Indian Journal of Science and Technology, Vol 9(29), DOI: 10.17485/ijst/2016/v9i29/85816, August 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Implementation of Separable Reversible Data Hiding Scheme in Image Encryption Process

P. L. Ajitha Merlin[1] and V. Rajamani[2]

[1]Department of Electrical and Electronics Engineering, St. Peter's University, Tonakela Camp Road, Sankar Nagar, Avadi, Chennai - 600054, Tamil Nadu, India; ajithamerlin@gmail.com
[2]Department of Electronics and Communication Engineering, Veltech Mutitech Dr. Rangarajan Dr. Sakunthala Engineering College, 42, Alamathi Road, Avadi, Thiruvallur, Chennai - 600062, Tamil Nadu, India; rajavmani@gmail.com

Abstract

Background/Objectives: Image encryption includes a vital role within the field of cryptography. Within the planned theme compression technique is introduced when the encryption and information concealment method to cut back the image size for quicker transmission. **Methods/Statistical Analysis:** Encryption scheme, 2 individual keys are used for image cryptography & information concealment with high level of security to safeguard a picture from unauthorized access. The owner of the content encrypts the first image that is not compressed by using a cryptography key. The LSBs of the image encrypted are compressed employing an information concealment key to form an area to imbed an extra information. Haar wavelet compression technique and Run - Length coding (RLC) were used. **Findings:** At the receiver end, the quality of the image retrieved and the information extracted are achieved solely from Run–Length Coding with their several keys. Extracted image quality is analyzed by standard and subjective metrics index are measured. **Application/Improvements:** Image Quality Assessment (IQA) technique shows the standard of retrieved image is same as that of the first image.

Keywords: Cryptography, Encryption, Haar Wavelet, Run Length Coding

1. Introduction

In the recent times, transmission of secured images plays a vital role in the field of cryptography. It is used for protecting the data. RLC method is a lossless scheme used for compressing the image by removing the spatial redundancy. They are implemented in[1]. If there are immediate transitions or changes, then Haar wavelet is applied to model using HVS[2].

In[6] encryption key is used for image encryption and also the data embedding is performed in an image exploiting data concealment key, with a disadvantage at the decoding stage is merely if data – hiding key and encryption key is known, then with the help of spatial correlation in natural image embedded knowledge is extracted properly and original image is recovered absolutely. Medical images are encrypted with this data concealment key within the non – Region of Interest (ROI) space of an image is bestowed[7].

A completely unique lossless data-embedding technique is bestowed in[18], to change the precise recovery of the first host signal upon extraction of the embedded data by generalizing the well-known least significant bit (LSB) modification and introduces extra operative points on the capacity-distortion curve. In[20], a completely unique high capability data concealment methodology is framed for JPEG images by using a capability table to estimate the quantity of bits that may be hidden in every DCT element in order that important distortions within the stego-image is avoided. A good performance comparison is performed between the varied cryptography symmetric and asymmetric techniques primarily based algorithms like the Advanced Encrypted standard (AES), Rivest-Shamir-Adleman (RSA), Rivest Cipher (RC2),

*Author for correspondence

data encryption standard (DES), 3DES, Digital Signature algorithm (DSA) are mentioned[21] and these encryption algorithms aren't utilized in our proposed theme due to its disadvantages. In[22], a new feature similarity (FSIM) index for full reference IQA is planned which is based on the very fact that human visual system (HVS) understands a picture primarily in line with its low-level features using section Congruency as the primary feature in FSIM. The performance of 11 chose full reference Image Quality Assessment (IQA) algorithms is tested on all the seven public IQA image datasets in[23].

This work performs a new dissociable reversible data hiding theme combined with compression techniques. Compression technique is used additionally with the prevailing dissociable reversible data concealment technique[24] for quicker transmission. An analysis is formed with each lossy Haar wavelet and lossless RLC compression techniques. From the analysis higher image and data retrieval is achieved in lossless compression technique[25]. Implementation in the Hardware is performed for the encryption and decryption method in Xilinx ISE machine. The overall manuscript is partitioned as follows. The section 2 demonstrates the planned theme. Image encryption key based encryption technique is represented in section 2.1. The Section 2.2 deals with data embedding scheme. Section 2.3 deals with lossy Run-Length Coding and lossless Haar wavelet. Section 2.4 deals with the decryption section recovering the content with their various keys. Section 3 shows the results of the proposed theme. Data embedding and image encryption process: results, application and extension of this analysis are shown in section 4.

