IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 62-68

Lossless stegangography in DCT Transforms by using Logistic map

N.Krishnaveni,
Head and Professor,Annai Women's College ,Karur,Tamil Nadu,India

Abstract: *The advent of digital era and technological advancements leads to generation of voluminous data-sets which increase the need for secured transmission of the data. Expansive research on developing strategies for data security during transmission resulted in two efficient strategies called cryptography and steganography.The study of Steganography applications in chaotic system are exponentially increasing within the recent years. Depending on the sensitivity to initial conditions, chaotic systems are unit characterised, similarity to continuous broad-band power spectrum and random behavior. The chaotic system is high sensitive to the initial condition and could be a high complicated nonlinear dynamic system. The chaotic sequence is unpredictable and extreme sensitivity to initial conditions. There are several applications to the chaotic system in many strategies like image compression, encryption, modulation and digital communication system. In this paper, associate formula supported to separate Discrete Cosine Transform (DCT) has been introduced by using Logistic map to urge the theme of chaos image encryption. The amount of security is extremely high and this algorithm will improve PSNR value.*

Keywords: *- Chaotic encryption, DCT, LSB, image encryption,quantization*

I. Introduction

Swift advancements in technology lead to generation of voluminous data which is being incessantly transferred over communication channel. With the advancement in this technology, the need for secure transmission also increases.Cryptography is about identifying protocols that prevent unauthorized user from reading private messages. Data integrity,confidentiality,authentication etc. are the major goals of cryptography. These kinds of protocols gets applied in different applications including ATM cards, computer authentications,e-commerce etc. Cryptography , in other words is the encryption of the original signal and sharing the decoding technique only with the intended recipients. Modern cryptography includes symmetric-key cryptography, public-key cryptography and cryptanalysis. Both the secret key and public key methods have their own limitations or flaws. Sharing of keys with the intended person itself is a major issue here.

Steganography on the other hand is the art of hiding information within the file. It refers to placing the file in the form of message,image or videso within another file,message,image or video. The Greek word 'steganos' means concealment while 'graphin' means writing and both together means covered writing. Steganography is preferred over cryptography because the intended message does not attract any attention to itself and provides more robustness. Media files are generally preferred for steganography because of the nature of their larger size helping way to hide information easily without modifying the source signal much.

II. Related Work

Discrete Cosine Transform (DCT) is similar to Discrete Fourier Transform (DFT) but uses only the real numbers. It represents the data points or samples as a sum of cosine functions at different frequencies. There are also many algorithms proposed in chaotic image encryption. Some chaotic functions are used to manipulate them and scattering the positons of pixels in frequency domain. Chaotic image encryption algorithms are proposed by Yen[1] where the pixels are rearranged by using a chaotic system method to generate a binary sequence randomly.S.A. Halim and M.F.A Sani [2] have indicated that more number of JPEG Steganography approaches are available for free to use and that has laid trivial research in the area of Steganalysis. So, they have introduced a novel method of JPEG steganography along with encryption which has a major role to play in message hiding.Fridrich[3] has suggested a new algorithm in chaotic encryption image, which does not need a chaotic random number generator by using 2D Baker's map transforms instead of the permutation of the pixel's position.Sasidharan[4] proposed a new algorithm as scheme of fast partial wavelet transform and stream cipher for image encryption.Matu Jokay and Tom[5] dealt with steganography algorithm that modifies LSB in JPEG image. They focused on minimizing the number of modified DCT coefficients by using Hamming codes. They have also examined the different dependencies between efficiency,coding and saturation.

III. Concepts of Chaos

Chaotic maps are thought of to be the wide used trend for enhancing the strength of image secret writing schemes. Completely different secret writing schemes supported chaotic maps emerge chiefly affected by the chaotic properties of dynamical systems like high sensitivity within the case of initial conditions,ergodicity,and topological transitivity. It's accepted that a good encryption algorithm should have a greater sensitivity to the secret key, and additionally possess an oversized key space creating brute-force attacks infeasible. Number of widely used chaotic maps are Logistic Map.Arnold's Cat Map,Henon Map,Tent Map,Sine Map,Gauss Map,Shift Map,etc.,

The advantages of the chaotic signal are as follows:

