International Journal of Electronic and Electrical Engineering.
ISSN 0974-2174 Volume 7, Number 10 (2014), pp. 1119-1126

http://www.irphouse.com

Simulation of Invisible Image Watermarking Using Pixel Pair Matching and DWT Technique

Shirin Shahana. A[1], Shamna N. V [2], Jose Alex Mathew[3]

[1]4TH sem DCN MTech, Department of EC, P. A College of Engineering, Mangalore-574153, Karnataka.
[2]Department of EC, P. A College of Engineering, Mangalore-574153, Karnataka
[3]Director, Department of EC, P. A College of Engineering, Mangalore-574153, Karnataka

ABSTRACT

The security and the confidentiality of the sensitive data has become of prime and supreme importance due to the explosive growth of internet and the fast communication techniques. Therefore how to protect secret messages during transmission becomes an important issue. This project proposes a combined data hiding and encryption techniques for the purpose of secure transmission of data. Here data hiding includes steganography as well as watermarking. In this sender encrypt image and data separately using AES and chaotic algorithm respectively, hides encrypted data in encrypted image using pixel pair matching (PPM) technique and performs watermarking using discrete wavelet transform (DWT) to conceal the encrypted image before sending to the receiver. At the receiver side, obtain the encrypted image, extract the data and decrypt the original image. A comparative study of DWT and singular value decomposition (SVD) is done here to analyze the amount of distortion in the image. Therefore, the idea of applying both cryptography and steganography together has more security levels and got a very highly secured system for data embedding.

Keywords: Image and data encryption; data hiding and Extraction, AES algorithm, chaotic algorithm, DWT, SVD.

INTRODUCTION:

Steganography and Cryptography proposes efficient ways of sending vital information in a confidential manner. Both the methods can be combined by encrypting message using cryptography and then hiding the encrypted message using

steganography. The resulting stego-image can be transmitted without revealing that secret information is being concealed. Watermarking is very similar to steganography in a number of aspects. Both seek to embed information inside a cover document with a little or no degradation of the cover-document. Watermarking however adds the additional requirement of Robustness.

LITERATURE SURVEY:

There are many conventional algorithms for cryptography. AES was designed after DES. AES is definitely more secure than DES due to the larger-size key. There are no differential and linear attacks on AES as yet. Numerous tests have failed to do statistical analysis of the ciphertext. [5]

In recent years, number of chaotic sequence based encryption algorithms are proposed. [2] As chaotic encryption algorithms provides high speed, complex, ergodic system, these maps can be safely combined in to data embedding. These chaotic systems appear to be random and disorderly but in actual there is a sense of order and pattern.

LSB substitution, optimum pixel adjustment process OPAP are the common techniques for data embedding which is basically focused on LSB modification of cover pixels. Pixel pair matching (PPM) is a new approach where the embedding unit is a pair of pixels instead of a single bit. Exploiting modification direction (EMD) and diamond encoding (DE)algorithms embed each bit of secret information in to a pair of pixels of cover image. Instead of embedding the data directly the secret bit act as a parameter, which determines the new pixel pair by which the original pixel pair is to be replaced. The maximum capacity of EMD is 1. 161 bpp and DE extends the payload of EMD by embedding digits in a larger notational system.

Information stored in digital format can be easily copied without loss of quality and efficiently distributed. The digital watermark is then introduced to solve this problem. Digital watermarking is used to hide proprietary information in digital media like photos, digital music, or digital video. Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer corresponding resolution needed

WORKING OF PROPOSED SYSTEM:

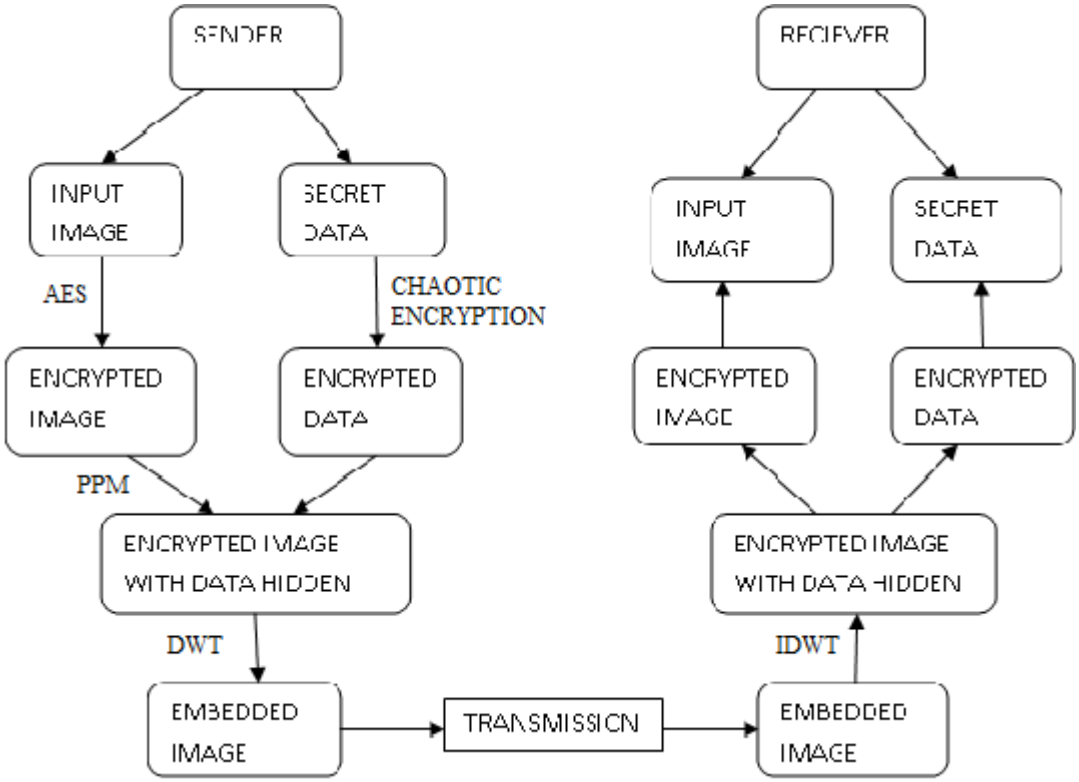

Fig: Proposed system architecture

A. Image Encryption:The user will browse the image from computer and encrypt the image using AES
B. Data Encryption:The user will browse data that he want to send and encrypt the original data using chaotic encryption
C. Data embedding:User will hide the encrypted data in encrypted image using PPM (pixel pair matching) with diamond encoding.
D. Watermarked image

User will again hide the encrypted image with encrypted data hidden into the original image inorder to obtain the invisible watermarked image using DWT.

E. File Sending

The sender will send the watermarked image to the receiver.

F. Embedded image extraction:

After receiving file from user, the receiver performs IDWT operation to extract the encrypted image with encrypted data hidden which is the embedded image.

G. Extact encrypted data:
Receiver obtains the encrypted data from encrypted image using the pixel pairs in which data is hidden by PPM method

H. Data Decryption
If receiver have data encryption key, then he will able to decrypt data. After decryption of data he will get the original data.

I. Image Decryption
Receiver obtains the original image using inverse of AES algorithm.

ENCRYPTION METHODS:

1. AES

AES is asymmetric key block cipher. Data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds. [7]Here key size of 128 bit is used, so it performs 10 rounds of encryption AES uses four types of transformations:

Substitution
Processing each byte of a state through an S-Box.

Shift rows
Shifting each row of state by left shift by 1, 2, 3 leaving first row as it is.

Mixing columns
Each byte of column is mapped into new value. For the last round of encryption, mix column step is avoided.

Key Adding
After key expansion, keys are xor ed to the state to obtain new state.

2. Chaotic encryption

Chaotic systems have property that its strength depend on initial conditions. The system key is denoted as k = (μ, x) the initial key conditions of chaotic system. [1]The I-dimensional map that exhibits complicated behavior is the logistic map from the interval [0 1] in to [0 1] parameterized by μ

$$x_i = \mu * x_{i-1} (1-x_{i-1})$$

The encrypting process consists of following steps:

- Step1. Arbitrarily select two values $x0$ in the interval [-1, 1] and μ such that $3.569 < \mu < 4$.
- Step 2. Chaotic sequence is generated using the keys.
- Step 3. Transform the chaotic sequence into a binary stream by a threshold function.

- Step 4. Plain text A (i, j) is modified using the binary stream and encrypted text A' (i, j) is created by bitwise-XOR operation

DATA HIDING METHODS:

PPM

Embedding:

It partitions cover image into non-overlapping blocks of two consecutive pixels and transforms the secret messages to a series of k-ary digits. Takes pixel pair (x, y) as the coordinate, and searches a coordinate (x′, y′) within a neighborhood set Φ (x, y) such that f (x′, y′) = sB, where f is the extraction function and sB is the secret digit in a B-ary notational system.

B= 2*K*K +2*K +1

Diamond function, f is used to compute DCV of (x, y)

f (x, y)= ((2*k+1)x + y)mod B

New stego image pixel pair is calculated by replacing f (x, y) with secret digit, s

d= (s-f (x, y)) mod B

where d= modulus distance between the s and f (x, y).