2. Proposed Scheme

Ordinarily encryption is improved image recovery. In this plan, compression strategies are utilized after the encryption to separate the substance with high level of accuracy and compression proportion. The proprietor makes use of an 8 bit key to encrypt the image. A 28 – bit data key is inserted into the hiding data. The compression scheme comprises of both lossy and lossless systems. Decompression is performed and substance is recovered in view of their particular keys. In the Decoding stage, encryption key is utilized to recuperate the image and information concealment key is utilized to extricate the implanted information. Steps need to handle the proposed plan is plainly appeared in Figure 1.

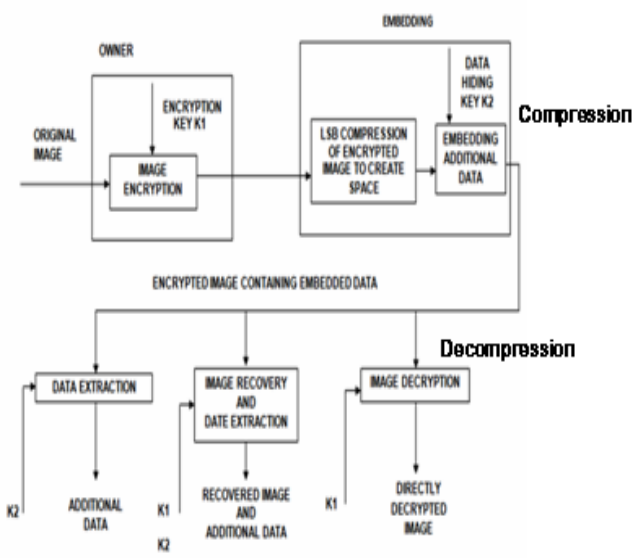

Figure 1. Block diagram of the proposed scheme.

2.1 Image Encryption

The image encryption is performed by using a 8 bit long key. The image is the original gray scale image with its gray values between 0 and 255. The encrypted bits are obtained by XORing the original bits and key bits.

2.2 Data Embedding

In this process of Data Embedding, the encrypted pixels are selected for hiding the data by incorporating the keys K2, M, L and S. They represent the bits of an uncompressed image that is encrypted, number of unions, no of pixels taken from LSB respectively.

2.3 Compression Technique

This technique is used to compress the image for speedier data transfer. The two techniques used are:

- Haar Wavelet Lossy Technique
- RLC Lossless Technique

2.3.1 Lossy Compression Technique

The sum and difference of adjacent components are calculated by using Haar wavelet method. Firstly this is applied on horizontal components and then on vertical components. The upside of Haar wavelet scheme is the

examination of sudden moves present in a picture that is conceivable. Haar wavelet method is not nonstop one so we can't separate effortlessly, taking into account this issue picture recovery and the size of the picture is also reduced.

2.3.2 Lossless Compression Technique

In the lossless compression system, Run-Length Coding is utilized for encoded image with installed information. The estimation of the gray pixels along a line of succession in a computerized image is considered as numbers. Length of the steady gray level pixels esteem with the line is spoken to by ni. The RLC is used to exploit the spatial redundancy and therefore the image size can be compacted to 20 KB. Image recovery is thus conceivable.

2.4 Data Extraction and Image Recovery

Reverse process of compression is the initial step at the receiver side[26]. Figure 2 shows the proposed scheme flow with their output results.

3. Implementation in the Hardware

The process of encryption and decryption is implemented using the XC3S100E FPGA. The code has been written using VHDL. First the encryption phase takes place and then decryption phase follows. The appropriate key is ought to be given to decrypt the image. As the space meant for storing the images in FPGA is less, the size of the images ought to be 32*32. The outcomes obtained from the FPGA unit is appeared in Figure 3(a) and Figure 3(b).

4. Results and Discussion

For the experimental investigation, the Lena Image has been considered. It is of the size 512*512. It has been displayed in Figure 4(a). An 8 bit key is used for encrypting the pixels in the input side. 34950 bits are padded to the image that is encrypted. The parameters are set to be as 2,15,2 for M, L and S respectively. The rate of embedding the data is 0.1333 bpp and the results are displayed in Figure 4(c).

