ISSN 23499842(Online), Volume 1, Special Issue 2(ICITET 15), March 2015
International Journal of Innovative Trends and Emerging Technologies

COMPRESSED DOMAIN DATA HIDING APPROACH ON ENCRYPTED IMAGES USING PPM

Miss. A. PREMALATHA[1] Mr. N. SIVANESAN[2]
[1]Student, Department of CSE, [2]Research Scholar, Faculty of CSE,
[1,2]Sri Krishna Engineering College, Chennai, India

***Abstract*-The project proposes the data hiding method using adaptive pixel pair matching and data encryption approach for secret data communication. The stegnography will be the art and science of hiding secret data in plain sight without being noticed within an innocent cover data so that it can be securely transmitted over a network. Here, the basic idea of PPM is to use the values of pixel pair as a reference coordinate, and it will search a coordinate in the neighborhood set of that particular pixel pair according to a given message digit. After that the pixel pair is then replaced by the searched coordinate to conceal the digit. Before hiding the data within cover image, two encryption schemes that are RSA encryption for secret messages and selective encryption for cover object proposed to increase the data protection. The proposed method offers lower distortion than DE by providing more compact neighborhood sets and allowing embedded digits in any notational system. The final solution will be proved that the proposed method not only provides better performance than those of LSB and OPAP, but also is secure under the detection of some well-known steganalysis techniques. Then image will be reconstructed from estimated key and modified encrypted image. The final result shows that used methodologies provides better performance in terms of compression ratio and reconstructed image quality.**

Keywords: Stegnography, Encryption, Compression.

I. INTRODUCTION

In recent years, communication security over the Internet is becoming more and more important because the multimedia and network are widely developed. The two different fields of research have been proposed to enhance communication security cryptography and information hiding. The major difference is the appearance of the transmitted data signal. The two cryptography methods, such as DES and RSA are exclusively to encryption which is the process of converting ordinary information (plaintext) into unintelligible gibberish. Then data encryption, the secret data appears to be a total chaos of seemingly meaningless message bits. However, the existence of the transmitted secret message can be detected.

However, information/data hiding referred to as a process to hiding secret data of various types (message, image, information, etc.) into another digital media ,can solve the intercepts problem. The concealing media is called “cover” or “host “media. If this cover media is a digital image and the altered cover image containing the secret information is called a stego-image. Embedding capacity and invisibility are the major concerns in a data hiding scheme analysis. The data hiding scheme capacity refers to the quantity of the secret data that can be embedded into the cover image, the term invisibility refers how imperceptible the fact is toil legal users when the cover image has been manipulated and turned to be a stego-image. To maintain the imperceptibility, data hiding techniques only alter the most insignificant parts of the cover image. It attempts to provide covert communication between trusting parties and the existence of the hidden message in the stego-image.

An efficient data hiding method is proposed for gray-scale images by utilizing the diamond encoding theory. We first transform the secret data into a sequence of digits.

Data hiding is a process to hide data into cover media. Data hiding process links two set of data, a set of secret data and another set of cover media data. Reversible data hiding, this can recover the original image without any change in the shape of the image after the hidden data have been extracted. The reversible data embedding is also known as lossless data embedding. The feature of reversible data embedding achieves real reversibility. To separate the process of data extraction and image decryption, Zhang [10] allocate some space for data embedding. From the application point of view reversible data hiding is used as an information carrier. To increase the payload capacity, Fist we select an embedding area in an image. Second embed both the payload and original value in this area. In this paper we present the high capacity and high visual quality, reversible data hiding for digital images. Our method can be applied to digital audio and video. This technique is used in military imagery, medical imagery and law forensics.

II. SCOPE

Encryption then compression method uses the key to encrypt an image. It enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. This system is still enhanced with encrypt messages using an asymmetric key

method. The data hiding technique uses the adaptive pixel pair algorithm for concealing the secret bits into the encrypted image. It is also focusing on quality of the image.

