ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Engrafting Data Using RDH by Reserving Room before Encryption

[1] G.Abinaya, [2]Deepanshu Garg, [3]Sarthak Kabra,[4] Shivani Priya, [5]Akanksha Priya
[1] Assistant Professor (O.G)
[1][2][3][4][5] Computer Science and Engineering, SRM Institute of Science and Technology
Ramapuram, Chennai, Tamil Nadu

Abstract: There is also a large number of tasks on data covering in the engrafted field. Most of the work on RDH concentrates on the encryption and decryption of the data. This method is by reserving a room before encryption using traditional RDH a technique, and thus it is simple for the data hider to reversible engrafts the data in the engrafted image. The method that we are proposing can accomplish real reversible-ness, and extraction of data and recovery of the picture are free of any fault. Thus the data hider can profit from the additional space Released out in the prior stage to make data hiding method smooth. The stated scheme can take benefit of all regular RDH procedures for definite pictures. It obtains great description without loss of perfect privacy. Furthermore, this new method can obtain actual reversibility, separate data wrenching and an excellent growth on the quality of marked decrypted Pictures. Testing showed that this scheme can secure more than ten times as extensive payloads for the same picture quality as the prior schemes. The data extraction and image recovery can be achieved by examining the block smoothness. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small dimension of encrypted data. With an encrypted image containing additional data, first we decrypt it using the encryption solution, and the decrypted version is similar to the original picture. According to the data-hiding key, with the aid of spatial similarity in a natural image, the embedded data can be successfully obtained and the original image can be perfectly revived.

Keywords: Encryption, Encrypted Image, Image Processing, Decryption, AES Algorithm, BitXOR

I. INTRODUCTION

An image is a matrix of pixels (square). Image processing converts an original image into digital image to transfer critical information. Due to advancements in technology Digital Image transmission has become a keen interest. Data security and discretion are important modules while transacting over internet. Encryption and decryption plays a vital role in providing Data security. Encryption involving mathematical algorithms and cryptographic keys to convert digital data into encrypted code for transmission over the channel. The inverse of the same algorithms are followed to decrypt the code at the receiving end. Various algorithms and techniques have been proposed over time to secure data (digital). One of the modern ones is Advanced Encryption Standard (AES). It is a symmetric cryptographic algorithm that can be executed over various hardware and software languages. Its high security standard makes it difficult for the intruder to obtain crucial information. AES may choose any one from 128, 192, 256 bits. In this research we chose 128 bit key to engraft data using Reversible Data Hiding (RDH) by Reserving room before encryption.

The process is saving Room before encryption with a popular RDH algorithm, and thus it is obvious for the data hider to reversibly secure the data in the encrypted picture. In the technical world, there is also a very large number of tasks on data hiding in the encrypted domain. The reversible data hiding in an encrypted picture is reviewed in. Reversible data hiding concentrates on the data embedding and obtaining on the common spatial region because most of the work depends on them. The suggested scheme can obtain true reversibility. The wrenching of data and recovery of the real picture are free of any fault. Thus the data hider can serve as the additional space Spilled out in the previous step to make data hiding process effortless. The proposed method can take benefit of all regular RDH methods for plain pictures and obtain great achievement without sacrifice of perfect secrecy.

Furthermore, this novel scheme can obtain true re-versibility, separate data wrenching and a great development on the quality of marked decrypted Pictures. Experiments show that this scheme can secure more than ten times as extensive payloads for the same picture

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

quality as the prior systems. The data extraction and image recovery can be achieved by examining the block smoothness. After encrypting the entire data of an uncompressed image by a stream cipher, the extra data can be inserted into the picture by transforming a small dimension of encrypted data.

2. EXISTING SYSTEM

In the present Scheme, we are paying more consideration to reversible data hiding in encrypted pictures. Since it preserves the crucial quality that the initial cover can be lossless revived after inserted data is extricated while protecting the picture contents confidentiality. prior techniques embed data by reversibly vacating room from the encrypted pictures, which may be subject to un-usual fallacies in data removal and/or picture. Prior systems achieve RDH in encrypted pictures by leaving a place after encryption, as exposed to which we introduced by keeping a place before encryption. Thus the data hider can benefit from the extra space emptied out in the previous stage to make data hiding process effortless.

