Image Encryption and Decryption using RSA Algorithm with Share Creation Techniques

M. Karolin, T. Meyyappan

Abstract—visual cryptography system proposed a image encryption and decryption method. In the proposed method Red, Green, Blue color images using visual cryptography. In existing system is working for share created, it is encrypted separately by using visual secret share creation (VSS) algorithms. The proposed work is original images share1 and ahare2 created XOR-Based visual cryptography. This proposed schemes share1 encryption and share2 encryption included in RSA algorithm. The share1 and ahare2 decryption process is enable secret image sharing and then stacking. The proposed system is value calculate the PSNR and MSE formula and then image security using NPCR and UACI formula. The visual cryptography existing work to compare the proposed work and better results quality of RGB color images. The color image encryption and decryption using RSA algorithm and matlab coding.

Keywords : Image security, Share creation Method, RSA algorithm, NPCR, UACI.

I. INTRODUCTION

Visual Cryptography is the methods for encrypting and decrypted using multiple numbers of secret images sharing and then stacked to original images .Visual cryptography works on visual information to be confidential, authentication integrity and non-reputation Visual cryptography received to original image and then share1 and ahare2 created. Visual cryptography takes original images and share creation methods transparent to stacked image and reverses the decrypted images.

II. RELATED WORKS

Visual top secret sharing for color images was introduce by Naor and Shamir based upon cover semi groups [2]. Rijimen presented a 2-out-of-2 VC design by apply the idea of color mixture. They used the binary encoding to represent

the sub pixels selected for each RGB color and applied the stacking sub pixels of every color in the cover images.

A. Existing system

The existing scheme generates the visual cryptography encrypts both share using AES algorithm and public key cryptography. The AES Existing work is public key cryptography and encryption decryption method.

III. PROPOSED METHOGOLOGY

Visual cryptography secret share creation technique original (RGB) color images and share1&share2 created and then share1, share2 encrypted. Decryption process is secret image share1 and share2. This proposed work is implemented with RSA algorithm and matlab coding. This result is better quality of RGB color images. RSA algorithm was secret image sharing and stacking. Proposed method is best results of Lena, Jet and Barbara images. Image security calculates the UACI and then NPCR values.

A. Visual secret share (vss) creation process

The RGB color pixel values original image and share1, share2 to the separate the key matrixes. Key value 1, 2…255.

$$RP = \begin{pmatrix} 127 & 127 & 127 & 125 \\ 127 & 126 & 127 & 123 \\ 126 & 125 & 126 & 127 \\ 126 & 126 & 126 & 127 \end{pmatrix}$$

$$Gp = \begin{pmatrix} 234 & 234 & 236 & 233 \\ 233 & 233 & 234 & 230 \\ 230 & 229 & 232 & 230 \\ 230 & 230 & 230 & 230 \end{pmatrix}$$

$$BP = \begin{pmatrix} 125 & 123 & 122 & 116 \\ 121 & 118 & 117 & 112 \\ 113 & 111 & 111 & 107 \\ 110 & 107 & 106 & 105 \end{pmatrix}$$

After that, basics matrix based created the shares shown in below matrix. For example R band share creation process initially generate the empty matrix this contain the 255 pixel values and VSS process based shares are created.

$$Rs1 = \begin{pmatrix} 63 & 63 & 64 & 62 \\ 63 & 63 & 63 & 61 \\ 63 & 63 & 63 & 63 \\ 63 & 63 & 63 & 63 \end{pmatrix} \quad Rs2 = \begin{pmatrix} 64 & 64 & 63 & 63 \\ 64 & 63 & 64 & 62 \\ 63 & 62 & 63 & 63 \\ 63 & 63 & 63 & 63 \end{pmatrix}$$

$$Gs1 = \begin{pmatrix} 117 & 117 & 118 & 116 \\ 116 & 116 & 117 & 115 \\ 115 & 114 & 116 & 115 \\ 115 & 115 & 115 & 115 \end{pmatrix} \quad Gs2 = \begin{pmatrix} 117 & 117 & 118 & 117 \\ 117 & 117 & 117 & 115 \\ 115 & 115 & 116 & 115 \\ 115 & 115 & 115 & 115 \end{pmatrix}$$

$$Bs1 = \begin{pmatrix} 63 & 63 & 61 & 58 \\ 60 & 59 & 59 & 56 \\ 55 & 55 & 53 & 53 \\ 55 & 54 & 53 & 53 \end{pmatrix} \quad Bs2 = \begin{pmatrix} 62 & 62 & 61 & 58 \\ 61 & 59 & 58 & 56 \\ 57 & 56 & 55 & 53 \\ 55 & 53 & 53 & 52 \end{pmatrix}$$

B. Key generation process

In the confidential image, the secret key K_m is provided by the column transformation can be worked out on the confidential image. Two keys are employed in the visual cryptography.