- **The sensitivity to the primary conditions**
  This means a minor change in primary amount will cause a significant difference in subsequent measures. It means if we have a little change in the signal amount, the final signal will be completely different.
- **The apparently accidental feature**
  In comparison with productive accidental natural number in which the range of the numbers cannot be produced again, the techniques used for producing the accidental number in algorithm based on the chaotic function will prepare the ground that if we have the primary quantities and the drawn function, we can produce the numbers again.
- **Mixing**
  Initial condition in a small interval has a characteristic that the system spread in its asymptotic evolution over the full phase space.
- **Ergodicity**
  The property when in phase space trajectory comes arbitrarily close to the first earlier states is called ergodicity . This property essentially reflects that it finally is confined to a spatial object and are a set of points, which is called an attractor. The essential property to cryptography that the desnsity of points which is time invariant.
- **Logistic Map:**

An one dimensional chaotic map with X output and input variable and two initial conditions X_0 and r represents the logistical map that may be mathematically depicted as follows:

$$x=u.*x.*(1-x) \quad \rightarrow (1)$$

Where r lies within the interval of [0,4] during which , the chaotic behavior is achieved when r is 3.9999. In our steganography we have a tendency to used logistical map to Shuffle the Pixels Mapping Arrays(PMA). The relative simplicity of the logistical map makes it a wide used concept of chaos. A chaos may be achieved efficiently when the chaotic systems exhibit an excellent sensitivity to initial conditions is that the map represents a repeated folding and stretching of space where it is defined. The quadratic difference equation describing the logistic map may be thought of as a stretching –and –folding operation on the interval(0,1).

A robust algorithm for image encryption was used by combining chaos encryption theory with Discrete Cosine Transform(DCT). The analysis of encryption security algorithm can be used from the key space perspective, key sensitivity analysis and statistical analysis. The results will show effectively image encryption, which is faster than traditional techniques, the transmitted amount of information, is low according to DCT and resists the brute-force attack and good key space is large enough encryption effect.

IV. Discrete Cosine Trasform

Transformation is a function by which it maps one set to another set through some mathematical operations. One popular transformation method in electronics and statistics is the frequency domain transformation method which refers to the analysis of mathematical functions with respect to frequency instead of the regular time based processing. Time domain or the spatial domain graph generally shows how a signal behaves over a certain period of time while a frequency domain graph shows how much of the signal lies within each given frequency band over a range of frequencies.

There are many frequency domain methods including Fourier series, Fourier transform and Wavelet transform. One variant of Discrete Fourier Transform (DFT) is the Discrete Cosine Transform (DCT) method which is very powerful in image processing. Joint Photographic Experts Group (JPEG), one of the most commonly available lossy compression method uses DCT for compression. Most of the images present in the internet are of this type. It is used for storing and transferring photographic images on the World Wide Web. Since it is widely followed also prompts us to look in to this method and specifically the DCT employed in it for image steganography. DCT methods helps separate the image in to several parts and then analyze them individually.The DCT transforms the image from the spatial domain to the frequency domain as depicted in figure 4.1 below:

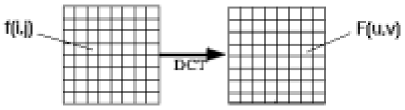


Figure 4.1 Discrete Cosine Transformation

The general equation for a 2D (N by M size image) discrete cosine transform is defined by the following equation:

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} A(i).A(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j)$$

→ 2

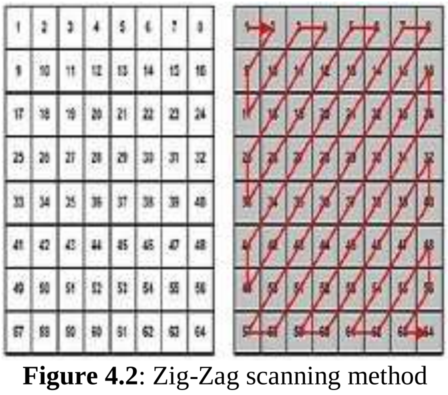
The steps involved in generating the DCT coefficients are as follows:

a) The input grey scale image of size N by M is selected;
b) f(i,j) is the intensity or the amplitude value of the pixel in row i and column j;
c) F(u,v) is the output DCT coefficient in row k1 and column k2 of the DCT matrix.
d) Smaller blocks of size 8*8 is selected for every pass and DCT is performed
e) Upper left corner of the DCT matrix represents the DC coefficient. This coefficient is the mean of all 64 values in the matrix obtained.
f) Lower right values represent higher frequencies and are called AC coefficients and are 63 in number.

