Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

ISSN NO. 2320-5407

Article DOI: 10.21474/IJAR01/2124
DOI URL: http://dx.doi.org/10.21474/IJAR01/2124

RESEARCH ARTICLE

PERFORMANCE ANALYSIS OF REVERSIBLE DATA HIDING USING AES AND HISTOGRAM SHIFTING.

Nidhi Antony and Rinju Mariam Rolly.
M.Tech Scholar, Assistant Professor, Department of Electronics and Communication, Rajagiri School of Engineering and Technology, Kakkanad, Kerala, India.

Manuscript Info

Manuscript History

Received: 25 September 2016
Final Accepted: 27 October 2016
Published: November 2016

Key words:-
AES, Histogram Shifting, Logistic Map, RDH, Performance Analysis.

Abstract

Reversible data hiding is a prominent field in secure communication. Its importance has been increasing nowadays due to lossless recovery of veiled data and cover image. Both veiled data and marked image can be extracted separately depending upon the availability of the keys. By means of a security key defined by user the content owner encrypt the cover image by 1D logistic map-chaotic based transposition algorithm. As an alternative to direct embedding of data into encrypted image the proposed method encrypt the data using AES and hence provide twofold layer security. Utilizing another user defined data hiding key the data hider hides AES encrypted data into the encrypted image by shifting its histogram. An assortment of performance analysis is carried out in this paper. Out of different RDH algorithms we use histogram shifting for data embedding since it offers better capacity. Hence, the proposed method is a reliable and secure technique for reversible data hiding.

Introduction:-

With the progression in technology extent of secure communication has gained significance. Security of image and data plays fundamental role in the field of communication. Image and data can be transmitted within seconds to any part of the world. This expertise can be used by terrorists or illegitimate users to hack the off the record documents and classified information. Unpredicted exposure of classified data or images of military, government or any other organizations may lead to terrific impacts. It may splinter the whole security system [7].

In data hiding lossless recovery of cover image is not ensured rather prominence is on recovery of secret data without any loss. Reversible data hiding is a method in which the exact cover image can be retrieved without any loss after the furtive messages are extracted .It is widely used in the field of medical imaging, military, law and government, where distortion of original cover is not allowed. A variety of types of reversible data hiding techniques have been proposed by researchers.

The main aim of this work is to carry out performance analysis of proposed method in [7]. It supports the property of lossless recovery after furtive data is extracted while protecting the cover image's secrecy [3]**.** Cover image is retrieved separately from marked image. In the content owner part cover image is encrypted by using 1D logistic map-chaotic based transposition algorithm [1].

Corresponding Author: - Nidhi Antony, Rinju Mariam Rolly
Address: - M.Tech Scholar, Assistant Professor, Department of Electronics and Communication, Rajagiri School of Engineering and Technology, Kakkanad, Kerala, India.

As an alternative of unswervingly embedding data into encrypted image we encrypt the data using AES for providing twofold layer security. The data hider hides AES encrypted data into the encrypted image by shifting its histogram, which uses an additional user defined data hiding key. Out of an assortment of RDH algorithms we make use of histogram shifting for data embedding since it offers better capacity [6]. Hence, the proposed method is a viable and secure technique for reversible data hiding.

Methodology:-

The methodology of this work is shown in the Fig-1. In the content owner side cover image is encrypted through user-defined security key derived-1D logistic map-chaotic based transposition algorithm. It has more intricate chaotic behaviors. This intricate logistic map is used to generate pseudo random sequences for strong key generation mechanism [1].

A series of pseudorandom numbers are generated by means of the logistic function,$R_{P+1}=T\times R_P\times(1-R_P)$.It uses an image encryption mechanism developed using these pseudo-random sequences under the framework of the transposition network, which is found to be very functional to uphold both confusion and diffusion properties in stream ciphers and block ciphers.

As an alternative of unswervingly embedding data into encrypted image we encrypt the data using AES for providing twofold layer security. The data hider inserts AES encrypted data into the encrypted image by shifting its histogram, which makes use of another user defined data hiding key.

Amongst an assortment of RDH algorithms proposed by researchers we make use of use histogram shifting for data embedding since it offers better capacity and constant PSNR over other methods [6].The block diagram of proposed method is shown in figure 1.It has mainly four sections image encryption using 1D logistic map, data encryption using AES, histogram shifting, data extraction and image recovery. It is explained in detail in following sections.