$K_p = H * K_m$

Let generate the key matrix K_m

$$K_m = \begin{pmatrix} 100 & 120 & 154 & 180 \\ 161 & 234 & 180 & 120 \\ 121 & 185 & 148 & 159 \\ 108 & 132 & 220 & 170 \end{pmatrix}$$

C. RSA Algorithm

The proposed algorithm developed by Rivest, Shamir Adlemenz). RSA algorithm working with public key is encryption and private key is decryption. RSA algorithm provides a original image share1and Share1 and share2 created and then share encrypted with in decrypted. Thus results RSA algorithm to assure the confidentiality, integrity, Authenticity and non-repudiation.
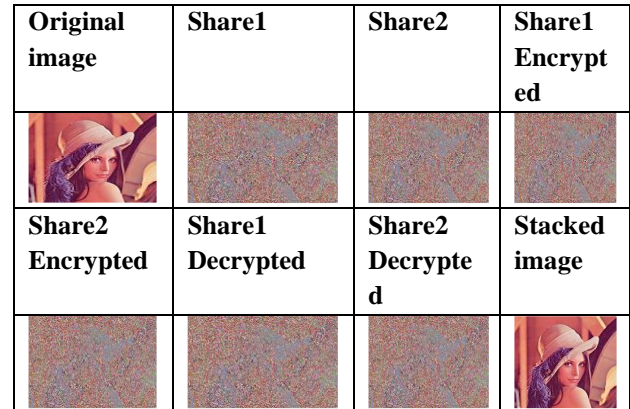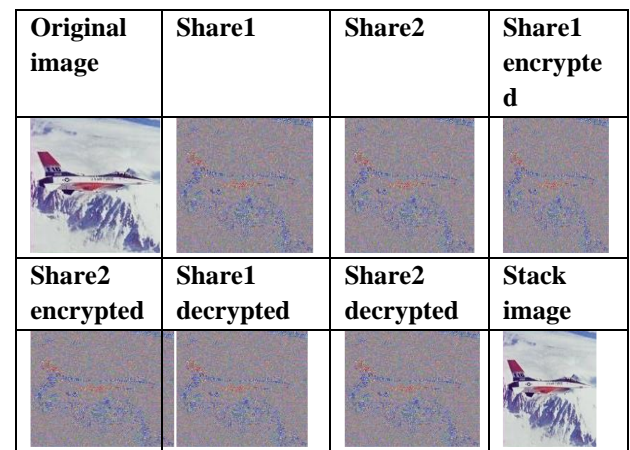
IV. RESULT AND DISCUSSION

The performance of the proposed scheme is image quality analyzed by using the PSNR and MSE values and then image security analyzed by using the NPCR and UACI value in all images. Proposed work best image quality and security.

Original image	Share1	Share2	Share1 Encrypted
Share2 Encrypted	Share1 Decrypted	Share2 Decrypted	Stacked image

Fig 1. Proposed scheme for Lena (image)

Original image	Share1	Share2	Share1 encrypted
Share2 encrypted	Share1 decrypted	Share2 decrypted	Stack image

Fig 2. Proposed scheme for Jet (image2)

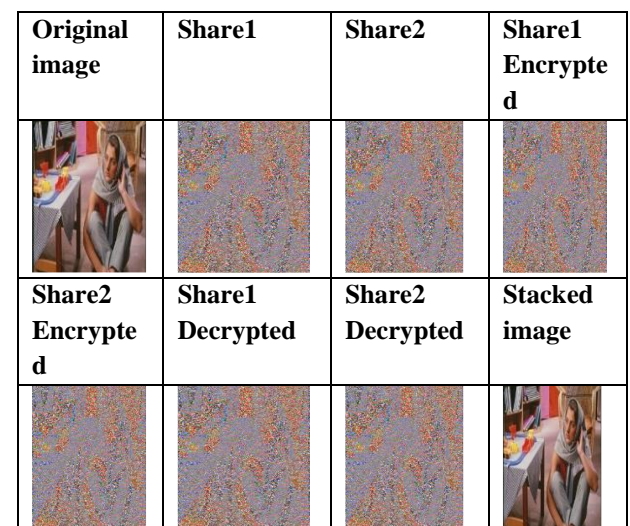| Original image	Share1	Share2	Share1 Encrypted
Share2 Encrypted	Share1 Decrypted	Share2 Decrypted	Stacked image

