size of secret image. Image that can be considered for Visual Cryptography can be Binary Image, Grayscale Image and Color Image. The scheme given by Naor and Shamir for sharing a secret binary image was by using their own coding table. In this scheme the binary image is divided into two shares, for the white pixel in the secret image, one of the upper two rows of table I is chosen to make share1 and share2. If the pixel of t he secret image is black, one of the lower two rows of table I is used to make share1 and 2. This scheme consists of pixel expansion where every pixel from the secret image is expanded to 4 pixels, so when the shares are generated and superimposed together the reconstructed image will be four times the original secret image size because of this pixel expansion. Also the resolution of the reconstructed image will be less than the original secret image as every white pixel is decomposed into two white & two black pixels. Only one secret could be hidden using this technique.

2. RELATED WORK

Arya k.rakhee baiju et al [1] worked on A Novel Visual Cryptographic Scheme for Improved Binary Image Quality. According to Arya Visual Cryptography is an encryption method which shares secret information into n shares and decrypted into original image without any cryptographic technique. Blundo & Stinson [2, 3] proposed extended visual cryptography in 1996. This scheme contains meaningful shares. The (2,2) EVC theme projected during this needed enlargement of one picture element within the original image to four sub pixels which may then be chosen to supply the specified pictures for every share. Up to 1997, Visual cryptography schemes were applied to only black & white images. In regional incrementing visual

cryptography an image is converted into a number of different regions with n secret levels. Each region is obtained by combining two shares of image. This region contains one level of information. Similarly three shares will results two level of information and likewise n+1 share will results n level of information. Levels of the regions are created automatically [5].

3. PROPOSED MRDHVC METHOD FOR GREY SCALE IMAGES

In this research work we are presenting a modified reverse data hiding method to improve privacy preserving in encrypted grey scale images using visual cryptography. Proposed MRDHVC methods firstly performs minimum pixel expansion method with bit rotation technique which provides better encrypted image and make hacking more difficult. In second steps MRDVHC method uses modified sigmoid function in spatial domain for contrast improvement in the resulting secret image. The resulting image possesses a much higher readability and proves highly effective in dealing with poor contrast images. MRDHVC uses following Modules-

3.1 Module 1- Reversal & Pixel expansion with bit rotation- In visual cryptography schemes, the image quality of retrieved image is reduced because every white pixel is replaced by a 2x2 block containing both black and white pixels and every black pixel is replaced by a 2x2 block of black pixel after overlapping the shares of the image. The novel visual cryptography includes two steps. The first step is revised visual cryptographic technique with some changes in the selection of blocks for black and white pixels. Second step include a post processing technique which improve the visual quality of the reconstructed image obtained from revised visual cryptography.

A. Reversal Method & Pixel expansion- Reversal (2, 2) visual cryptography split a secret image into 2 shares and both shares are needed to reproduce the original image. In order to preserve the aspect ratio each pixel in original image is replaced by 2x2 block of sub pixel in share images. If the pixel of the input image is black, then the sender takes any one of the six combinations which is shown in Table II is randomly selected for share1 and share2. If the pixel of the input image is white, the sender takes the other combinations randomly for share1 and complement of the pattern is selected for share2. Stacking the shares will results the appropriate pixels in the original image. Stacking can be defined as logical OR operation where white pixel is assigned to 1 and black to 0. After stacking the two shares will results the reconstruction of the original image in which white pixels are reconstructed completely and black pixels are reconstructed as a combination of black and white pixels. Hence the output requires a post processing step in order to recover the black pixels.

B. Bit rotation- Shuffling: the elements are shuffled in the individual shares. The elements are shuffled randomly using bit slicing and shifting of bits. We get shuffled bits in each shares, here we are diving no. of random shares into four equal shares. The random shares so generated individually does not provide any information about the secret image, however to recover the contents of an image all the random shares would be required. After recollecting all the random shuffled data shares, original image reconstruction can be performed.

C. Sigmoid Function- for Contrast Enhancement- The contrast is a range of brightness present on an image. The contrast variation affects the original form of image. Contrast enhancement is a process that allows image features more high resolutions. The Sigmoid Function is a mathematical function having an "S" shape (sigmoid curve). The sigmoid function refers to the special case of the logistic function and defined by the formula-

$$S(t) = 1 / 1 + e^{-t}$$

3.2 Module-2 Post processing- A basic block wise approach is used for post processing called simple block replacement [4]. In SBR scheme four pixels from the reconstructed image is considered as a 2x2 single block called secret block. Each secret block in reconstructed image is replaced by a predetermined block of four black pixels or four white pixels. The SBR technique is processed based on number of black pixel in each secret block. If the number of black pixel in a secret block greater than or equal to 2 then the secret block is converted to black block containing four black pixels ,otherwise secret block converted into white block containing four white pixels. This processing step converts the input image into fully black and white block of image. As per our novel visual cryptography the reconstructed image may contain block of white pixels and block of 2 white and 2 black pixels called candidate block. After SBR method applied over the reconstructed image, the white block in reconstructed image remains unchanged and candidate block converted into black block. This results a recovered image which is same as the input secret image with improved quality from the existing visual cryptography schemes for Grey scale images.