When compared with any Fourier-related transform, discrete cosine transforms (DCTs) define a mathematical function or a signal in terms of a sum of sinusoids with multiple frequencies and intensities. As similar to the discrete Fourier transform (DFT), a DCT also operates on a signal at a finite number of digital sampled data points. The apparent difference between a discrete cosine transform and a discrete fourier transform is that the former uses only cosine functions for computation, while the latter uses both cosines and sines. In DCT based image steganography methods, DCT coefficients are obtained for the given grey scale image first, or if the image is already JPEG compressed, then inverse discrete cosine transform (IDCT) is performed to get the DCT coefficients. Most transformed domain steganography algorithms will directly modify the non-zero AC coefficients with the message signal without any encryption process.

In this work, we propose to hide the secret image in a better way such that the unintended recipients could not identify the presence of hidden information in the carrier signal. For this purpose, the following steps are followed:

a) The input message signal is identified.
b) The AC and DC coefficients in the transformed domain carrier signal are tabulated in the zig zag order. Zigzag sequence is followed because multiple coefficients in the DCT converted image are reduced to zero values during the quantization process and it helps in hiding the information effectively as well. Figure 4.2 represents the zig-zag scanning.



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Figure 4.2: Zig-Zag scanning method

c) Now we take the first pixel in the secret image and Exclusive OR (XOR) it with the DC coefficient in the first 8*8 block. In cryptography, the XOR cipher is a type of additive cipher and is an encryption algorithm.
d) Once this encoding is done, we call this as the new message signal for hiding. This extra step helps us to hide the information in a better way than the traditional algorithms.
e) The new message signal is now encoded by LSB replacement with the non-zero AC coefficients. We also maintain a key matrix to identify the locations that gets modified. Key matrix contains values of 1 if modified and 0 if a particular location is not modified.

f) This key matrix is converted to a decimal value and is transferred only with the intentional recipients for effective retrieval process. The inverse XOR operation is also performed at the receiving end for recovering the secret message.

The above proposed and discussed algorithm has a high capacity and a good hidden as compared to the algorithms in the literature. We use PSNR method to measure the effectiveness of the proposed algorithm. PSNR value of original source image with stego-image shows the superior results and satisfactory security when compared with other existing steganography approaches.

4.3 Experimental Result

The signal and image processing institute of the University of Southern California has provided a USC-SIPI image database which is a collection of digitized images. It is been provided by the university for supporting the research people in image processing domain. First published in 1977 and is updated regularly.

The database is divided across different categories based on the character of the images. The size of the images present varies from 256 * 256 to 512 *512 or 1024 *1024. There are both color images as well black and white images contain 8 bit for representation.

At the high level , the images are categorized as follows:

a) Textures
b) Aerials
c) Misecllaneous
d) Sequences

Volume 3 representing miscellaneous images best suits our image steganography experimentations. There are a total of 44 images present in this folder .

4.4 Performance Evaluation

This project is simulated in MATLAB R2012a version.To compare the standard of cover image, two measures are normally used. That is Mean square error (MSE) & Peak Signal to Noise Ration (PSNR).

MSE is defined as:

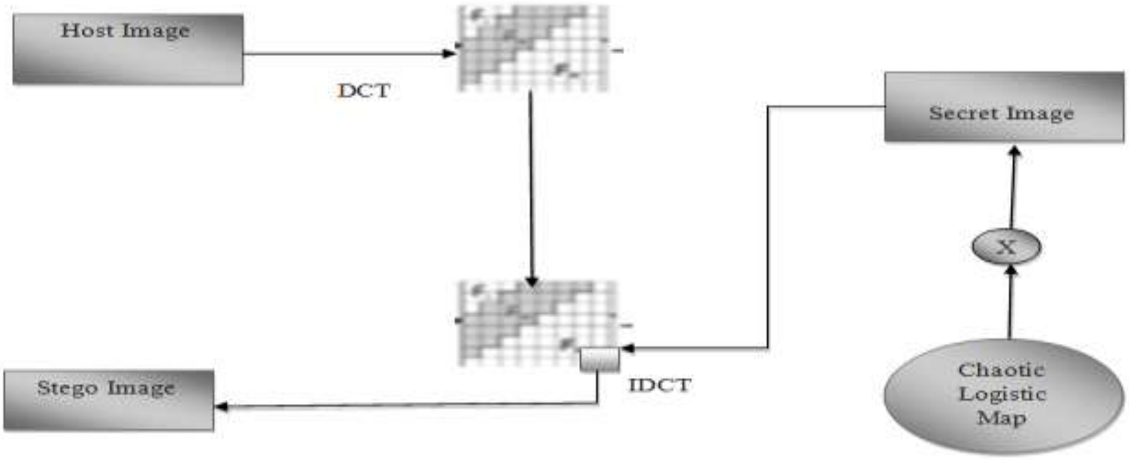
$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

PSNR is most simply outlined via the mean square error (MSE). Given a noise-free m×n monochrome image I and its noisy approximation K,

The PSNR (in dB) is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

The proposed algorithm depends on normalization of the secret image by chaotic logistics mapping followed by embedding it into high frequency band of the host image after DCT. The stego image is obtained through IDCT.