Fig 3.Proposed Scheme for Barbara (image3)

Table I: Performance analysis of value for the various test images

Images	MSE	PSNR	NPCR	UACI
Lena	93.44	69.91	92.16	18.07058
Jet	87.11	64.73	90	17.22352
Barbara	81	59.27	87.84	16.37647

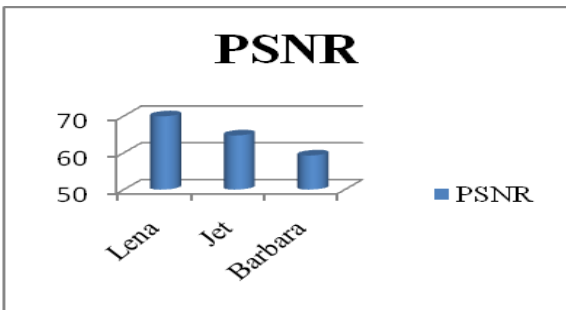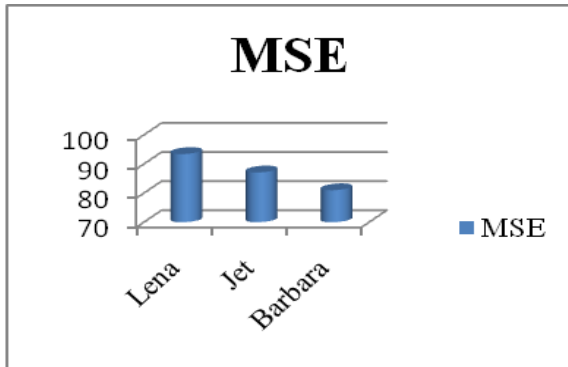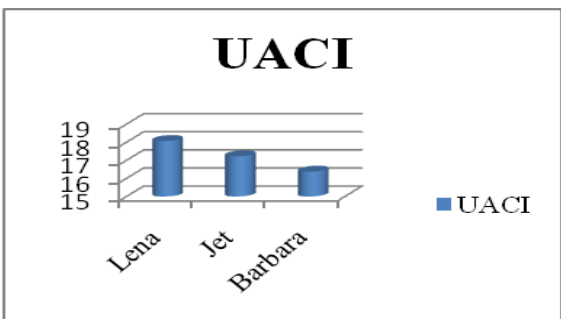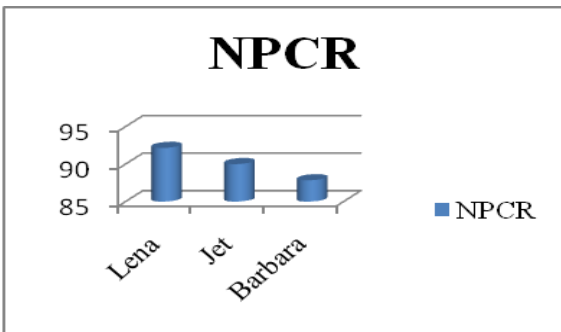**Chart1. Mse and Psnr value**

Chart2. NPCR and UACI value

A. Performance analysis of various method

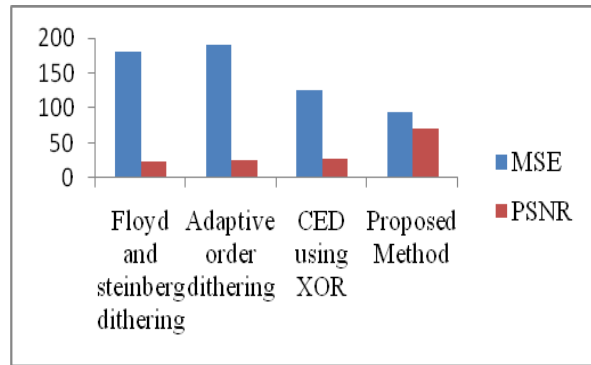Image security and quality using NPCR, UACI, PSNR and MSE as the results and fallow the value in table 2.