2.1. Disadvantages

The hackers obtain the embedding data in real picture because of the data stored in distinct bit position. Prior schemes insert data by reversibly leaving a place from the encrypted pictures, which may be directed to some faults in data wrenching and/or picture rehabilitation to attack the hidden data using the original image because referred the key value.

3. PROPOSED SYSTEM

The scheme can take benefit of all common RDH techniques for plain pictures and produce correctly production without loss of perfect privacy. This scheme can obtain real reversibility, separate data extraction and hugely develop the quality of marked decrypted images. the method of maintaining a room ere encryption with a popular RDH technique, and therefore it is easy for the data hider to reversibly safe the data in the encrypted picture. We can obtain original reversibility, that is, extraction of data and picture recovery is independent of any fault.

3.1. Advantages

This method can obtain true reversibility. The ex-traction of data and recovery of the real picture are free of any fault.

It is easy for the data hider to reversibly secure data in the encrypted picture. This scheme can secure more than ten times as extensive payloads for the same picture spirit as the initial schemes.

3.2. Advanced Encryption Standard (AES)

The most popular and widely used engrafting algorithm is Advanced Encryption Standard (AES). This algorithm at least six times faster than triple DES. DES key size is too small so, replacement of DES was needed. Because hackers can easily access the key. Triple DES was designed to overcome to solve this drawback but it was very slow. There are some features of AES as follows:

The symmetric key symmetric block cipher
Data is 128 bit, and keys are 128/192/256 bits. It is stronger and faster than triple DES.
It gives full specification and design details.

The software is implementable in Java and C. AES is based on Substitution and permutation. It contains a set of combined procedures, some of which include renewing in-puts by particular outputs (substitutions) and others include rearranging bits around (permutations). AES operates all its calculations on bytes rather than bits. Hence, AES handles the 128 bits of a plaintext segment as 16 bytes. These 16 bytes are systematized in four columns and four rows for processing as a model (matrix)-

The number of rounds in AES is changeable and depends on the extent of the key. AES uses 10 rounds, 12 rounds and 14 rounds for 128-bit keys,192-bit keys, and 256-bit keys respectively. Each of these rounds uses a separate 128-bit round key.

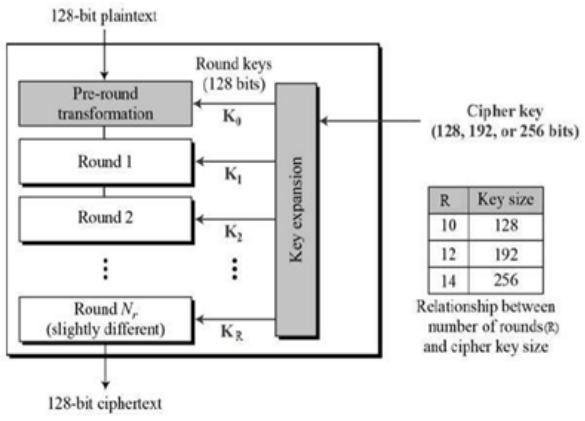

Figure 1. AES Structure

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

3.2.1. Encryption Process- In AES algorithm each round comprises of four sub-methods. The first round method is described below

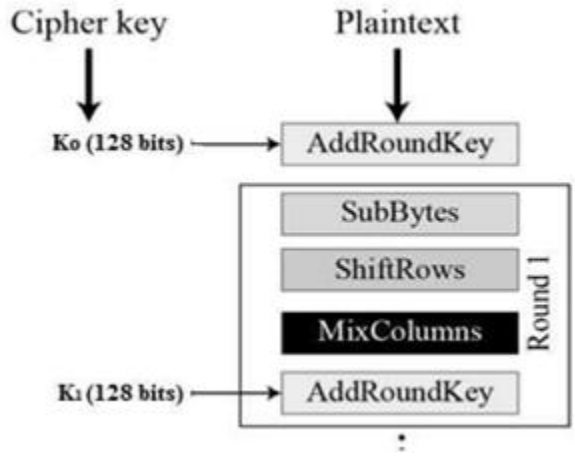

Figure 2. Add Round Key Process

3.2.2. Byte Substitution (SubBytes)- The 16 input bytes are replaced by seeing up to a fixed table (S-box). The de-cision is in a model (matrix) of four rows and four columns.

