ENCRYPTED DATA HIDING IN ENCRYPTED IMAGES

Dr. S. Kishore Reddy*

D Ravi Chandra**

R. Laxmi Kanth***

ABSTRACT

Data hiding is the process of secretly embedding information into data sources such as image, video, or audio signals without changing the perceptual quality of the data. The encryption is a general method for providing privacy protection such as confidentiality, data integrity, entity authentication and data origin authentication. Data hiding scheme for encrypted image is made of image encryption, data embedding and data extraction. The original image and the data to be embedded are encrypted and the data is embedded into the encrypted image. In the decryption side, the encrypted data is first extracted and decrypted using the encryption key. Secondly, the encrypted image is decrypted for further analysis. The main objective of this paper is to study the various encryption schemes to encrypt both image and data and to propose a new encryption algorithm for both image and data hiding.

Keywords: *Cryptography, Data hiding, Cat map transform.*

*Associate Professor, ECE, SBCE, Khammam, AP, India

** Assistant Professor, ECE, DARE, Khammam, AP, India

***Assistant Professor, Vijaya Engineeing College, Khammam, AP, India

I. INTRODUCTION

Cryptography is the science of writing a secret code (or) the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. The basic cryptographic schemes used are Symmetric (or) Secret key cryptography and Asymmetric (or) Public key cryptography. It employs complex computational algorithms for encryption and decryption. In order to reduce the complexity, Cryptography schemes can be used. The main need of cryptography is to hide the data with the secret key without knowing to the user.

The security of message transmission is very important in the modem computerized and interconnected world. Security problems, such as modification, forgery, duplication, and others, on the Internet have been focused on inevitably [1].Cryptography is concerned with construction of schemes that ensure the security services of confidentiality, authenticity and integrity of messages. Numerous encryption techniques are applied to different data streams, where different algorithms are performed to encrypt and decrypt confidential messages [3], [4], [5], [6], [7], [8],[9], [10]. Hiding significant data is the goal of encryption methods.The hidden message can be extracted to prove the ownership or to verify the message integrity or to secretly transmit the data in [10].

In recent years, some image encryption methods have been proposed [2],[5],[6],[7].Naveenkumar et al [1],proposed a distortion tolerant method. Tan Fei and Lia shaojun [4], proposed a method which is mainly based on RSA and the HSV characteristics of 24 bits BMP image.Sos Agaian and Yicong zhou [6], proposed an encryption method using image Steganography concept and PLIP model. These image encryption schemes have the advantage of the lossless recovery of the original message. However, due to the disturbances in the transmission media, it makes harder to execute the decryption algorithm for the encrypted data with noise. In this paper, we propose a new encryption method to recover the original image without distortion.

In this paper, three methods are proposed for image encryption. First method is reversible data hiding method in which the image is encrypted by doing XOR operation bit – by-bit. The second method is cat map transform method in which the image is scrambled using periodicity. The third method is RSA encryption /decryption method. By comparing all these methods, we are able to achieve a better image quality in cat map transform. The proposed algorithm is

simulated in matlab and their PSNR values are calculated.

The paper is organized as follows. In section II, Reversible data hiding method and Cat map transform are introduced i.e. how the original image is encrypted and decrypted. It also explains the security provided by the Steganography technique - watermarking and its properties. In section III the implementation of Steganography in encrypted images using cryptography scheme is explained. Section IV, gives the simulation results and section V draws the conclusion.

II. PROPOSED SCHEME

A. Image Encryption

Due to the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Because of widely using images in industrial process, it is important to protect the confidential image data from unauthorized access. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc.

Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. In order to transmit secret images to other people, a variety of image encryption schemes have been proposed.

