Hybrid Technique for Secure Visual Cryptography using a Hybrid Technique of Vigenere Cipher, Dithering Matrix and RSA Algorithm

Er. Varinder Saini, Er. Rajandeep Kaur
SBBSU (Sant Baba Bhag Singh University) Jalandhar, India

***Abstract*--** Information hiding in the communication spectrum became a critical task. Visual Cryptography is a special technique which is used to send the images securely over the network. It involves dividing the secret image into n shares and a certain number of shares (m) are sent over the network. The decoding procedure includes stacking of the shares to get the secret image. Thus secret shares are not available in their actual form for any alteration by the adversaries who try to create fake shares. It is a procedure to hiding secret binary image to hide messages containing text. The proposed technique use vigenère cipher algorithm, RSA algorithm and dithering matrix algorithm for high security of images and secret information. Both encryption algorithms double the security while transferring images over the network. The proposed scheme also uses the concept of half toning and reverses half toning for improving the quality of a secret image. The resulting scheme gives the perfect security of the shares that are well encrypted and the visual quality of the stacked image is very good. The experimental results of the proposed method are compared with Floyed, Jarvis, and Stucki, modified error diffusion algorithm and LSB techniques.

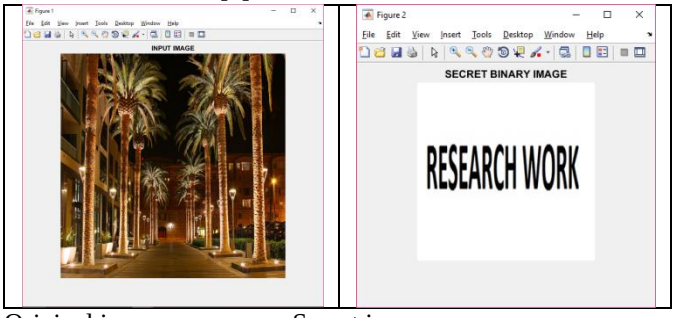
Keywords *- Visual Cryptography (VC), PSNR, HVS, MSE, RSA.*

I. INTRODUCTION

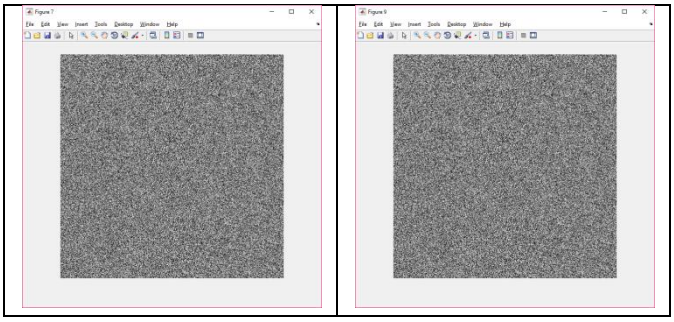
Visual Cryptography (VC) is a procedure utilized for securing picture based privileged insights. The principle idea of the first visual cryptography conspire is to encode a mystery picture into a few offers. Mystery data can't be uncovered with few offers. All offers are important to join to uncover the mystery picture. Halftoning is the essential component of visual cryptography. It gives security at the beginning period of visual cryptography. Halftoning is the reprographic procedures, whose procedure of changing over substantial tone (high force estimation of pixel) picture to low tone (low power estimation of pixel) picture [4].

The visual cryptography is a conceal data innovation. The visual mystery conspire unscrambles the mystery picture utilizing Human Visual System (HVS) with no calculation [5].

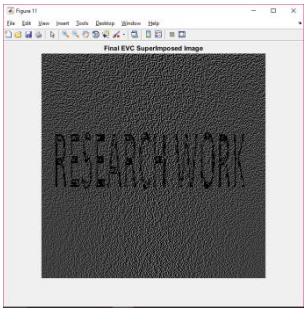
The visual cryptography utilizes sharing strategy apply for shroud data. Here utilized the (2, 2) greyscale picture strategy, 2 shares out of 2 stack the mystery will uncover and under 2 shares are not work [5].



Original image Secret image



Encrypted share 1 Encrypted share 2



Final Retrieved secret image

Fig.1: Illustration of Visual Cryptography

II. PROPOSED TECHNIQUE

The new technique has been purposed to hide the information along with security. The main aim of this technique can be purposed for the security of the secret information. The basic idea of this process selects the cover image and then selects the secret image. Now, perform the encryption technique vigenère cipher algorithm. If entered the correct key then half toning process starts and otherwise terminate the process. Then apply dithering matrix algorithm and the halftone image is created. After this perform reverse half toning process and the reverse half toned image is created. And then secret information is hidden in share 1 and share 2. Perform Encryption and Decryption of Share -1 and Share -2 using RSA Algorithm. At the end retrieve the final secret image. After that generate results in form of PSNR and MSE. PSNR (peak signal to noise ratio) is used to check the quality of the original image and the secret image. MSE (mean square error) is used to measure the average square error between the original image and the secret image. As the purposed technique uses the vigenère cipher encryption technique and RSA encryption algorithm, thus it provides more security while using dithering matrix algorithm helps to hide the secret information.