3.2.3. Shiftrows- Each of the four rows of the model (matrix) is shifted to the left. Any entries that fall off are re-inserted on the right side of the row. The shift is carried out as follows

The first row is not shifted.
The second row is shifted one (byte) position to the left.
The third row is shifted two positions to the left.
The fourth row is shifted three positions to the left.
The result is a new matrix consisting of the same 16 bytes but substituted with reverence to each other.

3.2.4. MixColumns- Each column of four bytes is now modified using a special numerical function. This function takes as input the four bytes of one column and outputs four entirely distinct bytes, which replace the initial column. The result is another new matrix consisting of 16 distinct(new) bytes. It should be remarked that this step is not accomplished in the last round.

3.2.5. Addroundkey- The 16 bytes of the model(matrix) is now acknowledged as 128 bits and perform XOR operation to the 128 bits of the round key. And is current round is the last round then the production is the cipher text. Oppositely the resulting 128 bits are translated as 16 bytes and we begin a different alike round.

3.2.6. Decryption Process. The decryption process of an AES is similar to the encryption method in the reversed order. Each round consists of the four methods (processes) managed in the reverse order

Add round key Mix columns Shift rows

Byte substitution

4. ARCHITECTURE

A random image is selected by the user to embed data over it (image) using an encryption key is generated by AES (Advance Encryption Standard) algorithm. Additionally, that critical data is also encrypted using public key and private key method. This image is divided into a matrix of rows and columns. So the process of embedding data over the image is called as Data embedding. Then that embedded image is encrypted using Reversible Data Hiding (RDH) to add additional security layer over the confidential data. Also by Reserving Room Before Encryption the efficiency of the data over image encryption is also increased. This process is referred as Image Encryption. Then multiple blocks of this image are created for efficient transfer through channel. This is done

Figure 3. Image Processing Architecture

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

5. MODULES

5.1. Reversible Data Hiding

Reversible data hiding is very valuable for some remarkable picture such as pharmaceutical images and armed images. In the reversible data hiding schemes, some schemes are big accomplishment at hiding ability but have a bad cover image quality, some schemes are good cover picture essence but have a low hiding ability. It is hard to find the equilibrium between the hiding ability and cover picture essence. In this document, a novel reversible data hiding system is intended. The proposed scheme uses a new embedding method, which is called Even-Odd embedding method, to keep the cover image quality in an acceptable level, and uses the multilayer embedding to increase the hiding capacity.

5.2. Image Encryption

This module illustrates the encryption of picture to be broadcasted. In this, we are using visual cryptography algorithm to encrypt the picture. So first the image is converting into streams of the data array and each data will be encrypted. The shares will be created based on the number of users. For example, if 5 users are there means we create five shares. For each share, the user can reveal the image but only after five shares he can view the full image. This algorithm not uses the encryption key because if the key is obtained by some unauthorized person then he will reveal the image very easily. Figure 2. shows the image encryption process.

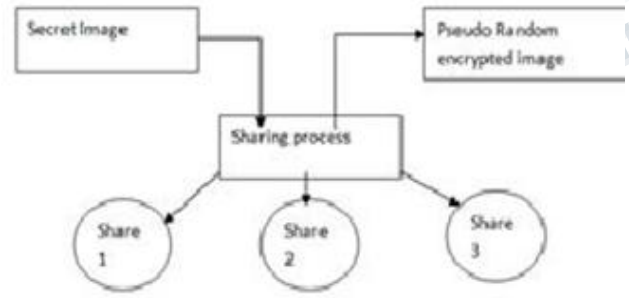

Figure 4. Image Encryption Process

5.3. Data Embedding

This module describes the embedding the data for secret sharing. It takes one random encrypted image. Watermark gives the identification of the provider. Here LSB algorithm for data embedding is used. Before data hiding, we first encrypt the data using a secret key. The embedding a technique of watermark is given as follows.

Assume that the size of the host image is 512512. Host image is divided into small MM blocks Z, block Z is divided into small M blocks Y. If M=8 is used, the size of block Y is 88.