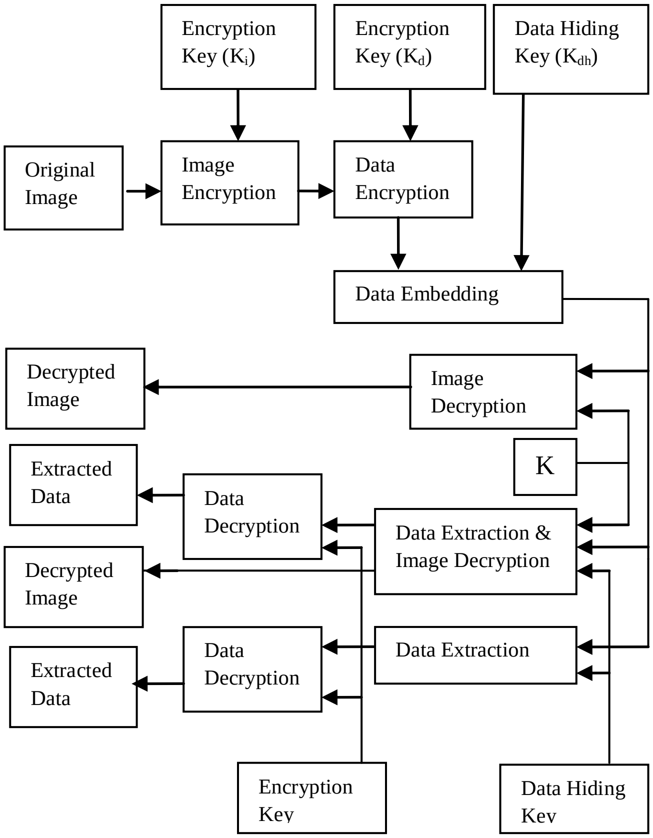


Figure 1:- Block Diagram

Image Encryption using 1D Logistic Map:-

Image encryption is performed using chaotic based 1D logistic map method. Security is improved by exploiting the strength of key derivation mechanism with the aid of 120 bit user defined key called encryption key.

A series of pseudorandom numbers are generated by using the logistic function, $R_{P+1}=T\times R_P\times(1-R_P)$.Where R_P indicates the value of chaotic function at p^{th} iteration and the value of T lies in the range [0, 4]. Usually initial seed of the logistic function lies between [0,1] but as an alternative to unswervingly specifying here algorithm insists the user to enter the 120 bit encryption key and calculate the initial seed from the key. Create N = xy pseudorandom numbers and store up them in a vector C (Chaotic). Arrange the chaotic vector in ascending order.

A location map (LM) is generated by considering the changes in location during sorting. Location map is such that, LM (1) is the original position of smallest value, LM (2) that of second smallest and so on. Sort out image pixels grey levels into a picture vector P (Picture). Rearrange P in accord with the location map LM. Restructure picture vector P into matrix sized m × n to obtain the encrypted image [3].

Data Encryption using AES:-

As an alternative to unswervingly embedding data into encrypted image we encrypt the data using AES for providing twofold layer security. The Rijndael algorithm is the basis of AES.It process data blocks of 128 bits. The cipher keys with lengths of 128, 192, and 256 bits are available. It has four transformations Sub Bytes, Shift Rows, Mix Columns, and AddRoundKey [4].

