IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.6, Issue.10, Oct. 2018 E-ISSN: 2347-2693

Reversible Data Hiding using RIT, AES and UES Frame Work

Akanksha Bansal[1*], Manoj Ramiya[2], Nirupma Tiwari[3]

[1,2,3]Dept. of computer science, ShriRam College of Engineering & Managment, RGPV Bhopal, India

[*]*Corresponding Author: akankshabansal1993@gmail.com, Tel.: -9039140667*

Available online at: www.ijcseonline.org

Accepted: 15/Oct/2018, Published: 31/Oct/2018

***Abstract*-** Image Steganography is an emerging field in computer science. There is a need of secured data transmission system to protect the data and maintain the privacy. This work is based on multilevel security method. The reversible data hiding has been implemented using a robust method. The secret image is encrypted using Reversible Image transformation, followed by AES (Advanced Encryption Standard) algorithm and finally the UES(Unified Encryption and Scrambling) is applied for data embedding into the carrier image. The secret key is also added to the encrypted image and it further makes the frame work more robust. The frame work is simulated using MATLAB and the statistical results like PSNR, MSQE and SSIM confirm the proposition.

Keywords—AES, UES, public channel, , image encryption, reversible image transformation, privacy protection, imperceptible , secret key, stego, public channel, scrambling, PSNR, MSQE, SSIM

I. INTRODUCTION

The public channels like internet and cloud services are popularly used at global level. There is a need of massive data exchange. There is heavy demand of temper proof data exchange systems and public storage like google drive. There is a dire need of well secured data encryption and decryption systems. The data owners need the accountability and full trust so as to rely upon the service providers like cloud and internet. These data providers offer the high level security. There are certain time critical missions which need extra security like online banking, defence, forensic systems, examination systems, paid services like information databases, travelling systems, online ecommerce etc. The smart solution to develop and deploy the well-designed stenographical systems which use their own methods of encryption at the senders end decryption at the receiving end with the help of secret key which is exchanged through private channel [1].

The RDH behind the carrier picture is the modern method of secret message transmission. The most popular techniques are classified as the SD (spatial domain) and the frequency domain methods. The secret data hiding using LSB, MSB, histogram shifting, EMD, Enhanced EMD , Generalized EMD are very common. These methods are combined with the histogram shifting to improve the payload capacity. The standard algorithms like AES, DES, UES are used to encrypt the semantic message and then hiding it behind the cover image. But, these methods are also vulnerable cyber-attacks. The methods like DWT (Discrete Fourier Transform) in frequency domain are more robust to cyber-attacks. The addition of noise to the stego image can further provide the security [2], [3].

Zhang et al. have adoptedthe HMA (Histogram based modification algorithm)forthe reversible data hiding using maximum modification chances[4],[5]. It is rather difficult to maintain the secrecy of the private messages. It has happened when the private photographs of Hollywood got leaked through the cloud. The RDH method thus fails in providing the complete security. The encryption can be adopted to hide the secret photographs behind some other cover image or video.

This RDH can be very safely applied to get RDH-EI. The cloud service provider cannot access the original data. Looking at the requirements of the secret methods many programmers have worked out very effective systems to protect the data. These developments are more in encryption area. The data is secured when data compression is done losslesly.

This the paper is organized in four sections. The section I, contains brief introduction to the steganography and the proposed work. The section II is the main part and it describes the proposed work. It briefly describes RIT, AES and UES algorithms. The third section contains simulation work and results. The IV section precisely concludes the work with the future direction of the research [6],[7],[8].