III. EXISTING SYSTEM

The existing system uses compression then encryption method for data embedding. The difference of the each pixel group is expanded. The data hiding capacity is low in this technique. In this "compression then encryption (CTE)", first compress the input image then encrypt using an encryption key. After producing the encrypted image, the data hider can embed some secret data into the encrypted image according to a data hiding key. Then a receiver, an authorized third party can extract the embedded data with the data hiding key and recover the original image from the encrypted image according to the encryption key. It introduced some error on data extraction. So it may degrade the image quality.

IV. PROPOSED SYSTEM

Since lossless data hiding in encrypted images is difficult. The new ETC with ppm data hiding technique works directly in encrypted images. The standard PPM algorithms can achieve better performance. The goal of encryption then compression is mainly focus on image quality. In this method first encrypt the original image and then compress the encrypt image with the encryption key. Data extraction and image recovery are free of any error. It achieves excellent performance without loss of perfect accuracy. Data hiding technique uses RSA asymmetric key algorithm and adaptive pixel pair matching (PPM) method. It increases the payload capacity. Parameter Analysis (MSE, PSNR, Correlation, Elapsed time)

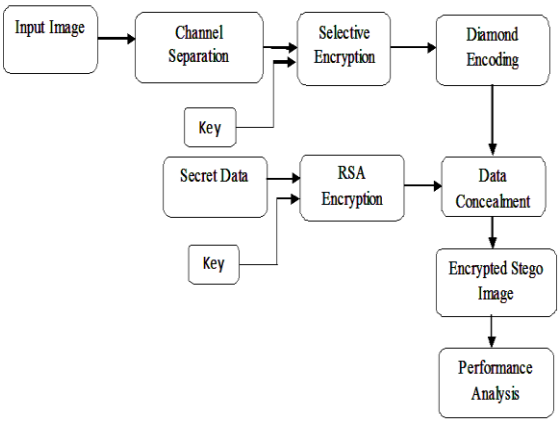


Figure1. Image Encryption and Embedding

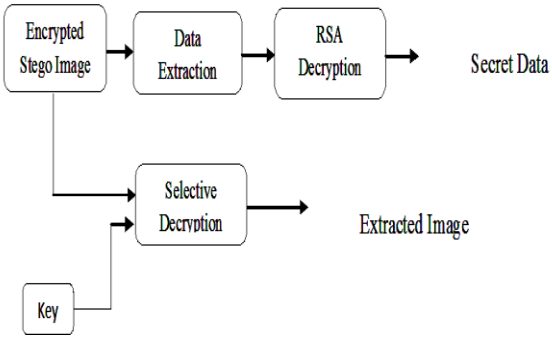


Figure2. Image Decryption and Extraction

V. METHODOLOGY

A. Diamond Encoding

In this section, we shall introduce the general operation of the diamond encoding technique. The EMD scheme embeds (2n + 1)-ary digit into n cover pixels, but diamond encoding scheme can only conceal (2k2 + 2k + 1)-ary digit into a cover pixel pair where k is the embedding parameter. This scheme can be defined as follow. Assume that a, b, p, and q are pixel values, where k is a positive integer value. The neighborhood set Sk (p, q) represents the et that contains all the vectors (a, b) with the distance to vector (p, q) smaller than k, and Sk (p, q) is defined as the following form:

$$S_k(p,q) = \{(a,b) \mid |p-a| + |q-b| \le k\}.$$

Let the absolute value |Sk| denote the number of elements of the set Sk, the every member in Sk is called neighboring vector of (p, q). We calculate the value of |Sk| to obtain them bedding base and embedded base with a parameter k.