By utilizing the compression based on haar wavelet method, it is watched that the quality of the image is poor as appeared in Figure 5(a) and additionally data extraction is not accurate, results are appeared in reenacted waveform in Figure 5(b). In this way, the RLC compression method is utilized for the compression of an encrypted image for better recuperation and information extraction. Performance analysis results tried amongst information and yield Lena image is recorded in Table 1. PSNR esteem acquired from the distinctive tried images is appeared in Figure 6.

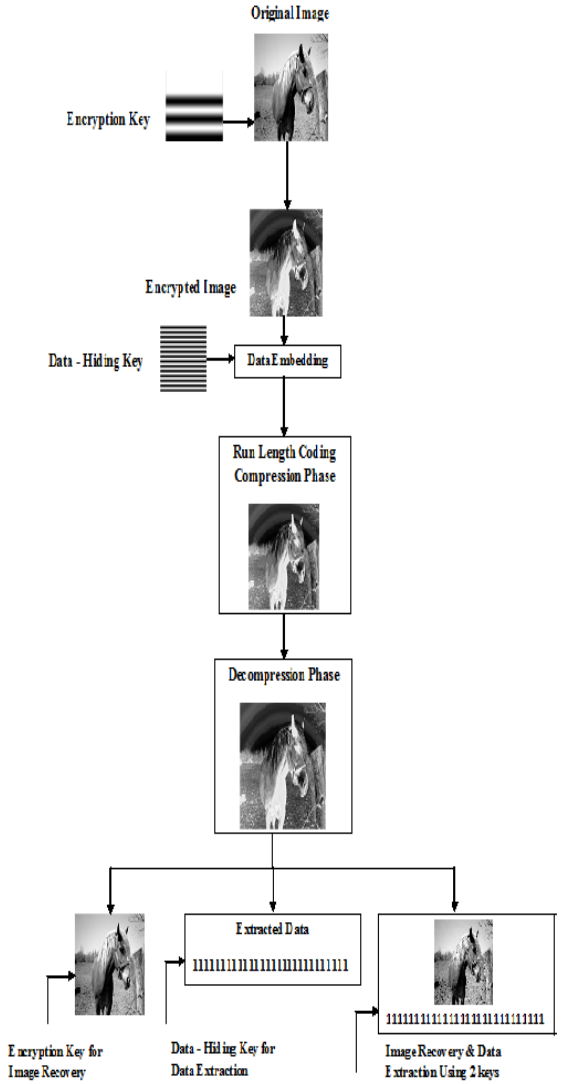

Figure 2 Image encryption and data embedding flow diagram.

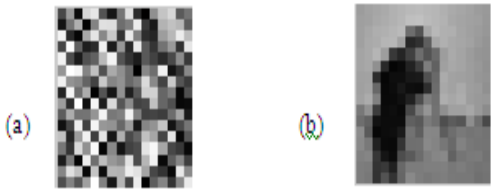

Figure 3 Hardware implementation of (a) Encrypted image and (b) Decryption image.

Figure 4 RLC Compression Technique Results, (a) Tested image, (b) Encrypted image and (c) Decrypted image.

Figure 5(a) Image Retrieval from Haar Wavelet Compression (White grains are present inside the image)