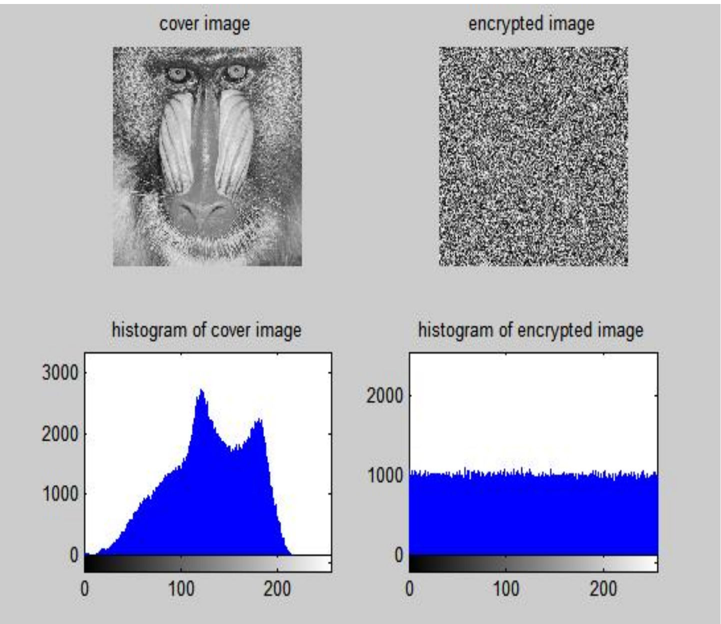


Figure 2:- Image Encryption

Histogram Shifting:-

Existing histogram shifting algorithms utilized the valley point of the histogram of a cover image and then slightly modifies the pixel grayscale values to create legroom for furtive data to be embedded. It has low execution time and low computational complexity**.** It offers a lesser amount of capacity [5].

Step l.The valley point and the peak point of histogram are found. The valley point refers to the grayscale value in which there are no pixels in the given image. The peak point refers to the grayscale value in which there is the maximum number of pixels in the given image.

Step 2. The whole image is scanned in a chronological order, such as from top to bottom, as row-by-row. The range of grayscale value of pixels between 120 (including 120) and 155 (including 155) is incremented by "1", i.e., perturbing the range of the histogram, [120 155] to the right-hand side by 1 unit and leaving the grayscale value 120 empty.

Step 3.Hide the secret data into the grayscale value of 119 and 120.

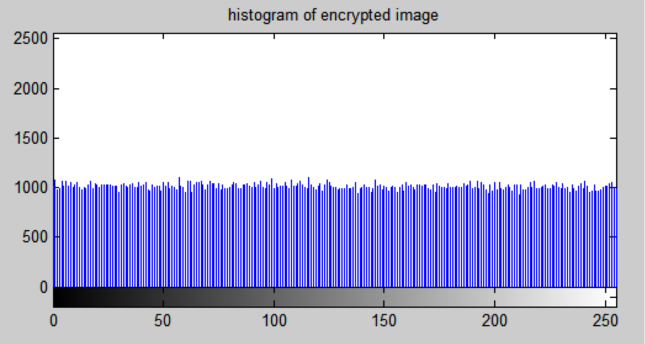


Figure 3:- Histogram with minimum and maximum points

This technique does not have much legroom for hiding data. So when the amount of secret data to be embedded is more the customized approach is used. The customized approach has more embedding capacity. The customized approach is as follows:

Step 1. Find out one peak point which is location of 120 and two valley points which are location of 155 and 210.

Step 2.The location information is stored in location map in turn to recover original images. The location information of the pixels consists of peak point, left valley point, and right valley point.

Step 3. Embedding space is generated by shifting the pixels that are located in histogram between left valley point and left side of the peak point (pixel value of 120) one pixel left.

Step 4. Hide the secret data into the grayscale value of 118 and 119 or 121 and 122.

D. Data Extraction & Image Recovery:-
When the receiver has,

Data Hiding Key alone:-
When receiver has only data hiding key alone and encrypted cover containing veiled message, then extraction of veiled information alone is possible. Decryption of encrypted cover or any small portion or region of encrypted cover will not be possible.

Encryption Key alone:-
When receiver has encryption key alone and encrypted cover containing hidden veiled message, then only the decryption of the cover alone is possible. The extraction of veiled secret message or any splinter of veiled secret message is not possible.

Both Data hiding and Encryption Keys:-
When the receiver has both keys, then both the cover image and hidden data can be retrieved. Hence the condition of separability also satisfied.

Performance Analysis:-
The performance analysis of proposed method is carried out in this paper. We used images lena.tiff, baboon.tiff, grass.tiff, which is of size 676x598 as cover images for analysis. For the simulation we used MATLAB 2013a. Histograms of respective images are shown in figure 4.These images are encrypted via 1D logistic map. The encrypted images and their histograms are illustrated in figure 5.