We can obtain|S1| = 5, |S2| = 13, |S3| = 25, and so on. Moreover, we compute the |Sk| value by the following given equation, and the particular embedding base equals to the value of

$$\begin{aligned}
|S_k| &= \left(\sum_{i=0}^{k}(2i+1)\right) + \left(\sum_{i=1}^{k}(2i-1)\right) \\
&= 1 + \left(\sum_{i=1}^{k}(2i+1)\right) + \left(\sum_{i=1}^{k}2i-1\right) \\
&= 1 + \left(\sum_{i=1}^{k}(2i+1)+(2i-1)\right) \\
&= 1 + \left(\sum_{i=1}^{k}4i\right) \\
&= 1 + \frac{k(k+1)}{2} \times 4 \\
&= 1 + 2k(k+1) \\
&= 2k^2 + 2k + 1.
\end{aligned}$$

Diamond function f, compute the diamond characteristic value in embedding and the extraction procedures.

B. SELECTIVE ENCRYPTION

This method is one of the advanced encryption standard to encrypt the image for secure transmission. It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bit XOR operation. Here logistic map is used for generation of chaotic map sequence. It is very useful to transmit the secret image through unsecure channel securely which prevents data hacking. The identification of objects in an image and this process would probably start with image processing techniques such as noise removal, followed by (low-level) feature extraction to locate lines, regions and possibly areas with certain textures. Chaos encryption algorithm is used to secure the encrypted image.

The generation of encrypted image follows three steps: image partition, self reversible embedding and image encryption. The main goal of image partition is to construct smoother area. The standard RDH algorithms such as [3] , [6] can achieve better performance. The goal of self reversible embedding is to embed the LSB of complex textures into smoother area with traditional RDH algorithm. To demonstrate the process of self-embedding, we simplify the method in [3].

To digitally process an original image, it is first to reduce the original image to a series of numbers that can be manipulated by the computer. Each number will point the brightness value of the image at a particular location is called a picture element. A typical digitized image may have 512 × 512, although much larger size images are becoming general. Once the image has been digitized, there are three basic methods that can be performed on it in the computer. For local operations, several neighboring pixels in the input image determine the value of an output image pixel. In a global operation, all of the input image pixels contribute to an output image pixel value. It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bit XOR operation

Algorithm Description

Step 1: The generation of encrypted image follows three steps: image partition, self reversible embedding and image encryption.

Step 2: First Initiate constant factors then,

Find the chaotic bit sequence using the following equation,

$$Xn+1= u * x(1-x)$$

Step 3: Chaocastic bit sequence and threshold functions are Bit XOR with input image.

Step 4: Finally obtain the Encrypted image.

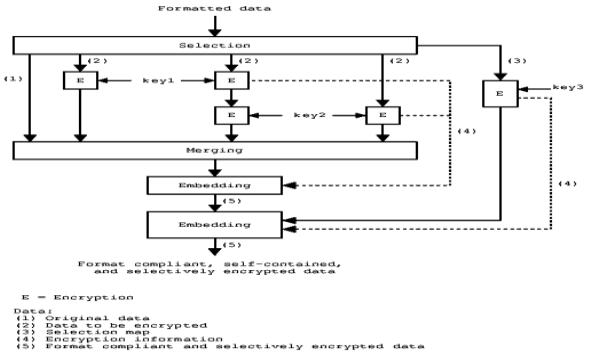


Figure3. Image Encryption

C. ASYMMETRIC KEY CRYPTOGRAPHY

Once the data hider received the encrypted image, he can embed some data into it and he does not get access to the original image. The asymmetric key encryption which is an RSA algorithm is used for both public key encryption and digital signatures. It is the most widely used public key encryption algorithm. The security of the RSA algorithm is that it is mathematically difficult to factor sufficiently large integers. The RSA algorithm is to be secure only if its keys have a length of at least 1024-bits. Cryptography allows secure transmission of secret information over insecure channels.

The receiver side who knows the secret keys only that person able to read the hidden data in an image. An encrypted image containing additional information, if a receiver has the secret key, he can extract the additional information but he does not know the image content. If the receiver has the encryption key, he can decrypt the data to obtain an image similar to the original one, but cannot extract the additional information. If the receiver has both the data-hiding key and the encryption key, he can extract both additional data and recover the original content **RSA** – Public Key Cryptography **Public key (E)** and Modulus *N* are known to all users**Private key (D)** (secret key)

Step 1: Cipher text = C ^ E mod N

Where, C – Each Character of Input text message **= p * q**;

N – Modulus parameter,

p & q – two largest prime number obtained from user given 8-bit key.