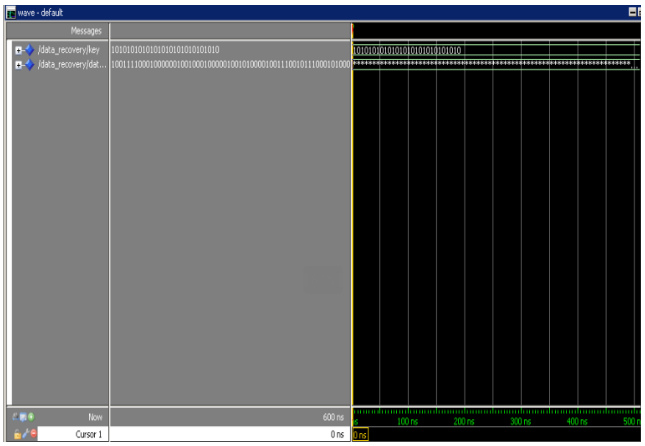

Figure 5(b) Simulation result showing data extractions using Haar wavelet

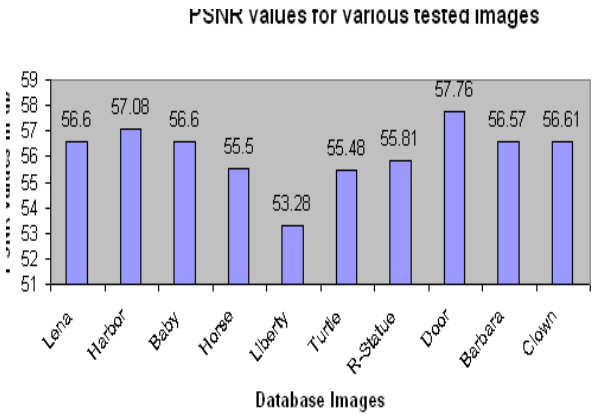

Figure 6 PSNR values for various tested images

From the Table 1, PSNR values are high, which shows image quality is good. Mean, variance and standard deviation values of input image (original image) are equal to values of an output image (decrypted image). This result shows statically decrypted image is equals to the original image (pixel values are unaltered).

7. Conclusion and Furture Enchancement

A novel methodology incorporating separable information concealment using reversible method is employed for the encryption process. The input data is encrypted by using a key. Data concealment key pads the LSB of the encrypted data for embedding the data. The lossy method based on Haar wavelet technique was not able to accomplish the retrieval of the image when compared to the Run-Length Coding method. Both the methods of Image encryption & the keys used for hiding will be used for

Table 1. Performance analysis results tested between input and output images.

Tested image	Measured Parameters	Input Image	Output Image	Quality
Lena	PSNR	-	56.6292 db	Excellent
	Mean	124.1080	124.3872	
	Variance	2.2551e+003	2.2581e+003	
	Standard Deviation	47.4877	47.5197	
Harbor image- A57	PSNR		57.0835	Excellent
	Mean	125.9987	126.2823	
	Variance	1.5646e+003	1.5669e+003	
	Standard Deviation	39.5551	39.2837	
Baby Image- A57	PSNR		56.6008 db	Excellent
	Mean	177.8406	178.1094	
	Variance	2.9400e+003	2.9429e+003	
	Standard Deviation	24.2214	24.2214	
Horse image-A57	PSNR		55.5018db	Excellent
	Mean	158.325	158.325	
	Variance	1.9302e+003	1.9302e+003	
	Standard Deviation	42.625	42.635	
Liberty Statue -CSIQ	PSNR	-	53.2836 db	Moderate
	Mean	177.8406	154.1589	
	Variance	2.9700e+003	1.2911e+003	
	Standard Deviation	54.2214	35.9314	
Turtle-CSIQ	PSNR		55.4887 db	Excellent
	Mean	106.1182	106.3548	
	Variance	2.7006e+003	2.7081e+003	
	Standard Deviation	51.9672	52.0393	
Roman Statue -TID2008	PSNR		55.8131 db	Good
	Mean	77.8715	78.1150	
	Variance	2.3398e+003	2.3440e+003	
	Standard Deviation	48.3714	48.4145	
Door image- TID2008	PSNR		57.7647 db	Good
	Mean	79.2085	79.5156	
	Variance	649.9072	652.0090	
	Standard Deviation	25.4933	25.5362	
Barbara Image- IVC	PSNR		56.5781 db	Excellent
	Mean	113.7633	114.0316	
	Variance	2.2194e+003	2.2219e+003	
	Standard Deviation	47.1102	47.1369	
Clown -IVC	PSNR		56.6156 db	Good
	Mean	95.7828	96.0528	
	Variance	3.3217e+003	3.3241e+003	
	Standard Deviation	57.6345	57.6551	

extracting the needed original content. The results prove that it is very similar to the Human Visual System (HVS) and with the best quality reports.