In this proposed technique, use of two RSA algorithms of public key cryptography encryption and decryption performed on share1 and share2 that provide security of shares. And vigenère cipher encryption technique used for security purpose. If the correct key entered then next process starts otherwise terminate the process. If hackers get one share, then the hacker is not able to retrieve the secret information from one of the images.

III. ANALYSIS OF RESULT

Proposed arrangement of secure visual cryptography actualized by joining the vigenère cipher, dithering matrix and RSA calculation for security of secret pictures. For accomplishing the objectives of the proposed framework MATLAB R2015a is utilized. The outcome is essentially actualized with the assistance of PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error) parameters. PSNR is figured to check the nature of a yield picture. Higher the estimation of PSNR, better the nature of a yield picture. Be that as it may, for the better outcomes MSE esteem ought to be low. In proposed method outcome is based on parameters PSNR and MSE. Parameters can be depicted as take after:

Peak Signal to Noise Ratio

PSNR is utilized to quantify the nature of the picture after the reconstruction.. Higher PSNR esteem demonstrates that secret picture quality is superior to the first picture. PSNR is typically communicated in decibels [6].The PSNR between two pictures can be depicted as take after:

$PSNR = 10 \log_{10} [MAX^2/MSE]$

Where, MAX^2= Maximum value of pixel in original image
MSE= Mean Square error

Mean Square Error

MSE estimate the average of the squares of the "errors." Mean Square Error is the risk function that represents the cumulative error between the original image and the secret image [6]. It is depicted as follow:

$$\mathbf{MSE = 1/MN \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (C(X, Y)-S(X, Y)^2}$$

Where (X, Y) are the two Coordinates of the image, (M, N) are the two dimensions. So (X, Y) creates Secret image and (C, Y) creates cover image.

TABLE 1: Comparative analysis of hybrid technique with existing data hiding techniques Floyed, Jarvis, and Stucki, modified error diffusion algorithm and LSB in terms of average values of PSNR and MSE on whole USC-SIPI Image Database

Picture Quality Evaluation	PSNR	MSE
Floyed	7.9221	2.24432
Jarvis	8.0330	2.18553
Stucki	8.01981	2.19223
Modified Error Diffusion	35.47261	9.15866
LSB	41.019055	5.143555
Proposed technique	53.69755	0.290375

The Table 1 shows the performance of the system in terms of PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error).The results show that Proposed technique shows better results in case of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Ratio) because for better results the value of PSNR is high and the value of MSE is low.

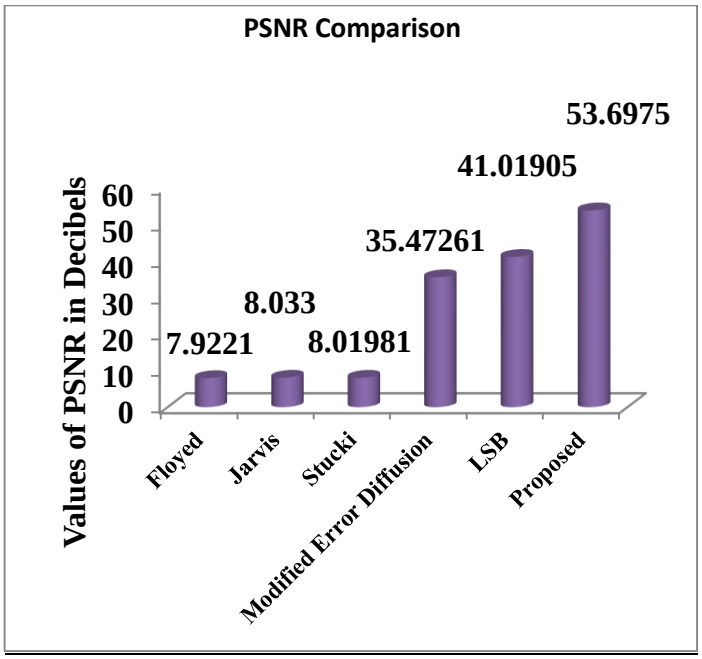


Figure 2: Comparison between average values of PSNR for Floyed, Jarvis, and Stucki, modified error diffusion algorithm, LSB and Proposed Technique