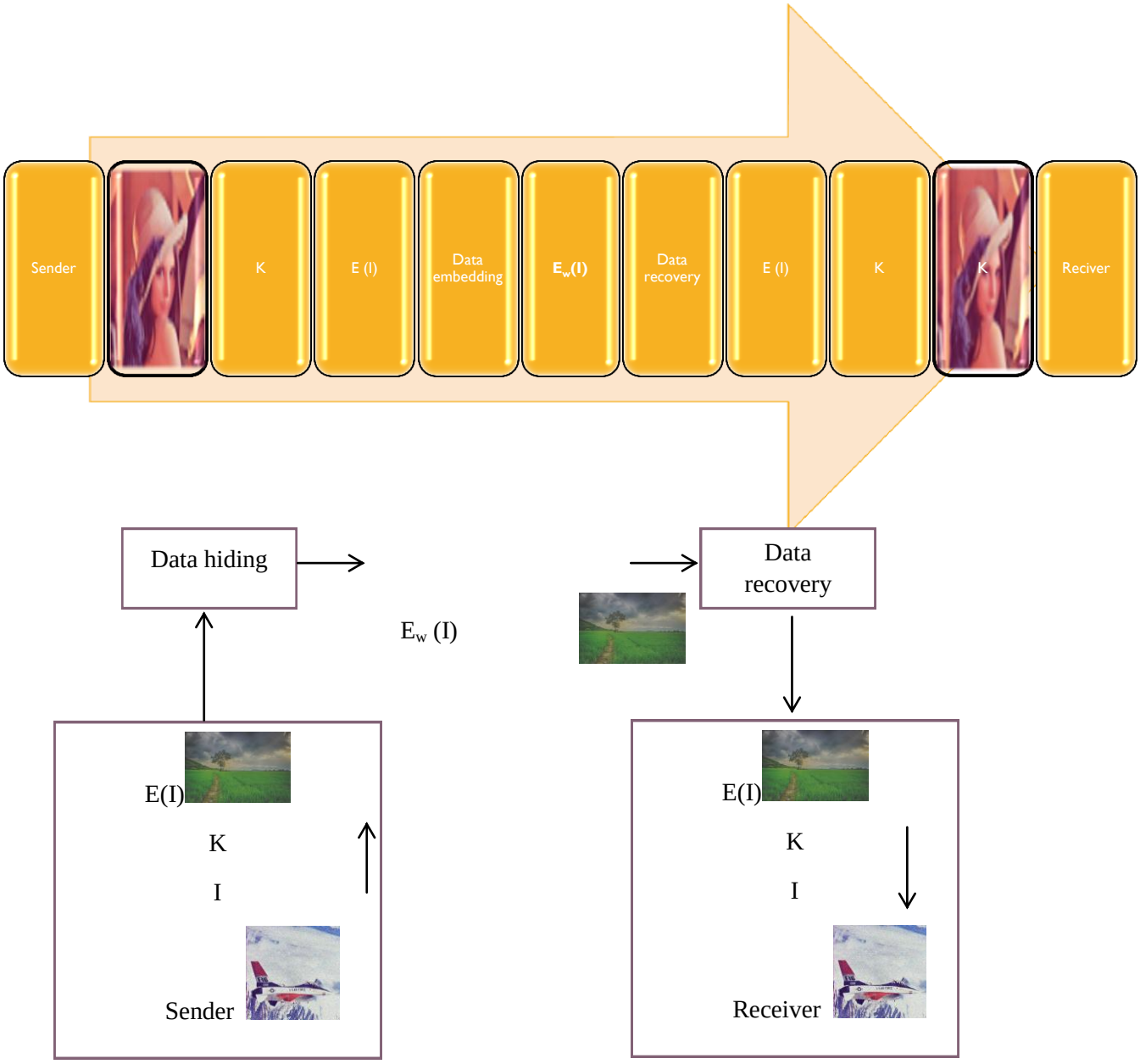

Fig.1 RDH method for plaintext images.

II. THE PROPOSED WORK

(a) REVERSIBLE DATA HIDING METHODS FOR PLAINTEXT IMAGES

II This design involves a very smart and unique reversible data hiding (EI) frame work. It uses Reversible Image Transformation (RIT). This method changes the image I into image J. The word reversible means that the recovered image is same without any distortion. This is called as Semantic Transfer Encryption. The output image E(I) is encrypted and it is very similar to J. The encrypted image has text format. The private cloud service provider can hide the data in the image J.[9]

The RIT method is described in fig 1.. The image I ciphered and E(I) is in the form a simple text. The secret key is added to make the work temper free. All the image data will be stored in the form of text whether encrypted or not on the public service provider. The cloud server can hide or recover the data in E(I). We can get back E(I) from the Ew(I) i.e image containing the watermark. This can be sent to the user having password. The revers RIT method

is used by the receiver to recover the secret message provided he has the secret key K.

The advantages of RIT are : (a) The method or RIT can be smartly sent to the service provider in the form of simple text. The attackers will not doubt the popular service provider. (b) The service provider can use any RDH method to hide the text or can get it back. This does not affect the purpose of sending and receiving the secret image.[10].

RIT (Algorithm 1). The working is as under:
The secret Image is I and key is K (INPUT)

E(I).(Encrypted Image) (OUTPUT)

1. RDH is applied to get E(I) and Image J from AI.
2. Apply AES and use key K to decrypt AI and get CIT of I. $\Delta u_i(\theta_i(1 \leq i \leq N)$
3. Divide J in N blocks and find SD of each block.
4. CITs of J' are used to reorganize the groups of J'
5. For each blockT_i' of J' for $1 \leq i \leq$ Nrotate T_i'in the reverse orientation of θ_i and then minus $\Delta u_i$from pixel value of T_i' and the secret image I
6. AI(Accessorial Information) is hidden in J' and get output E(I)