Data decryption will be done by,

Step 2: Plain text = Cipher ^ D mod N

D. DATA HIDING USING ADAPTIVE PPM AND COMPRESSION

A 8-bit gray scale image matrix consisting m × n pixels and a secret message consisting of k bits. The first bit of message is embedded into the pair of pixel and the second bit of message is embedded into the second pixel and so on according to the message value. The resultant Stegno-image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the Stegno-image is not visually perceptible. This hiding process will introduce the error between input and output image and it is determined by mean square error and Peak signal to noise ratio determines the image quality.

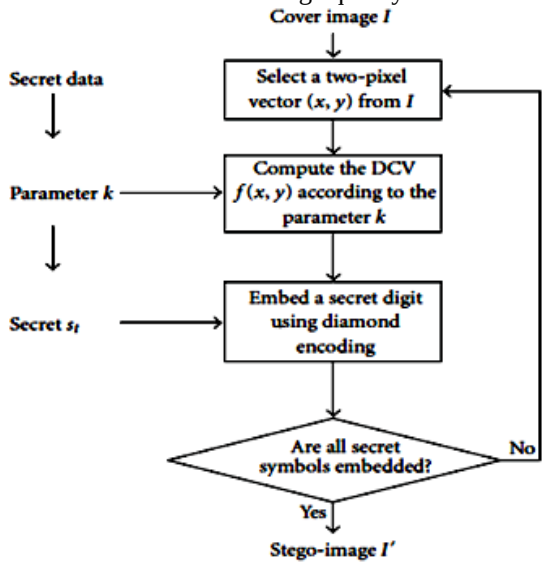


Figure4. Encode Hidden Data

E. DATA RECOVERY BY DECRYPTION

In the data extraction module, the secret data will be extracted by using relevant key for choosing the encrypted pixels to extract the data. By using the decryption keys, the image and extracted text data will be extracted from encryption to get the original information. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery. The following steps are performed in this decryption side. Take the transform of the modified image**,** Find the coefficients below a certain threshold, Extract bits of data from these coefficients, and Combine the bits into an actual message.

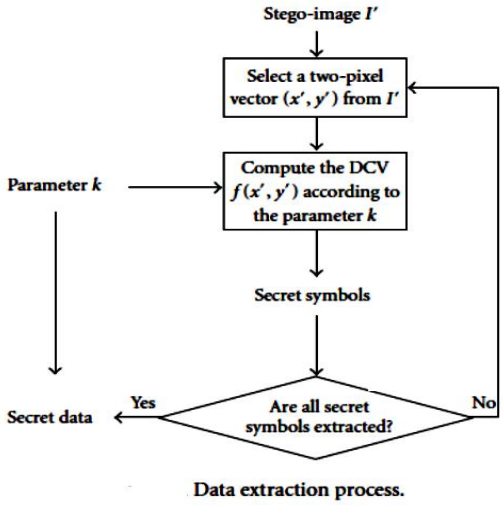


Figure5. Decode Hidden Data

F. PERFORMANCE PARAMETER EVALUATION

Peak Signal to Noise Ratio (PSNR) is used to evaluate the quality of stegno image after embedding the secret message. The PSNR is denoted by dB. The performance is evaluated in terms of capacity and PSNR. The larger PSNR is, the higher the image quality. This means only the little difference between original image and encrypted image. A small dB value of PSNR means that there is great difference between the cover-image and the stegno-image. The PSNR, above 40dB will give the good quality image.