8. References

1. Kodituwakku SR, Amarasinghe US. Comparison of Lossless Data Compression Algorithms for Text Data. Indian Journal of Computer Science and Engineering. 2010; 1(4):416-25.
2. Lai YK, Kuo JCC. A Haar Wavelet Approach to Compressed Image Quality Measurement. Journal of Visual Communication and Image Representation. 1999; 11(1):17-40.
3. Alam FI, Khanam Bappee F, Khondker FUA. An Investigation Into Encrypted Message Hiding Through Images Using LSB. International Journal of Engineering Science and Technology (IJEST). 2011; 3(2):948–60.
4. Bhattacharyya D, Roy A, Roy P, Kim TH. Receiver Compatible Data Hiding in Color Image. International Journal of Advanced Science and Technology. 2009; 6(5):15-24.
5. Puech W, Chaumont M, Strauss O. A Reversible Data Hiding Method for Encrypted Images. San Jose, CA, USA: SPIE, IS&T'08: SPIE Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents. 2008.
6. Zhang X, Reversible Data Hiding in Encrypted Image. IEEE Signal Processing Letters. 2011; 18(4):255–58.
7. Lavanya A, Natarajan V. Watermarking patient data in encrypted medical images. Indian Academy of Sciences. 2012; 37(6):723–29.
8. Indrakanti SP, Avadhani PS. Permutation based Image Encryption Technique. International Journal of Computer Applications. 2011; 28(8):45–47.
9. Yadav D, Singhal V, Bandil DK. Reversible Data Hiding Techniques. International Journal of Electronics and Computer Science Engineering. 2012; 1(2):380-83.
10. Johnson M, Ishwar P, Prabhakaran V. Schonberg D, Ramchandran K. On Compressing Encrypted Data. IEEE Transactions on Signal Processing. 2004; 52(10):2992–3006.
11. Fallahpour M, Megias D, Shi YQ. Lossless Image Data Embedding in Plain Areas. SPIE Proceedings. 2011; p. 872-77.
12. Krikor L, Baba S, Arif T. Image Encryption Using DCT and Stream Cipher. European Journal of Scientific Research. 2009; 32(1):48-58.
13. Gautam A, Panwar M, Gupta PR. A New Image Encryption Approach Using Block Based Transformation Algorithm. International Journal of Advanced Engineering Sciences and Technologies. 2011; 8(1):90–96.
14. Rathod H, Sisodia MS, Sharma SK. Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm). International Journal of Computer Technology and Electronics Engineering (IJCTEE). 2011; 1(3):7–13.
15. Zhang X. Reversible Data Hiding with Optimal Value Transfer. IEEE Transactions on Multimedia. 2013; 15(2):316–25.
16. Hong W, Chen TS, Wu HY. An Improved Reversible Data Hiding in Encrypted Images Using Side Match. IEEE Signal Processing Letters. 2012; 19(4):199–202.
17. Fallahpour M. Reversible Image Data Hiding based on Gradient Adjusted Prediction. IEICE Electronics Express. 2008; 5(20):870–76.
18. Celik MU, Sharma G, Tekalp AM, Saber E. Lossless Generalized-LSB Data Embedding. IEEE Transactions on Image Processing. 2005; 14(2):253–66.
19. Imran AS, Javed MY, Khattak NS. A Robust Method for Encrypted Data Hiding Technique Based on Neighborhood Pixels Information. International Journal of Computer Science and Engineering. 2007; 1(3):159–64.
20. Tseng HW, Chang CC. High Capacity Data Hiding in JPEG-Compressed Images. Informatica. 2004; 5(1):127–42.
21. Jeeva AL, Palanisamy V, Kanagaram K. Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms. International Journal of Engineering Research and Applications (IJERA). 2012; 2(3):3033-37.
22. Zhang L, Zhang L, Mou X, Zhang D. FSIM: A Feature Similarity Index for Image Quality Assessment. IEEE Transactions on Image Processing. 2011; 20(8):2378-86.
23. Zhang L, Zhang L, Mou X, Zhang D. A Comprehensive Evaluation of Full Reference Image Quality Assessment Algorithms. Orlando, FL: 2012 19th IEEE International Conference on Image Proceesing, ICIP. 2012; p. 1477-80.
24. Zhang X. Separable Reversible Data Hiding in Encrypted Image. IEEE Transactions on Information Forensics and Security. 2012; 7(2):826–32.
25. Tamilselvi R, Ravindran G. Image Encryption using Pseudo Random Bit Generator Based on Logistic Maps with Radon Transform. Indian Journal of Science and Technology. 2015; 8(11):1-7.
26. Smitha M, Jayanthi VE and Ajitha Merlin. Image encryption using separable reversible data hiding scheme. 2013 Fourth International Conference on Computing Communications and Networking Technologies (ICCCNT). 2013.