Extraction:

For each stego-pixel pair x' and y', DCV of (x', y') is calculated to get secret digit, s.

f (x', y ')= ((2*k+1)x' + y')mod B

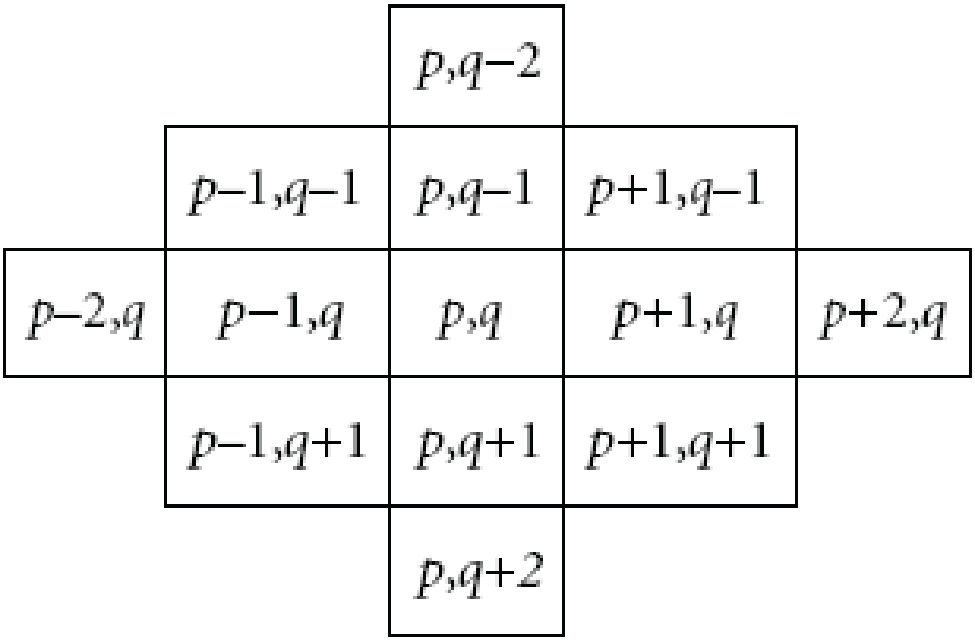

fig: diamond encoding patterns with for k=2

DWT

In two dimensional transform, first apply one step of the one dimensional transform to all rows and then repeat to all columns. Haar-DWT is simplest form of DWT. DWT splits component into numerous frequency sub bands as: LL, LH, HL, HH. Perform IDWT to combine 4 sub-bands at the receiver side.

RESULTS AND ANALYSIS:

We use MSE (mean square error) to measure the image quality. A smaller MSE indicates that the stego image has better image quality.

- Mean Square Error (MSE): It is defined as the square of error between cover image and watermarked image.

MSE= $\frac{1}{mn}\sum_{j=1}^{n}\sum_{k=1}^{n}\ (xj,k-yj,k)^2$

Peak Signal to noise Ratio (PSNR): Measures the statically difference between the cover and watermarked image is calculated using below equation

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

A comparative study between DWT and the previous method alone for example SVD (Singular value decomposition) shows that MSE is increased and PSNR value is decreased in case of SVD. Thus DWT is a better hiding method because it produces very less distortion compared to other method

The results shows that the proposed algorithm which is an excellent combination of many techniques causes minimum mean square error after embedding the secret message in the cover image. Thus PSNR value is maximum and MSE is minimum using DWT and PPM.

fig: Test images and Stego images for proposed algorithm (a)cake (b)nature

Table 1: MSE AND PSNR OF THE PROPOSED METHOD

Image	MSE	PSNR (db)
Cake	0. 0030	73
Nature	0. 0032	72

Table 2 Comparative study of MSE and PSNR between DWT and SVD

Image	DWT		SVD	
	MSE	PSNR (db)	MSE	PSNR (db)
Lena	0. 0030	73	3. 39	45
Baby	0. 0032	72	3. 23	44

CONCLUSION:

In this paper, an effective method of integrating cryptography and steganography by combining chaotic encryption with PPM embedding is done. For more security, image encryption is done using AES. Thus Low MSE and high PSNR is obtained by the combined application of pixel pair matching and DWT.

References

[1] Najeena K. S', B. M Imran‘’An Efficient Data Concealment approach based on Pixel pair Matching and Encryptions technique’’, 2013 International

Conference on Signal Processing, Image Processing and Pattern Recognition [ICSIPRI, 2013]

[2] J. Fridrich, M. Goljan, and R. Du, “Reliable detection of LSB steganography in color and grayscale images, ” in Proc. Int. Workshop on Multimedia and Security, 2001, pp. 27–30.

[3] R. M. Chao, H. C. Wu, C. C. Lee and Y. P. Chu (2009)" A novel image data hiding scheme with diamond encoding”.

[4] Rakesh S, Ajitkumar A, Kallar, Shadakshari B. C Annappa B, (20 12) "Image encryption using block based uniform scrambling and chaotic logistic mapping " International Journal on Cryptography and Information Security (IJCIS), VoI. 2, No. 1. pp-49-5

[5] Soumiya Rasheed, P. Karthigaikumar”Simulation of Image Encryption using AES Algorithm”, IJCA Special Issue on “Computational Science-New Dimensions & Perspectives”NCCSE, 2011.

[6] A Mansoori, A mahmoudi Azenvenh and F torkamani Azar, “SVD-based digital image watermarking using complex wavelet transform”, *Department of Electrical and Computer Engineering*, Tehran, 1999, *Sadhana* Vol. 34, Part 3, June 2009, pp. 393–406.