Reverse Transformation (Algorithm 2)
Input: The ciphered picture E (I) and secret key K.
Output:I the hidden original image

1) The target image J and I as cover image having same size..
2) Divide I , J in 4 x 4 size bins , calculate the and Std. Deviation of each block.
3) Categorize the blocks on the basis of percent quantile of SDs and create CITs for I and J
4) Pair bins of I with J bins using the CITs
5) For block pair (B_i,T_i) ($1 \leq i \leq N$), find the mean difference Δu_i Add $\Delta u_i$to each pixel of B_i next rotate the block into the optimal direction θ_i ($\theta_i \in \{0°, 90°, 180°, 270°\}$and get T_i' .
6) The carrier image J, replace each block T_i with the transformed block $T_i'$for $1 \leq i \leq N$, find J'.

(b) REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE

The output of RIT is the ciphered image E(I). The attractive feature of this method is the image remains apparently meaningful when compared with classical RDH methods. The cloud server can deploy any method at its discretion. The final PSNR values is basis of selecting the method. We have used Unified Data Embedding and scrambling method to hide the large amount of the payload. The result is the trade-off between payload and PSNR of the image.

UNIFIED ENCRYPTION AND SCRAMBLING (UES)

The UES method has been used here. This is applied on already encrypted image. The AI data is large and thus the classical RDH provide low quality stego images. The cloud server can blend the watermark along with UES[11]. This deteriorates the image quality.

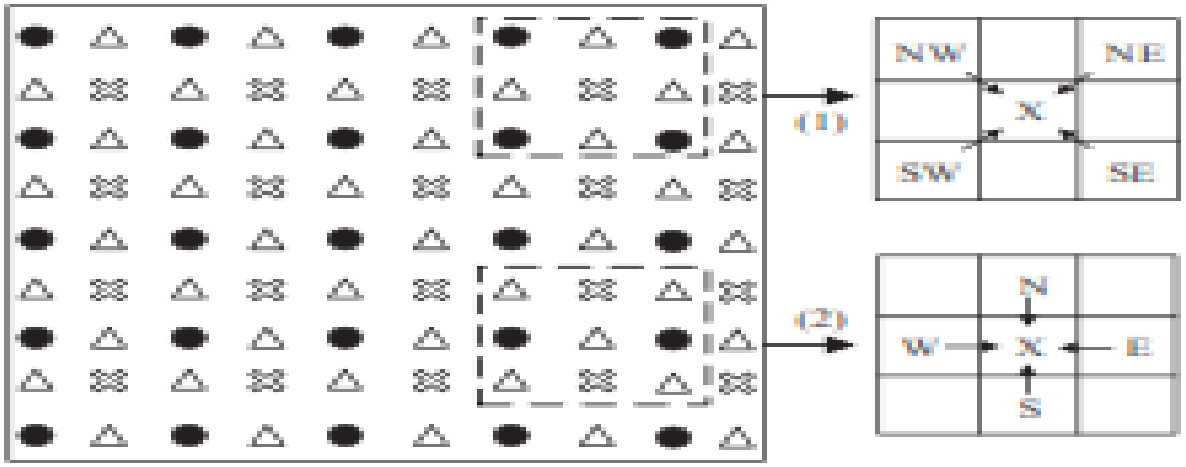

Fig. 2 Check board prediction (CBP)

The UES frame work is like a checkerboard probability (CBP). This reduces the size of the algorithm. It is illustrated in figure 10. The picture consists of the set of pixels which are grouped in three ways. The pixels are marked as solid circles, cross mark and delta sign. The cirles are fixed and used as reference to guess the pixels falling in two other types. The cross set is guessed by rounding the results of Eq. (1) and then delta set is guessed by rounding the results of equation(2). [12]

$$X = \begin{cases} (NW + SE)/2, if||NE - SW|| > ||NW - SE|| \\ (NW + SE)/2, if||NE - SW|| < ||NW - SE|| \\ (NW + NE + SW + SE)/4, otherwsise \end{cases} \quad (1)$$

$$X = \begin{cases} (W + E)/2, if||N - S|| > ||W - E|| \\ (N + S)/2, if||N - S|| < ||W - E|| \\ (W + N + W + S)/4, otherwise \end{cases}.$$

(2)

1. The prediction errors are determined.
2. use HC (Huffman Coding) to reduce prediction errors size.
3. Insert the predicted error and Watermark and use the guessed positions and replace the pixels. The watermark when recovered by the receiver confirms the validity of the message. The PE(prediction errors) are decompressed and summed with the pixel values by the values of CBP. The UES algorithm is changed and becomes reversible. We are aware of the fact that UES technique is not reversible but it is modified by using e_{ij}. 13], [14], [15]

III. THE SIMULATION AND RESULTS

Table 1 The Encryption and Decryption results for the base work.