Chart3. Performance analysis of proposed method

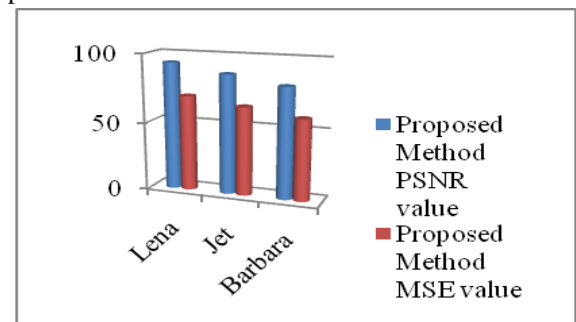**TableII: Performance of Existing Method to Proposed Method:**

Existing Scheme			Proposed Scheme		
Images	PSNR value	MSE value	Images	PSNR value	MSE value
Lena	85.33	65.88	Lena	93.44	69.91
Jet	80.23	59.68	Jet	87.11	64.73
Barbara	69.43	54.11	Barbara	81	59.27

Table III: Comparison of Existing Method to Proposed Method:

Existing Method
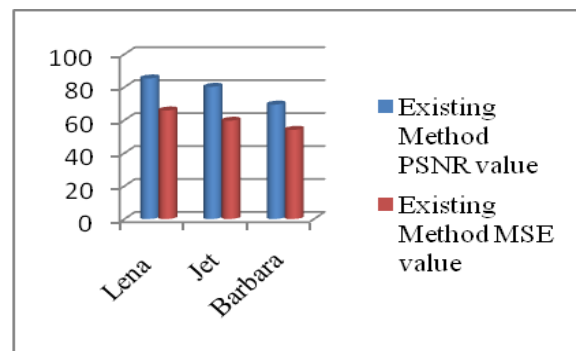
Proposed Method

V. CONCLUSION

Visual cryptography proposed work is implemented with RSA Algorithm and matlab coding. Existing work is compare to the proposed work and then better results for Lena jet and Barbara images comparative analysis of image quality to PSNR and MSE and then image security to UACI and NPCR performance for better results

REFERENCES

1. M. Naor and A. Shamir, "Visual cryptography," Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes Computer Science, Vol. 950, pp. 1 - 12, 1995.
2. C. Yang and C. Laih, "New Colored Visual Secret Sharing Schemes", Designs, Codes and cryptography, 20, pp. 325–335, 2000.
3. R. Lukac, K.N. Plataniotis, "Bit-Level Based Secret Sharing For Image Encryption", Pattern Recognition 38 (5), pp. 767–772, 2005.
4. Anantha Kumar Kondra, Smt. U. V. RatnaKumari, "An Improved (8, 8) Color Visual Cryptography Scheme Using Floyd Error Diffusion", in International Journal of Engineering Research and Applications, Vol. 2, Issue 5, September- October 2012, pp.1090.
5. L. N. Pandey and NeerajShukla, "Visual Cryptography Schemes using Compressed Random Shares", in International Journal of Advanced Research in Computer Science and Management Studies, Volume 1, Issue 4, September 2013, pp:62 – 66.
6. M.Karolin Dr.T.Meyyappan,"RGB Based Secret Sharing Scheme in Color visual cryptography", in International Journal of Advanced Research in Computer and Communication Engineering,Vols. 4, Issue 7, July 2015.
7. AshaBhadran R,"An Improved Visual Cryptography Scheme for Color Images" International Research Journal of Engineering and Technology (IRJET), Volume.0.2, Issue: 05, August 2015.
8. M.Karolin Dr.T.Meyyappan .SM.Thamarai: "Image encryption and decryption of color images using visual cryptography" International Journal of Pure and Applied Mathematics, Volume. 118, No. 8, 2018, 277-281.
9. M.Karolin Dr.T.Meyyappan "secret multiple share creation with color images using visual cryptography" International conference on communication and signal processing april4-6 2019, page no: 0058-0062.
10. Komal D Patel , Sonal Belani, Image Encryption Using Different Techniques: A Review International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 1, November 2011.

AUTHORS PROFILE

M.Karolin, PhD Research scholar, Department of computer science Alagappa University, M.sc., M.phil. M.Karolin Dr.T.Meyyappan "secret multiple share creation with color images using visual cryptography" International conference on communication and signal processing april4-6 2019, page no: 0058-0062.

Dr. T. Meyyappan, Department of computer science Alagappa University, M.Sc., M.Phil., M.B.A.,Ph.D. ,Dr.T.Meyyappan"A New approach for the recognition of character from vehicle number plate Images using K-nearest neighbor classifier and Enhanced Artificial Neural Network" International conference(Advanced in computer science &information technology) Jan-2018.