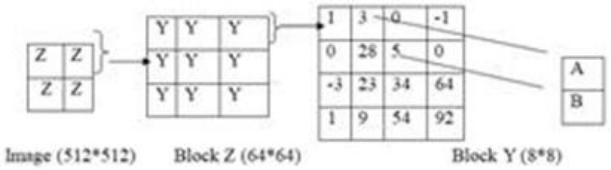

Figure 5. Image Resizing and Data embedding

A number of pairs of coefficients (A,B) in block Y are chosen as A = a1, . . . , an, B = b_1. . . b_n based on a pseudo-random numbers, and mapping key that contains index of original chosen coefficients are kept.
For embedding, two coefficient values (a_i, b_i) are modified by add parameter which is a parameter for watermark strength. i=1,, n.

Continue the above process according to n. Each block Y is embedded 1 bit watermark and watermark length decides how many blocks Y is embedded.

$$X_{i;j} \quad 0 \quad X_{i;j} \quad 1; :::; X_{i;j} \quad 7$$
$$X_{i;j}\, a \quad = \quad \overset{..}{2^{a}} \quad \#_{mod2} \quad a = 0; 1; :::; 7: \qquad (1)$$
$$\underline{\quad X_{i;j} \quad}$$

The encrypted bits can be calculated through XOR operation

$$E_{i;j}\, a = X_{i;j}\, a \quad b_{i;j}\, a \qquad (2)$$

where

$E_{i;j}\, a$ = Encrypted Bits

$b_{i;j}\, a$ = stream cipher encryption key

On Steganography data as based on the linear property of feature extraction. However, ImgSeek assumes the images are with the same scales and orientations. Gabor filtering has better accuracy than ImgSeek for searching similar images with rotated objects. When using Gabor filtering, Steganography is not suitable to protect data anymore, because the feature extraction in Gabor does not show linear properties. Homomorphism encryption can be used in Gabor retrieval because Gabor filtering mostly performs additions and multiplications on encrypted data.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

5.5. Extracting Data from Encrypted Images

To handle and modernize the individual data of pictures which are encrypted for preserving customers secrecy. The mediocre database administrator may only get access to the data hiding passkey. And it has to manipulate data in encrypted domain. The order of data wrenching before picture decryption assures the workability of our job in this situation. When the database administrator receives the data hiding passkey, he can decrypt the LSB- planes of and extract the additional data by directly reading the decrypted version. When inquiring about refreshing data of encrypted pictures, the database manager, then, renews data by LSB replacement and encrypts the modernized data according to the data hiding key all over again. As the whole process is entirely operated on an encrypted domain, it avoids the leakage of original content. The decrypted E' version of containing the embedded data can be calculated by

$$\text{and} \quad X_{i;j}'' \; a = E_{i;j}'' \; a \; b_{i;j} \; a \qquad (3)$$

$$X_{i;j}'' \; a = X_{i;j}'' \; a \; 2^{a} \qquad (4)$$

where

$X_{i;j}''$ a = Binary bits obtained by $X_{i;j}$ a

E'' a = Binary bits obtained by E a

5.6. Extracting Data from Decrypted Images

Into the encrypted images, the cloud server labels the pictures by inserting remarkable cipher code. It includes the identity of the owner of the image and the uniqueness of the cloud server and also timestamps. It manages the encrypted images too. The cloud server has no power to do any Permanent loss to the pictures. An authorized user, Hari who has been assigned the encryption passkey and the data hiding passkey. Who downloaded and decrypted the pictures. Hari expected to get marked decrypted pictures, i.e., decrypted pictures still carrying the symbol, which can be used to determine the origin and records of the data. The series of picture decryption before/without data wrenching is absolutely fitting for this fact. After this, we illustrate how to deliver a marked decrypted picture.

6. EXPERIMENTAL SETUP

In this section we present the experimental results of stego-image on well-known image Lena.