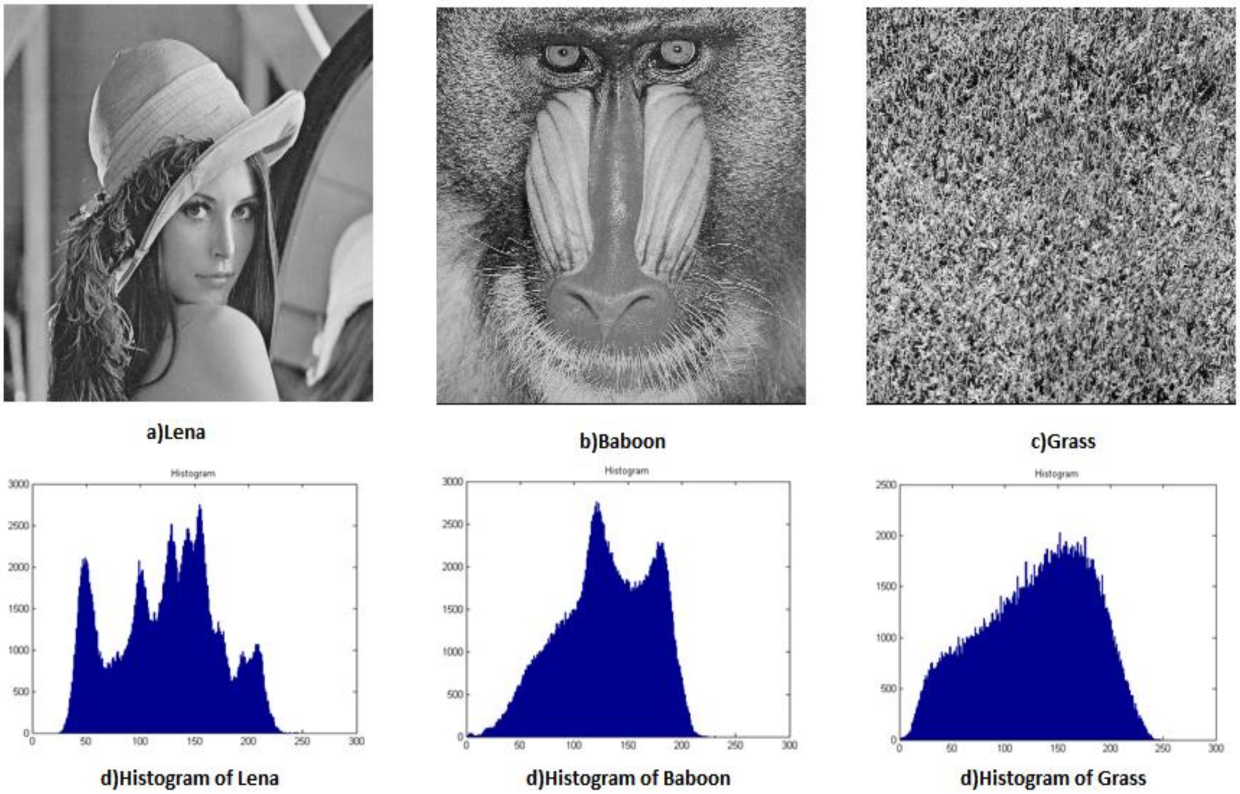
The histogram analysis of encrypted image is one of the basic methods to ensure the encryption quality of the images. Uniformly distributed histogram for encrypted image depicts that encryption method is adept. Since it encrypts a cover image to random-like its altercation to attacks is sturdy [7].

Embedding rate is the ratio of size of bits to number of samples in the host. It is expressed in terms of bpp. Bpp or bits per pixel indicates the number of bits per pixel. The number of different colors in an image is depends on bits per pixel. Location map shows location of each value in image. The graph that illustrates the relationship between embedding rate and location map is for three images are shown in figure 6.In Lena.tiff irrespective of embedding rate location map lies in zero axis. It shows the initial state. In Baboon.tiff and Grass.tiff graph shows exponential behavior.

PSNR is the peak signal to noise ratio. It is one of the most significant feature.PSNR is an approximation to human perception of reconstruction quality. Higher the PSNR value betters the performance. Since higher PSNR indicates less amount of noise in images. Table 1 shows PSNR values of three images for different embedding rates. It is clear from the tabulation that PSNR is higher for 0.1bpp.

Table 2 shows the time elapsed for processing for each images. The proposed method achieves better performance in reversibility, original image recovery at receiver without any loss of information rather than traditional methods.