4. ALGORITHM FOR PROPOSED MRDHVC METHOD

// MRDHVC Method for Visual Cryptography

Step 1: Read image i.e. Grey Scale Image

Step 2: Image Processing

i) Obtain all the image pixel positions

ii) Apply Pixel reversal

If A is a sample image the Aij, with position i and j are the original pixels

Apply pixel reversal

$Aij^{|} = 255 – Aij$

Step 3: Decide the total number of 'N', Where N represents total number of Shares to be created

Step 4: Create Shares of Image, Apply (MSSS method) modified Shamir's Secret Sharing Scheme.

4.1 By using function called Rand, generate random coefficients.

4.2 Initialize the random coefficient.

4.3 Generate the Polynomial equation.

4.4 Generate the n pieces of partial information i.e. shares.

Step 5: Select any (n-1) shares out of 'n' shares.

Step 6: Apply Pseudo Random Generator Function (values from 0.1 to 0.9)

6.1 PRG ( );

6.2 Return reduce **$Aij^{|}$**

6.3 Calculate difference D_Aij , Where D_Aij= Aij- **$Aij^{|}$**

6.4 Call Pixel_reversal( ); Performs $Aij^{|} = 255 – Aij$

6.5 Stores results in Matrix called Matrix_share_1

6.6 Calculates the difference of two random number generators with original pixel value Aij

6.7 Call Pixel_reversal( ); Performs $Aij^{|} = 255 – Aij$

6.8 Stores results in Matrix called Matrix_share_2

6.9 Performs XOR operation

Matric_Share = Matrix_share_1 XOR Matrix_share_2

Step 6: Combines the (n-1) shares collectively by Lagrange's interpolation.

Step 7: Call Modified sigmoid Function for image enhancement on each pixels

7.1 MS_g();

Step 8: Apply feedback_indicator ()

// checks each pixel quality

Step 9: Results Final Encrypted image

5. SIMULATION AND RESULT COMPARISON

In this research paper we are presenting a modified reverse data hiding method to improve privacy preserving in encrypted grey scale images using visual cryptography.

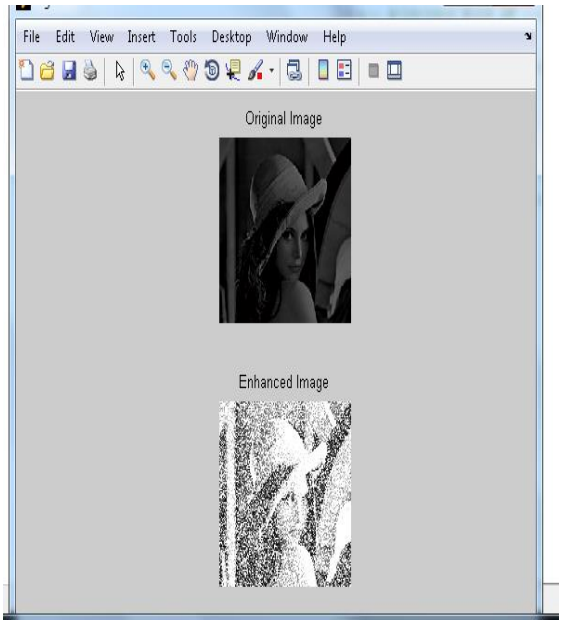

Figure 1: Original and Enhanced Image

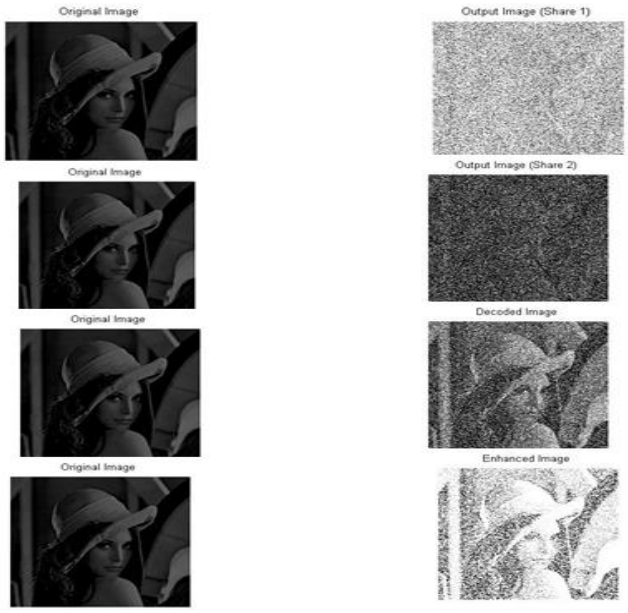

Figure 2: Simulation Outputs Images (Sets of Images)