Base work input (LEENA)	ENCRYPTION			DECRYPTION		
Target Image	**MSE**	**SSIM**	**PSNR**	**MSE**	**SSIM**	**PSNR**
Peppers	**1150.12**	**0.51024**	**40.349**	**10.87**	**0.99483**	**86.96**
Baboon	**492.49**	**0.5836**	**48.83**	**8.1826**	**0.995**	**89.90**
Airplane	**938.69**	**0.4354**	**42.38**	**4.2654**	**0.997**	**96.32**

Table 2 The Encryption and Decryption results for the proposed work

Proposed work input (LEENA)	ENCRYPTION			DECRYPTION		
Target Image	**MSE**	**SSIM**	**PSNR**	**MSE**	**SSIM**	**PSNR**
Peppers	**123.72**	**0.777**	**62.64**	**170.95**	**0.9714**	**59.4**
Baboon	**85.89**	**0.8145**	**66.29**	**167.73**	**0.972**	**59.60**
Airplane	**171.32**	**0.6805**	**59.38**	**167.465**	**0.9729**	**59.61**

IV. CONCLUSION AND FUTURE WORK

The simulation results of the base work are tabulated in Table1 and the proposed results in Table 2.The three standard images are used as the career image. The standard 'Lena' image is encrypted using the base methodology which is based on AES but UES is not used for the embedding the secret image. The encrypted data is sent in RGB frames only. The proposed method is mainly uses RIT and UES algorithm to embed the data. The RGB frames are not used instead YUV (also called as YCbCr) colour space model is used.The careful comparison of the metrics shows that the proposed work out performs base work. The PSNR values for the encrypted image is above 60 and the similarity index is 0.8 with low MSQE values. The decrypted secret image has very high SSIM close 1 and still PSNR around 60. It means that the recovered image has a very good quality and at the same time stego image is imperceptible.

The Future Work: This work is only limited to image as the secret data and the RDH method adopted is vulnerable to cyber-attacks. The more secured embedding method like DWT can be used. The high-resolution images can be used for this purpose. The research can be extended to video and audio as the carrier of the secret message.

REFERENCES

[1] K. Hwang, D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, Sept.-Oct. 2010.

[2] F. Bao, R. H. Deng, B. C. Ooi, et al., "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," IEEE Trans. on Information Technology in Biomedicine, vol. 9, no. 4, pp. 554-563, Dec. 2005.

[3] F. Willems, D. Maas, and T. Kalker, "Semantic lossless source coding," 42nd Annual Allerton Conference on Communication, Control and Computing, Monticello, Illinois, USA, pp. 1411-1418, 2004.

[4] W. Zhang, X. Hu, N. Yu, et al. "Recursive histogram modification: establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. on Image Processing, vol. 22, no. 7, pp. 2775-2785, Jul. 2013.

[5] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. on Circuits and Systems for Video Technology, vol.19, no.7, pp. 989-999, Jul. 2009.

[6] B.ou, X. Li, Y. Zhao, R. Ni, Y. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," IEEE Trans. on Image Processing, vol. 22, no.12, pp. 5010-5021, Dec. 2013.

[7] Ioan-CatalinDragoi, DinuColtuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. on Image Processing, vol. 23, no. 4, pp. 1779-1790, Apr. 2014.

[8] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354-362, Mar. 2006.

[9] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. on Circuits and Systems for Video Technology, vol. 13, no.8, pp. 890-896, Aug. 2003.

[10] X. Hu, W. Zhang, X. Li, N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," IEEE Trans. on Information Forensics and Security, vol. 10, no. 3, 653-664, Mar. 2015.

[11] X. Cao, L. Du, X. Wei, et al., "High capacity reversible data hiding in encrypted images by patch-level sparse representation," IEEE Trans. on Cybernetics, vol. 46, no. 5, pp. 1132-1143, May. 2016.

[12] S. Yu, C. Wang and K. Ren, "Achieving secure, scalable, and finegrained data access control in cloud computing," IEEE Proceeding of INFOCOM 2010, pp. 1-9, Mar. 2010.

[13] I. Lai and Wen. Tsai,"Secret-fragment-visible mosaic image-a new computer art and its application to information hiding," IEEE Trans. on Information Forensics and Security, vol. 6, no. 3, pp. 936-945, Sept. 2011.

[14] Y. Lee and W. Tsai,"A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformation," IEEE Trans. on Circuits and Systems for Video Technology, vol. 24, no. 4, pp. 695-703, Apr. 2014.

[15] BossBase image database, [Online]. Available: http://agents.fel.cvut.cz/stegodata/RAWS