B. Reversible Data Hiding Method

Several proposals have dealt with data hiding in image encryption implementations. The reversible data hiding scheme is used for encrypting the images. It is mainly used to embed additional message into some distortion, with a reversible manner so that the original content can be perfectly restored after extraction of the hidden messages. The proposed scheme is the content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. The data hider embeds additional data into the encrypted image using a data hiding key though he does not know the original content. Within an encrypted image containing additional data, a receiver must first decrypt it using the encryption key and the decrypted version is similar to the original image.According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted

version. The detailed procedures are as follows:

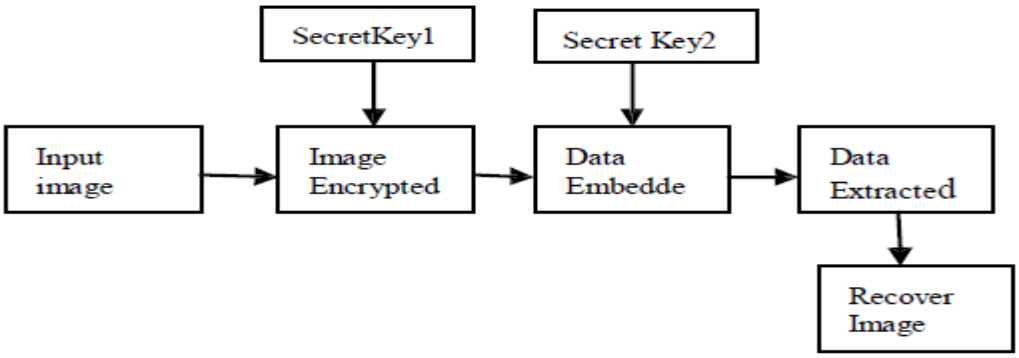

Fig. 1. Sketch of proposed scheme

STEP 1: Consider a image, which is considered as a cover image.

STEP 2: Convert the cover image to binary

STEP 3: Random bits are generated which act as the encryption key

STEP 4: XOR operation is performed between the random bits generated and cover image

STEP 5: Convert the above binary image to grayscale image. Thus, encrypted image is obtained.

C . LSB Method

This method is used to hide the data in encrypted images. In 8-bit gray scale images are selected as the cover media. These images are called cover-images. Cover-images with the secret messages embedded in them are called stego- images. For data hiding methods, the image quality refers to the quality of the stego-images.

One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity. This allows a person to hide information in the cover image and make sure that no human could detect the change in the cover image. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted. The detailed procedures as follows:

STEP 1: Consider an encrypted image (cover image).

STEP 2: Consider the message or data that should be hidden into the cover image.

STEP 3: Convert all the pixel values of the encrypted image from grayscale to binary (8-bit).

STEP 4: Embed the message or data into the cover image by hiding the data into the LSB bit of

cover image.

STEP 5: The original image along with the data is recovered with less distortion and the PSNR value is calculated.

D. Cat Map Transform

This is the transform which stretches an image that is composed of n by n pixels and effectively wraps the stretched portions around to restore the original image. The proposed scheme is by using cat map transform and exclusive OR operation to produce scrambled images**.** The cat map transform is defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N$$

where (*x*, *y*) is the image pixel location of an N *N image.a,b are positive integers.(*x* ', *y* ') is the new pixel location, y, (x ', y ') 1, 2,...*N* .The cat map transform above can efficiently scramble the2D images. The user can choose the number of iterations for applying the cat map transform to the image in order to achieve a higher level of security. The parameters a, b and iteration times N can act as security keys for the image scrambling process. The same procedure is used for data hiding using LSB method.

III. RSA ENCRYPTION/DECRYPTION

RSA algorithm is currently accepted as the most mature and complete public key cryptosystem in both the theory and application. The first one can be used for both data encryption and digital signature, also, is the representative of public key cryptosystem. This paper applies the RSA algorithm in the pre-processing phase of information hiding to ensure the security of information.RSA algorithm is based on the theory of a special kind of reversible arithmetic for modular and exponent. The steps for RSA algorithm is as follows:

(1) Find two large primes p, q.

(2) n = p * q, z = (p - 1) * (q-1).

(3) Select a number e which is less than n and prime to z, so that e and z have no common factors.

(4) Select another number d, where (e*d - 1) is divisible by z.

(5) The public key is (n, e) and the private key is (n,d).

(6) For a message m, if the cipher text is c, decryption and encryption process as follows:

Encryption:

c = m ^ e mod n. Decryption:

m = c ^ d mod n.

Thus, the image encryption is obtained.