The cover image (Lena) 128*128 (The Message)
The Stego-Media(Lena) 128*128 SRM INSTITUTE

6.1. Feasibility Study

Feasibility analysis is the check of a system proposal according to its workability, influence on the organization, ability to meet user needs, and effective use of recourses. It focuses on the evaluation of existing system and procedures analysis of alternative candidate system cost estimates. Feasibility analysis was done to determine whether the system would be feasible. The development of a computer-based system or a product is more likely plagued by resources and delivery dates. Feasibility study helps the analyst to decide whether or not to proceed, amend, postpone or cancel the project, particularly important when the project is large, complex and costly. Once the analysis of the user requirement is a compliment, the system has to check for the compatibility and feasibility of the software package that is aimed at. A remarkable result of the preparatory research is the measurement that the system inquired is achievable.

6.2. Technical Feasibility

The technology used can be developed with the current types of equipment and has the technical capacity to hold the data required by the new system. This technology supports the modern trends in technology. Easily accessible, more secure technologies. The professional probability of the current method and to what extent it can maintain the suggested expanding. We can add new modules easily without affecting the Core Program. Most of the parts are running on the server using the concept of stored procedures.

6.3. Operational Feasibility

This proposed system can easily be implemented, as this is based on JSP coding (JAVA) and HTML. The database created is with MySql server which is more secure and easy to handle. The resources that are required to implement/install these are available. The personnel of the organization already has enough exposure to computers. So the project is operationally feasible.

6.4. Economic Feasibility

Economic analysis is the various generally used schemes for estimating the effectiveness of a new rule. More generally known cost or bonus judgment, the plan is to define the benefits and gains that are expected from a petitioner method and compare them with values.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

6.5. Experimental Results

Implementation of this project is done in MATLAB environment. The portraits are as follows:

An image is selected by the user to engraft data that is embed data. This image is divided into matrix consisting of multiple rows and columns. As shown in Figure 6.

Figure 6. Selection Of Image

As an image is comprised of three color planes also known as RGB (Red Blue Green). In this implementation we selected blue plane as PSNR (Peak Signal to Noise Ratio) is very less as compared with the other two. Thus efficiency of transfer within the channel increases. Thus that image is transformed into B plane (Blue plane) image.[Figure 7.]

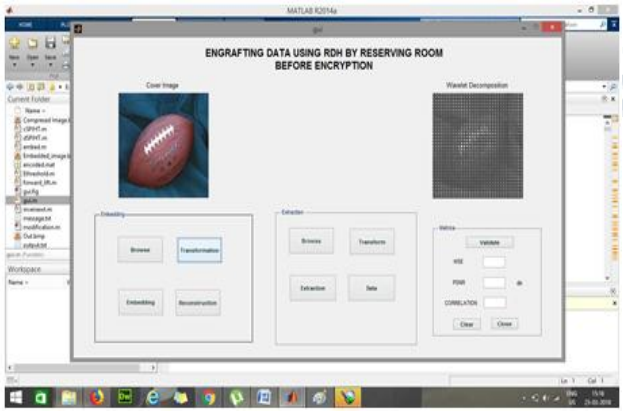

Figure 7. Transformation

The encrypted data is then embedded over the image cells (image is first divided into a matrix) using RDH and by Reserving Room before Encryption. This embedded image is then encrypted and is transferred over the channel in individual blocks (shares). As shown in Figure 8.

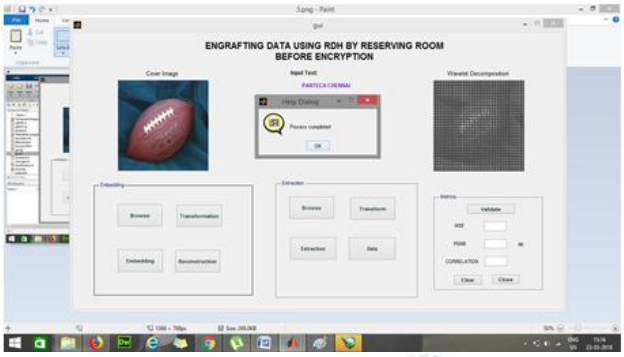

Figure 8. Data Embedding

At the receivers end, each shares of the image acquires its original position and this image is decrypted using the same key used for Image Encryption process and the ciphered data is obtained. This data is then decrypted using the key shared by the user. Refer Figure 9.