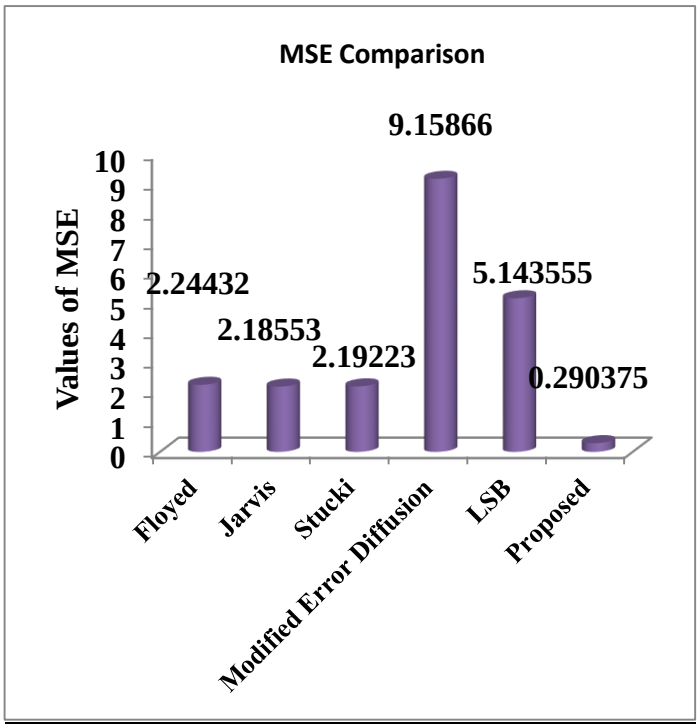


Figure 3: Comparison between average values of MSE for Floyed, Jarvis, and Stucki, modified error diffusion algorithm, LSB and Proposed Technique

IV. CONCLUSION AND FUTURE SCOPE

With the growth and advancement in digital media, it is necessary to find a technique which assures secure transmission of secret data that is Visual Cryptography (VC). Secret share is completely secured using public key encryption (asymmetric cryptography) that makes secret image shares not possible to be changed by any unauthorized access. Visual Cryptography (VC) with asymmetric algorithms like RSA assured the security of secret images through a channel. The proposed system is tested on 40 images of USC-SIPI Image Database. In my work proposed Visual Cryptography hybrid technique depending on some complex computations like vigenère cipher encryption technique, dithering matrix and RSA algorithm which giving high security than the traditional methods. The PSNR (Peak Signal to Noise Ratio) value calculated by using proposed hybrid technique on 40 images is 53.69755 in decibel. The MSE (Mean Square Error) value by using proposed hybrid technique on 40 images is 0.290375. And results shows that proposed hybrid technique produces better results in terms of PSNR and MSE than other existing techniques Floyed, Jarvis, and Stucki, modified error diffusion algorithm and LSB.

The proposed system works just on two dimensional images. In future, this system can be extended to work for three dimensional images. In future enhance the quality of recovered final image and compare the results with other parameter like Normalised Corelation (NC).

V. REFERENCES

[1] Swati Kashyap, Neeraj Madan, "A Review on: Network Security and Cryptographic Algorithm" in IJARCSSE, Vol. 5, Issue 4, April 2015.
[2] Rajesh R Mane, "A Review Cryptography Algorithms, Attacks and Encryption Tools" in IJIRCCE, Vol. 3, Issue 9, September 2015.
[3] Monika Agrawal, Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques", in IJCSE, Vol. 4 May 2012.
[4] Shruti M. Rakhunde, Manisha Gedam, "Survey on Visual Cryptography: Techniques, Advantages and Applications", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 06-12.
[5] Febin Baby, Arun R, Suvanam Sasidhar Babu, "ViCry: Visual Cryptography Schemes for Security (An overview of different types of visual cryptography schemes)", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 15-18.
[6] Anshul Sharma, "PERFORMANCE OF ERROR FILTERS IN HALFTONE VISUAL CRYPTOGRAPHY", International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.3, September 2012.
[7] Monika Bhosale, Rajshree Chaudhary, PrathameshGaddam, AyushiKedar Yogesh. J.Pawar, "Visual Cryptography Scheme for Secret Image Retrieval", in IJARSET Vol. 3, Issue 3 March 2016.