Algorithm to hide the data in encrypted image using LSB method:

STEP 1: Consider an encrypted image (cover image).

STEP 2: Consider the message or data that should be hidden into the cover image.

STEP 3: Convert all the pixel values of the encrypted image from grayscale to binary (8-bit).

STEP 4: Embed the message or data into the cover image by hiding the data into the LSB bit of cover image.

STEP 5: The original image along with the data is recovered with less distortion and the PSNR value is calculated

IV. SIMULATION RESULTS

In this paper, we select the classical image of 256*256 cameraman.tif with 256 gray level as the original image and adopt the reversible data hiding method, Cat map transform and RSA algorithm for image encryption. We use MATLAB 2010 to simulate the experiment.

A. *Reversible Data Hiding Method:*

The test image Cameraman sized 256 *256 shown in Fig. 2(a) was used as the original cover in the experiment. After image encryption, the 8 encrypted bits of each pixel are converted into a gray value to generate an encrypted image shown in Fig. 2(b). Then, we embedded data into the encrypted image by using LSB method. The encrypted image with message is given as Fig. 2(c), The decrypted image is given as Fig. 2(d), and the values of PSNR caused by data embedding is 51.4 dB. At last, the embedded data were extracted and the original image was perfectly recovered from the decrypted image.

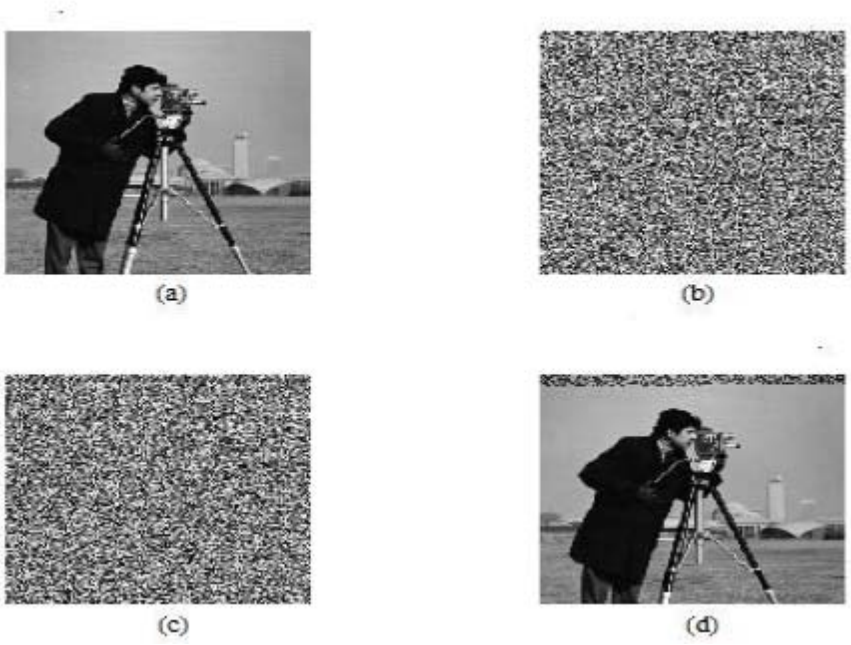

Fig.2.(a)Original image,(b)its encrypted version,(c)Encrypted image with message and (d) decrypted version

B. Cat map Transform

The test image Cameraman sized 256 *256shown in Fig. 3(a) was used as the original cover in the experiment. Make the parameter in the Arnold cat secret, the images which are iterated 33 times and 21 times in a period are showed as figure 3(b) and figure3(c) The decrypted image is given as Fig. 2(d), and the values of PSNR caused by data embedding is 91.6 dB.. The number of times may be selected according to visual effect.Through,the cat map, it realizes the scrambling and attain the purpose of encryption. It is safe to keep the secret of the parameters and the iteration times, but the attacker can also attract through the method of statistics analysis and exhaustion. So we still need to change the pixel value to encrypt further