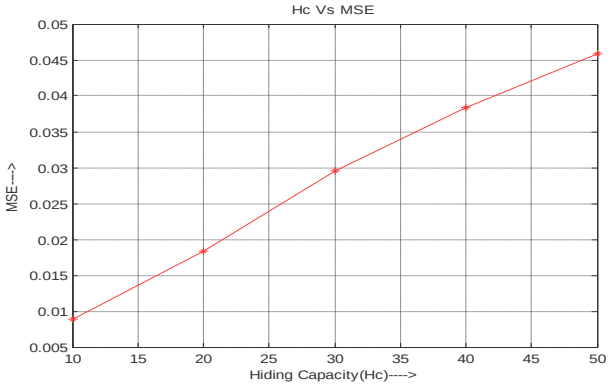
PSNR = 10 $\log_{10}$ (255^2/MSE)

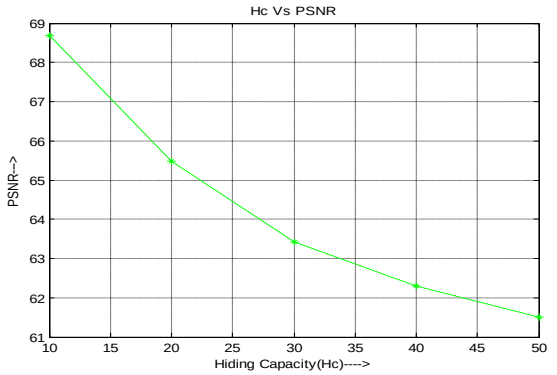
MSE = (1/ (M ×N)) Σ Σ (xij - yij)^2

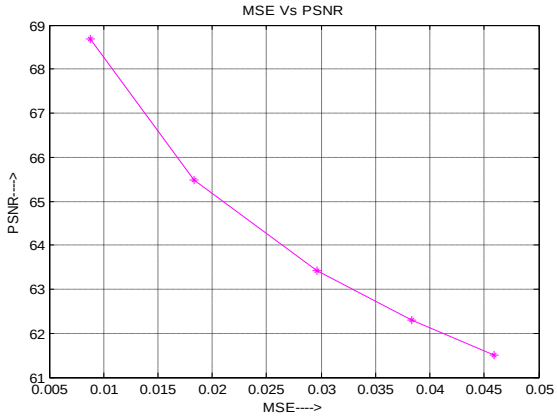
Where,

M,N are Number of Rows and Columns

xij -Input Image and yij – Reconstructed Image







VI. CONCLUSION

Compressed domain data hiding approach on encrypted images using PPM scheme states, data extraction and image restoration is free of any error for all kind of images. The gain in terms of PSNR is significantly high at embedding rate. The Encryption then compression system with data hiding techniques for image achieve excellent performance. The improved ETC with data hiding method can embed more than 10 times as large payloads for the same acceptance PSNR as all other previous methods. The data hider can benefit from the extra space emptied out in previous stage to make the data hiding process effortless. This method can achieve more security, separate data extraction and greatly improvement on the quality of marked decrypted image. The computer experiments show it will give excellent PSNR after embedding. The future work is to add secret key to the data followed by image decompression then decryption and data recovery.

REFERENCES

[1] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[2] T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357.

[3] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[4] D.Schonberg, S. C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in Proc. 43rd Annu. Allerton Conf., 2005, pp. 1–3.

[5] D.Schonberg, S. C. Draper, and K. Ramchandran, "On compression of encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 269–272.

[6] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers," IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.

[7] R.Lazzeretti and M. Barni, "Lossless compression of encrypted grey level and color images," in Proc. 16th Eur. Signal Process. Conf., Aug. 2008, pp. 1–5.

[8] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in Proc. MMSP, 2008, pp. 760–764.

[9] W. Liu, W. J. Zeng, L. Dong, and Q. M. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Imag. Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[10] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," IEEE Trans. Imag. Process., vol. 21, no. 6, pp. 3108–3114, Jun. 2012. [14] A. Kumar and A. Makur, "Lossy compression of encrypted image by compressing sensing technique," in Proc. IEEE Region 10 Conf. TENCON, Jan. 2009, pp. 1–6.