Various security analysis such as Key space analysis, key sensitivity analysis, histogram analysis, NPCR, information entropy analysis, are performed to guarantee the security of anticipated method as in [7].


a)Lena

b)Baboon

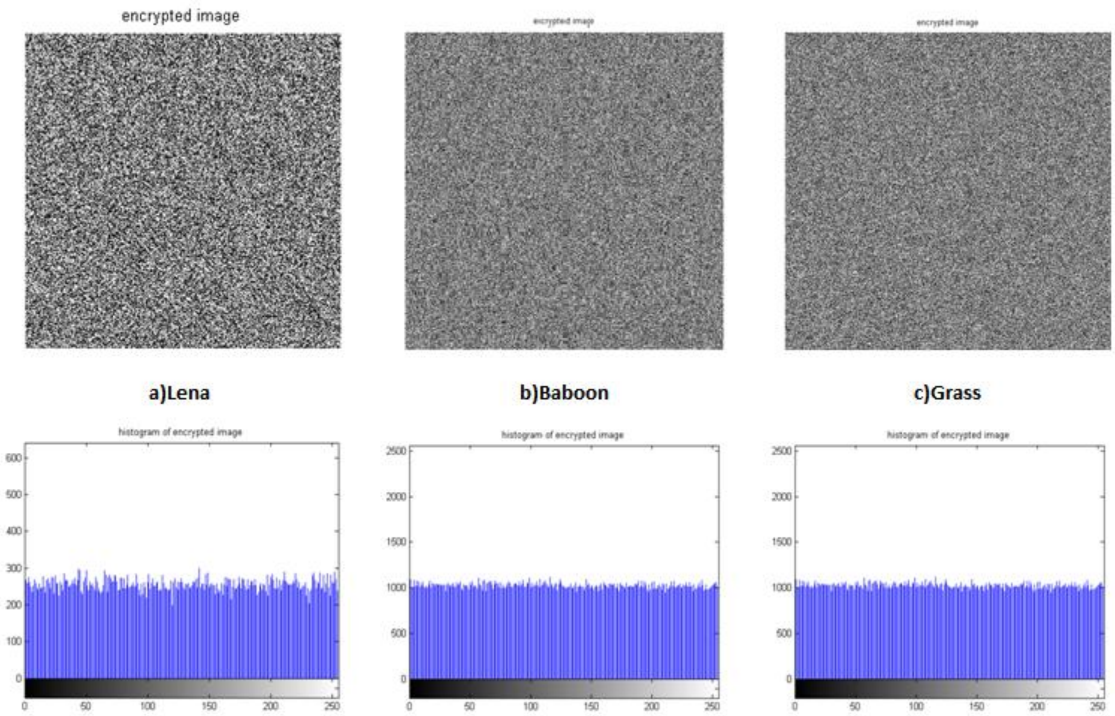
c)Grass

d)Histogram of Lena

d)Histogram of Baboon

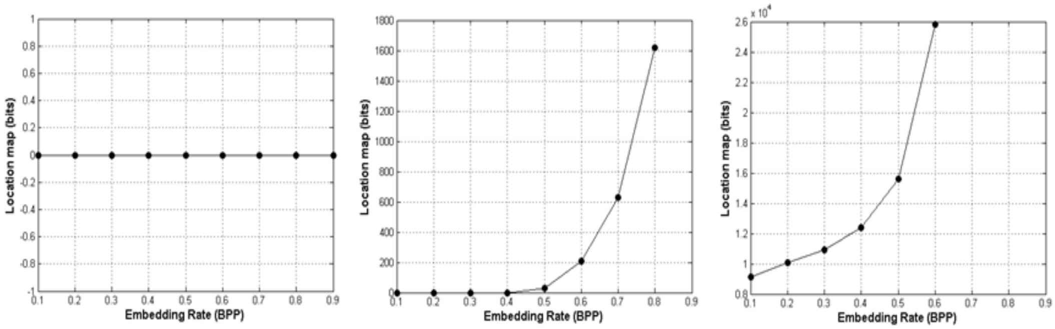
d)Histogram of Grass

Figure 4:- Cover images and Histograms



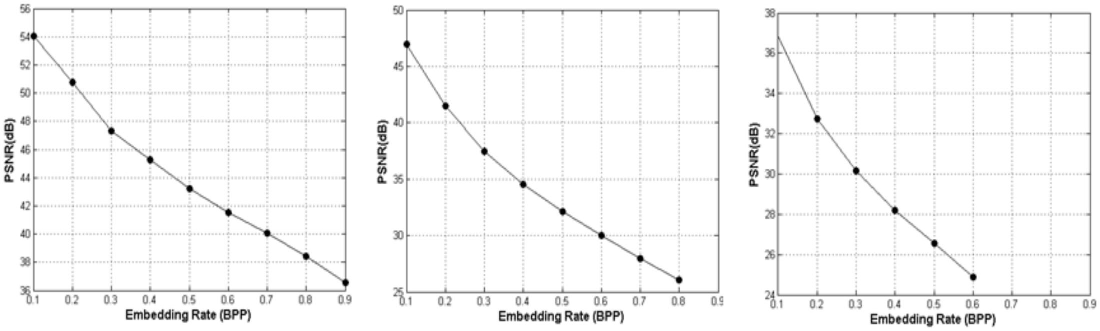
a)Lena b)Baboon c)Grass

Figure 5:- Encrypted images and Histograms



a)Lena b)Baboon c)Grass

Figure 6:- Embedding Rate v/s Location Map.



a)Lena b)Baboon c)Grass

Figure 7:- Embedding Rate v/s PSNR

Table 1:- PSNR for different Embedding Rates

Embedding Rate(BPP)	Lena-PSNR(dB)	Baboon-PSNR(dB)	Grass-PSNR(dB)
0.1	54	47	37
0.2	51	42	32.5
0.3	47.5	38	30
0.4	45.6	34	28
0.5	43.5	32	26.2
0.6	41.8	30	24.5

Table 2:- Execution time.

Image	Execution time(in s)
Lena.tiff	61.445387
Baboon.tiff	45.493662
Grass.tiff	24.229680

Conclusion:-

This work proposes a novel algorithm for secure transmission of data and image with lossless recovery in a separable manner. The algorithm has mainly four sections like image encryption, data hiding, data extraction and image recovery phases. The proposed image encryption method adopts a 1D logistic map based transposition algorithm [1]. This increases the image encryption quality. As an alternative of unswervingly embedding data into cipher text image this method encrypts the data by means of AES algorithm for ensuring twofold layer security. The cipher text image obtained from the proposed image cipher has strong confrontation to all recognized attacks. Performance analysis of proposed method was carried out.It includes Histogram analysis, Embedding rate v/s Location map, Embedding rate v/s PSNR, Execution time. PSNR values of three images for different embedding rates were calculated.