Figure 9. Reconstruction

The B plane image is again converted back to its original form. Thus the original image is also received at the receiving end. As shown in figure 10.

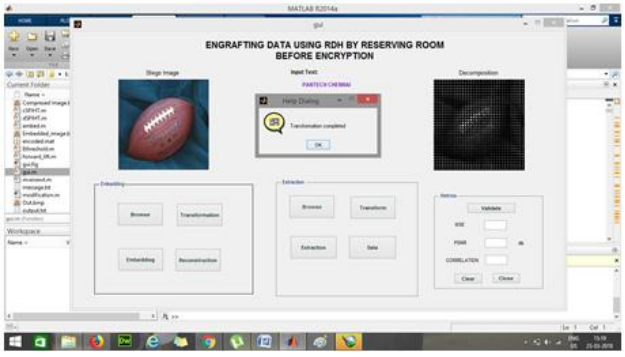

Figure 10. Transformation Process

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

At the end, the receiver extracts the encrypted data and decrypts it and also receives the original image with very less distortion. As shown in figure 11.

Figure 11. Extraction Process

Images	Luoet al	Liet Al	Ouet al	Sachdevet al	Purposed
Fotball	55.79	58.60	59.49	58.26	59.557
Lake	55.33	58.28	58.76	56.64	60.20
Lena	57.37	58.19	59.76	58.24	59.23
beam	54.09	55.54	57.58	56.23	60.444

TABLE 1. PSNR RESULTS FOR DIFFERENT IMAGES

6.6. Implementation Issues

The proposed RDH method has been applied to standard test images including ”football”, ”beam”, ”Lena”, ”lake” which is the size of size 512 512. Table I shows the PSNR for distinct images for embedding capacity of 10,000 bits in which proposed method has achieved high PSNR.
PSNR achieved is very high than any other RDH methods such as Luo et al. [4], Li et al. [9], Ouet al. [10], Sachdev et al. [11], and Drago and Coltuc[12].

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \quad (5)$$

Where
M AX = Maximum Possible Pixel Vallure of Image
MSE = Mean Squared Error
To calculate MSE we use following formula:-

$$MSE = \frac{1}{m\,n} \sum_{X} \sum_{X} [I(i,j) - K(i,j)]^2$$

where
I i; j = Input Image
Ki; j = Reconstructed Image

7. CONCLUSION

A novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases. In the first phase, the content owner en-crypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original con-tent without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. However, the lossy compression method compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

REFERENCES

[1] J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890896, Aug. 2003.

[2] Z. Ni, Y. Shi, N. Ansari, and S. Wei, Reversible data hiding, IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354362, Mar. 2006.

[3] X. L. Li, B. Yang, and T. Y. Zeng, Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection, IEEE Trans. Image Process., vol. 20, no. 12, pp. 35243533, Dec. 2011

[4] L. Luo et al., Reversible image watermarking using interpolation tech-nique, IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187193, Mar. 2010.

[5] X. Zhang, Reversible data hiding in encrypted images, IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255258, Apr. 2011.

[6] X. Zhang, Separable reversible data hiding in encrypted image, IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826832, Apr. 2012

[7] W. Zhang, B. Chen, and N. Yu, Improving various reversible data hiding schemes via optimal codes for binary covers, IEEE Trans. Image Process., vol. 21, no. 6, pp. 29913003, Jun. 2012.

[8]] J. Fridrich and M. Goljan, Lossless data embedding for all image formats, in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572583.

[9] D.M. Thodi and J. J. Rodriguez, Expansion embedding techniques for reversible watermarking, IEEE Trans. Image Process., vol. 16, no. 3, pp. 721730, Mar. 2007.

[10] W. Zhang, B. Chen, and N. Yu, Capacity-approaching codes for reversible data hiding, in Proc 13th Information Hiding (IH2011), LNCS 6958, 2011, pp. 255269, Springer-Verlag.

[11] [6] Announcing the ADVANCED ENCRYPTION STANDARD (AES), csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[12] [3] Mazhar Tayel, Hamed Shawky, Alaa El-Din Sayed Hafez, A New Chaos Steganography Algorithm for Hiding Multimedia Data Feb. 19 22, 2012 ICACT2012.