Proposed MRDHVC methods firstly performs minimum pixel expansion method with bit rotation technique which provides better encrypted image and make hacking more difficult. In second steps MRDVHC method uses modified sigmoid function in spatial domain for contrast improvement in the resulting secret image. The resulting image possesses a much higher readability and proves highly effective in dealing with poor contrast images. Proposed and existing methods both are simulated by using MATLAB simulator and various comparison parameters are calculated such as PSNR, direct co relation measure, normalize cross co relation measure etc.

5.1 Experimental result for Direction correlation measure existing method and proposed method

Table 1: Results for DCM for existing and proposed method

IMAGE TYPE	Direction correlation measure in %	
	EXISTING METHOD	PROPOSED METHOD
Image 1	91.25	93.56
Image 2	90.45	92.54
Image 3	89.69	93.44

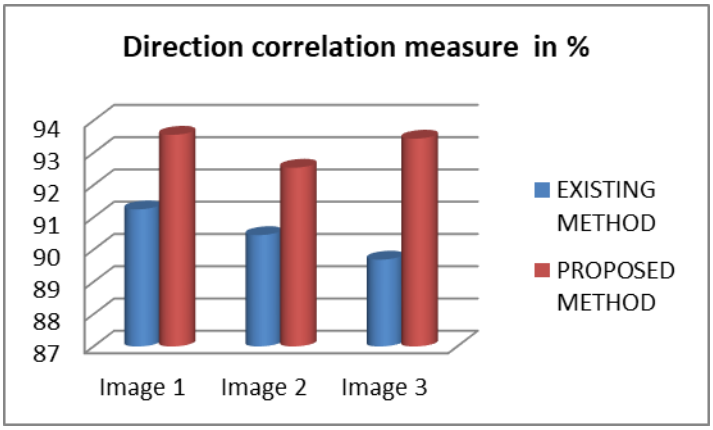

Figure 3: Results Comparison in terms of Direction Correlation Measure in Percentage

5.2 Experimental result for Normalize cross correlation measure existing method and proposed method-

Table 2: Results Normalize cross correlation measure existing method and proposed method

IMAGE TYPE	Normalize cross correlation measure %	
	EXISTING METHOD	PROPOSED METHOD
Image 1	0.781	0.689
Image 2	0.641	0.544
Image 3	0.712	0.569

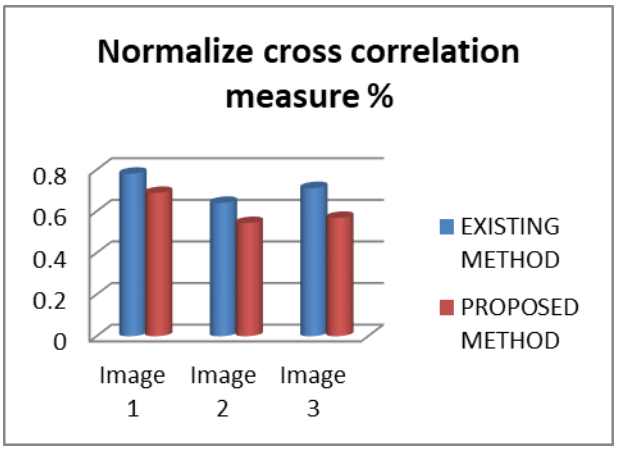

Figure 4: Results Comparison in terms of Normalize Cross Correlation Measure in Percentage

5.3 Experimental result for PSNR value existing method and proposed method-

Table 3: Results PSNR existing method and proposed method

IMAGE TYPE	PSNR %	
	EXISTING METHOD	PROPOSED METHOD
	PSNR	PSNR
Image 1	51.44	59.6
Image 2	48.78	49.58
Image 3	53.22	56.55