The proposed algorithm follows the following steps:

1. The given cover image is transformed through DCT by grouping the pixels into non-overlapping blocks of 8 x 8 pixels and the pixel blocks are transformed into 64 DCT coefficients. That is, even a change of a single DCT coefficient will in turn affect all 64 image pixels in that block.
2. Quantization of the DCT coefficients of the transformed cover image will lead to loss of data with only few pixels modification. Hence, instead of quantization, MASK is created to select coefficient from reserved region and the secret image is embedded along with the selected cover image block coefficient.
3. The embedding process compares the block pixels and mask coefficient. The embedding host blocks are selected randomly with a secret key for performing DCT. The absolute value of the coefficient is decreased by one if modification is needed otherwise the LSBs of quantized DCT coefficients can be substituted with the data bits.
4. The proposed algorithm embed data bits into randomly selected DCT coefficients and also employs matrix embedding to minimize the required number of modifications for data concealment. In the process of data embedding, the length of data and the number of non-zero AC coefficients are used to determine the best matrix so that the number of modifications is minimized.

4.3.1 DCT Embedding Algorithm

Proposed Algorithm (DCT & Chaos Encryption)

The three phases of the proposed scheme is given below

Phase I: Encryption of the given threshold and input secret image using chaotic series
generated by 1D logistic map.

Algorithm1:

Step 1: Select the secret image from the Input Database.
Step 2: Resize the secret image 8 * 8 and convert the secret image from RGB to Grayscale
Step 3: Assign Threshold value as 128
Step 4: Use Chaotic logistic map to generate 1-D matrix using the equation
$X(n+1)=r*x(n)*(1-x(n))$
Step 5: Generate Chaotic Cipher image by applying Bit XOR method between 1-D logistic map and Secret image along with threshold value
Step 6: Chaotic cipher image is calculated.

Algorithm2: Selection of Cover image

Step 1: Calculate Mean, Median, SD, Variance for the secret image
Step 2: Calculate the Statistical values like Mean, Median, Standard Deviation, variance
for the entire Input Database.
Step 3: Compare the extracted features with those stored in the database to find the closest image that can be used as source signal. Use Euclidean Distance to find the similarity between the secret image and the source image.
Step 4: The cover image is selected based on closest matching.

Phase II: DCT is applied to cover image and block coefficient is selected by mask
reserved coefficients.

Algorithm 3: DCT conversion

Step 1: Apply DCT for cover image
Step 2: Divide the DCT into 8*8 blocks
Step 3: Create Mask Matrix to select the coefficient from reserved region
Step 4: Check Mask (row,col)==1 then the DCT block(row,col) is selected for embedding
Step 5: Embed the chaotic cipher image into DCT block.

Phase III: Encrypted secret image is embedded to DCT coefficient and stego image is
obtained.

Algorithm 4: Embedding procedure

Step 6: Testing Chaotic Cipher image and Cover image Check whether the size of the cover-image and the embedded-image are in the ratio 2:1. The size of both the cover image (Sc) and embedded image (Se) is calculated by the following equation
Se =embedded height □ □ embedded width
Sc =cover height □ □ □ cover width

Step 7: Apply chaotic cipher image to the selected DCT coefficient block
Step 8: Apply Floor and Abs function for DCT 8*8 block and check
Mask(row,col)==1 then
i) Select the coefficient of that block
ii) Pass the selected coefficient, chaotic cipher image and bit selection to the
embedding function
Step 9: Find the coefficient using Bit AND between cover image and highest pixel value s=254
Step 10: If secret image bit AND value is equal to 128 then, select the pixel to perform embedding. Similar to the spatial domain image steganography, XOR is performed on the secret image with the carrier image before concealment in frequency domain too and the only difference lies is the selection of values for XOR operation. Every single DC coefficient is selected and the message signal value is XOR'ed with it for increasing the robustness of the proposed algorithm.
Step 11: Ensure that the size, visual features and the quality of the carrier image are not altered significantly and the changes occur only in the high frequency invisible pixel value components in embedding process.
Step 12: Apply Inverse DCT for the resultant image to retrieve stego image. The embedding capacity of the proposed algorithm depends on the number of potential pixels identified in the carrier image which in turn is dependent on the threshold rule set. The number of bits that gets modified in the identified potential pixel values also adds to the embedding capacity of the proposed algorithm.