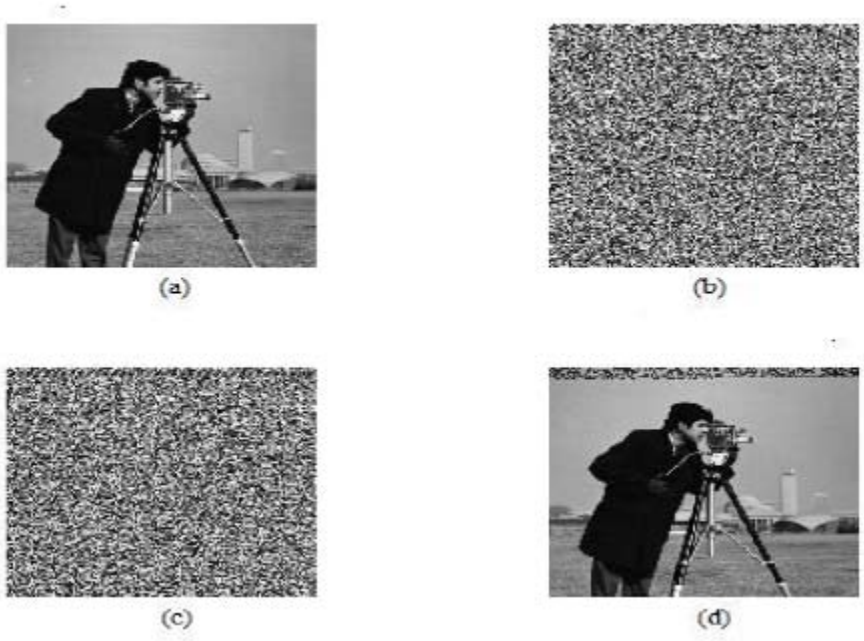

Fig.3.(a)Original image,(b)Scrambled images (33&21 times),(c) Encrypted images with message (d) decrypted version..

D. RSA Encryption/Decryption

The test image Cameraman sized 256 *256 shown in Fig. 4(a) was used as the original cover in the experiment. Then, we embedded data into the encrypted image by using LSB method. The encrypted image with message is given Fig.4(c), is the encrypted file by public key. Fig. 4(d) shows the extracted information that was decrypted by the private key. The test demonstrate that it is impossible to get the original information when input the wrong key which provides the protection to the hidden information

Fig.4.(a)Original image,(b)Scrambled image (c) Encrypted images with message (d) decrypted version

IV. CONCLUSION AND DISCUSSION

In this paper, we demonstrate that the image encryption algorithm is efficient and highly secure. All parts of the proposed encryption system were simulated using MATLAB.The scheme can resist most known attacks, such as statistical analysis and brute-force attacks . All the experimental analysis shows that the proposed encryption algorithm: (i) has high level of security with less computation. (ii) is highly robust towards cryptanalysis

REFERENCES

[1]V.Naveenkumar, Santosh Hariharan, Kumar Rajamani 'Data hiding scheme for medical images using lossless code for mobile HIMS', IEEE International conference on Communication system and networks, pp.1-4,2011.

[2] Min Wu, and B. Liu, 'Data hiding in digital binary image,'IEEE transactions on multimedia, vol 6, no.4, 2004.

[3] Santosh Hariharan, V.Naveenkumar, Mrigank Rochan,'An improved anti-counterfeiting technique for credit card transaction system' IEEE International conference on communication system and networks,pp. 1-4,2011

[4] Tan Fei, Liao Shaojun,'Research and implementation of information hiding based on RSA and HVS', IEEE International conference on e-business and e-commerce,pp.1-4,2011.

[5] ChengZ hi-Gang, Yue-li cui, ZhengWei,'Image Encryption and hiding based on Wavelet Packet Transform and Bit plane decomposition' IEEE International conference

on Wireless Communications, Networking and Mobile Computing,(pp1-4),2008.

[6] Sos Agaian, Yicong Zhou, 'Image Encryption using the image steganography concept and PLIP model 'IEEE International conference on System Science and Engineering,pp 699-703.2011.

[7] Lhoussain EL Fadil, Youssef Za , 'Enhancer EPR Data Protection using Cryptography and Digital Watermarking', IEEE International Conference on Multimedia and computing systems,pp 1-5,2011.