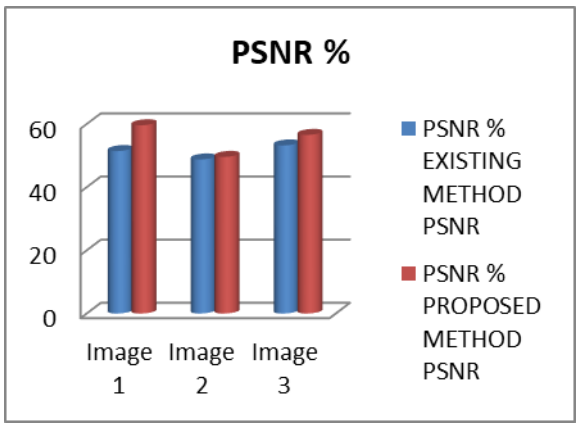

Figure 5: Results Comparison in terms of PSNR in Percentage

6. CONCLUSION & FUTURE WORK

Reversible data hiding in encrypted image is drawing lots of attention because of privacy preserving requirements. The proposed scheme gives a completely new framework for reversible data hiding technique. Here in this approach a new technique is used for encryption of image. The data hider can take benefit from the extra space emptied out in previous stage before encryption to make data hiding process effortless. In the proposed technique we can take advantage of visual cryptography for encrypting the image. Hence, the image is protected during transmission and secret data is also transmitted securely. Proposed MRDHVC methods firstly performs minimum pixel expansion method with bit rotation technique which provides better encrypted image and make hacking more difficult. In second steps MRDVHC method uses modified sigmoid function in spatial domain for contrast improvement in the resulting secret image. The resulting image possesses a much higher readability and proves highly effective in dealing with poor contrast images. Proposed method shows better results over existing method in terms of PSNR, DCM and NCRM. In future work we will implements this method with RGB, CMY images for real time data.

REFERENCES

[1] Arya k.1,rakhee baiju2, sreenarayanan n. M.3 , lakshmi m.4, nimisha mohan 5, soumya m. K.6, aswathy a.s.7, reshmi k.c., a novel visual cryptographic scheme for improved binary Image Quality, International Conference On Information Communication And Embedded System(ICICES 2016), PP 252-257

[2] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li. Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption. IEEE Transaction on Information Forensics and Security: March 2013; Vol.8; No.3.

[3] Jun Tian. Reversible Data Embedding Using a Difference Expansion.Transactions on circuits and systems for video technology: AUGUST 2003; VOL. 13, NO. 8.

[4] Siddharth Malik, Anjali Sardana, Jaya. A Keyless Approach to Image Encryption. International conference on Communication systems and Network Technologies: 2012; IEEE.

[5] R. Vijayaraghavan, S. Sathya, N. R. Raajan. Security for an Image using Bit-slice Rotation Method–image Encryption. Indian Journal of Science and Technology: April 2014;Vol 7(4S); p 1–7.

[6] C. Anuradha, S. Lavanya. Secure and Authenticated Reversible Data Hiding in Encrypted Image. International Journal of Advanced Research in Computer Science and Software Engineering: April 2013; volume 3, issue 4.

[7] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su. Reversible Data Hiding. IEEE transactions

on circuits and systems for video technology: March 2006; vol. 16, no. 3.

[8] Asha S.N, Dr. Shreedhara. Performance Evaluation Of Extended Visual Cryptography Schemes With Embedded Extended Visual Cryptographic Scheme. International Journal of Scientific & Engineering Research: April-2012; Volume 3, Issue 4.

[9] R. Lukac, K.N. Plataniotis. Bit-level based secret sharing for image encryption. The Journal of Pattern Recognition Society: 2005.

[10] InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee. Color extended visual cryptography using error diffusion. IEEE: 2009.

[11] Yi, Feng; Wang, Daoshun; Luo, Ping, Huang, Liansheng, Dai, Yiqi.Multi Secret Image Color Visual Cryptography Schemes for General Access Structures. April 2006; Volume 16, Number 4; pp. 431-436.

[12] J. Fridrich, M. Goljan, and D. Rui. Lossless Data Embedding - New Paradigm in Digital Watermarking. In Special Issue on Emerging Applications of Multimedia Data Hiding: February 2002; Vol. 2; pp. 185-196.

[13] Chen Y, Tsai D-S, Horng G (2012) Comment on Bcheating prevention in visual cryptography. IEEE Trans Image Process 21:3319–3323

[14] Corke P (2011) Image feature extraction robotics. Vision Control, Springer 73:335–379

[15] Corke P (2011) Image feature extraction. Robotics, Vision Control, Springer 73:335–379

[16] Desmedt Y, Van Le T (2000) Moire cryptography. In: the 7th ACM conference on Computer and Communications Security, 116–124