[8] Shikha Kuchhal, Ishank Kuchhal, "Data Security Using RSA Algorithm In Matlab" in IJIRD, July, 2013, Volume 2, Issue 7.
[9] Asad Mansoori, Vijay kumar joshi, "Halftoning by Error Diffusion Method in Visual Cryptography for Greyscale Image", International Journal of Computer Applications (0975 – 8887) Volume 148 – No.10, August 2016
[10] Alaa Kadhim, Rand Mahmoud Mohamed, "Visual Cryptography for Image Depend on RSA & AlGamal Algorithms", Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA) – IRAQ (9-10) May 2016.
[11] Rimsy Dua, Narender Singh, "Enhancement of security in Visual Cryptography using DES algorithm" in IJIRCCE , July-2016, Vol. 4, Issue No.7.
[12] Vinita Malik, Mamta Ghalan, Dheeraj kaushik, "Securing of colour images using Visual Cryptography and Digital Enveloping", in COMPUSOFT IJACT, April-2016, Vol. 5, Issue No.3.
[13] Ch. Rupa, D. Sasidhar, "Keyed Visual Cryptography scheme for secure data transmission" in 2016, World Applied Sciences Journal 34 (4): 529-534, ISSN 1818-4952, DOI:10.5829/idosi.wasj.2016.34.4.395.
[14] Kashmira S. Gulhane, P.L.Ramteke, "VISUAL CRYPTOGRAPHY USING IMAGE" in IJRISE, Vol. 2, Issue 1.
[15] Kalyan Das, Aromita sen, Samir kumar Bandyopadhyay, " A new Visual Cryptography scheme for color images using sliding puzzle technique" in IJIRR, Volume 03, Issue 04, April 2016.
[16] Nidhal Khdhair El Abbadi, Samer Thaaban Abbas, Ali Abd Alaziz, "New image encryption algorithm based on Diffie – Hellman and Singular value Decomposition" in IJARCCE, Vol. 5, Issue 1, January 2016.
[17] K.Kanagalakshm, M.Mekala, "Enhanced Blowfish algorithm for image encryption and decryption with supplementary key "in IJCA, Vol. 146-No 5, July 2016.
[18] Gaurav kumar , Sachin chaudhary, "A Visual Cryptography scheme to secure black and white image shares using Digital Watermarking " in IJARCSSE, Volume 6 Issue 5, May 2016.
[19] Rimsy Dua, Narender Singh, "Secured Visual Cryptography scheme using meaningful shares" in IJIRCCE, Volume 4, Issue 4,April 2016.
[20] Sankar Das, Asoke Nath, Arijit Samanta, Abhishek Roy, Saptarshi Bhattacharyya, " A Secure Approach for Data Hiding using Visual Cryptography", in IJIRCCE Vol. 4, Issue 6, June 2016.
[21] Asha Bhadran R, "An Improved Visual Cryptography Scheme for colour images" in IRJET, Aug-2015, Vol. 2, Issue No.5.
[22] M.Karolin, T. Meyyapan, "RGB based secret sharing scheme in color Visual Cryptography", in IJARCCE, July 2015 vol. 4, Issue No. 7.
[23] Chandan Sharma, Vinod Sharma and Ankush Sharma, " Three Quadrant Method for Securing Image by Using Visual Cryptography", CPUH-Research Journal: 2015, 1(2), 59-61 ISSN (Online): 2455-6076.
[24] Aarti, Pushpendra K Rajput, "An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding", I.J.Computer Network and Information Security, 2014, 2, 54-60 Published Online January 2014 in MECS ,DOI: 10.5815/ijcnis.2014.02.08
[25] PallaviB, Vishala I. L, "Double Layer Security Using Visual Cryptography And Transform Based Steganography'', International Journal of Research in Engineering and Technology, 2014.
[26] Manika Sharma, Rekha Saraswat, "Secure Visual Cryptography technique for color images using RSA algorithm", in IJEIT,April-2013, Vol. 2, Issue No.10.
[27] Sozan Abdulla, "New Visual Cryptography Algorithm for colored image", in JOURNAL OF COMPUTING ,April 2010, Vol. 2, Issue No.4, ISSN 2151-9617.
[28] Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran," Digital Image Encryption Based on RSA Algorithm", Journal of Electronics and Communication Engineering, Volume 9, Issue 1, Jan. 2014
[29] B.Sridhar, K.V.V.S. Reddy, A.M.Prasad, "An Unsupervisory Qualitative Image Enhancement using Adaptive Morphological Bilateral Filter for Medical Images", International Journal of Computer Applications, Volume 99 – No.13, August 2014
[30] Poonam Bidgar, Neha Shahare , "Secret Image Transmission through Image Sharing using Secret Key and LSB Embedding", International Journal of Electronics Communication and Computer Engineering , Volume 5, Issue (4) July, Technovision-2014.