References:-

1. Y.Wu, G.Yang, H.Jin and J.P. Noonan, “Image Encryption using the Two-dimensional Logistic Chaotic Map”, in Journal of Electronic Imaging, January 2012.
2. K.Ma, W.Zhang, X.Zhao, N.Yu, and F.Li, “Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption”, in IEEE Transactions On Information Forensics And Security, Vol. 8, No. 3, March 2013.
3. A.K.Mohan, S.M.R and K.Anusudha, “Improved Reversible Data Hiding Using Histogram Shifting Method”, in Proceeding(s) of Signal Processing, Informatics, Communication and Energy Systems (SPICES), IEEE Conference, 2015.
4. J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999.
5. J.Gupta, P.Gupta, S.C.Gupta, “Reversible Data Hiding Technique Using Histogram Shifting”, in Proceeding(s) of 2nd International Conference on Computing for Sustainable Global Development (INDIA Com), 2015.
6. M.Nosrati, R.Karimi and M.Hariri, “Reversible Data Hiding: Principles, Techniques, and Recent Studies”, World Applied Programming, ISSN: 2222-2510, Vol (2), Issue (5), May 2012. 349-353.
7. Nidhi Antony, Rinju Mariam Rolly, “Security Enhanced Reversible Data Hiding using AES and Histogram Shifting”, International Journal of Research in Advent Technology, Vol.4, No.3, March 2016. E-ISSN: 2321-9637.
8. X. Zhang, “Reversible Data Hiding in Encrypted Images,” IEEE Signal Process. Lett., Vol. 18, No. 4, pp. 255–258, Apr. 2011.
9. X. Zhang, “Separable Reversible Data Hiding in Encrypted Image,” IEEE Trans. Inf. Forensics Security, Vol. 7, No. 2, pp. 826–832, Apr. 2012.