4.4 robustness analysis of the proposed algorithm

In all DCT based embedding schemes, JPEG compression of the stego image involves the quantization process leading to loss of some embedded data bits. Hence, this study proposes the use of Floor, Absolute function to the low frequency component alone for embedding the secret data image leaving the other components.

SSIM (Structural Similarity Index Matrix) is a method used to improve the parameters such as PSNR and MSE to determine the similarity of between cover image and stego image through measuring the changes in brightness, contrast and structure of an image. SSIM is obtained by combining the average intensity of the brightness, the variations in the contrast and the structure of the cross-correlation between the original and stego-image.

This study uses MSE,PSNR and SSIM for assessing quality of the image and the values are presented in Table 4.1

Table 4.1 MSE, PSNR, SSIM using DCT method

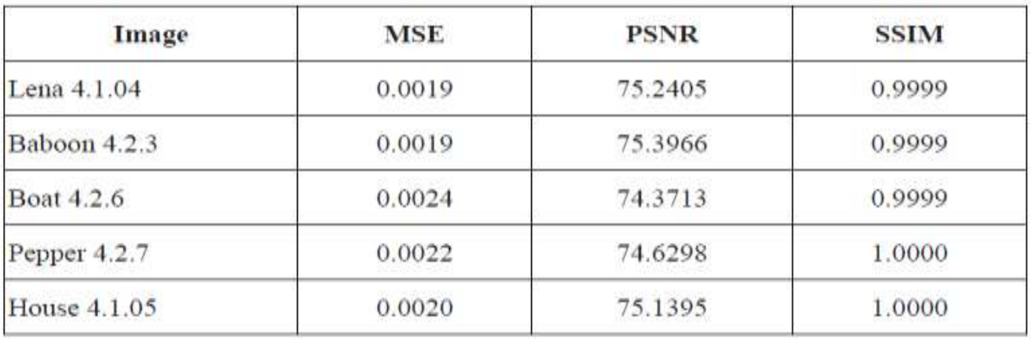


Image	MSE	PSNR	SSIM
Lena 4.1.04	0.0019	75.2405	0.9999
Baboon 4.2.3	0.0019	75.3966	0.9999
Boat 4.2.6	0.0024	74.3713	0.9999
Pepper 4.2.7	0.0022	74.6298	1.0000
House 4.1.05	0.0020	75.1395	1.0000

In terms of payload, the proposed algorithms have higher capacity to carry large amount of data based on the threshold value (first algorithm) and the partitioning blocks (second algorithm). Since the secret image is embedded in more robust areas and is spread across the whole carrier image instead of getting concentrated in a single region, the proposed algorithm is very robust to blind the steganalysis attacks. The proposed algorithm also possesses an advantage of the flexibility in adjusting the number of components identified for embedding the secret image based on the required payload, robustness and applications.

V. Conclusion

The proposed methods successfully hide the arbitrary data and remain visually undetectable as well. The algorithms were tested on a huge amount of different textual and secret messages and it works satisfactory. The proposed algorithms were found to be highly robust, provide advance level security and also powerful in embedding. It has high capacity image steganography method with tolerable level of noiselessness and alteration in the source image and good level of overall security. Various statistics attacks were also directed to show the robustness of the method. Also the PSNR values calculated show better results when compared with present steganography approaches.

References

[1]. Yen. J,C and Guo, J.I., "A New Chaotic Key Based Design for Image Encryption and Decryption, Proceedings of the IEEE International Symposium Circuits and Systems,2000,4-52 vol 4.

[2]. S.A. Halim and M.F.A Sani. " Embedding using spread spectrum image steganography with GIF," in proceedings of the IMT-GT-ICMSA ,2010 pp.659-666, 2010.

[3]. Fridrich.J., Symmetric Ciphers Based on Two Dimensional Chaotic Maps,Int J.Bifurication and chaos .1998 8(6)

[4]. Sapna Saidharan , Deepu Sleeba Philip," A Fast Partial Image Encryption sechme with wavelet transform and rc4", The college of Information Sciences and Technology 2015 The Pennsylvania State University

[5]. MatuJokayand Tom Moravik,"Image based JPEG steganography", Tatra Mountains Mathematical Publications ,DOI 10.2478/v10127-010-0006-9,2010.

[6]. Omed Khalind and Benjamin Aziz, "LSB Steganography with improved embedding efficiency and Undetectability", 4th International Conference on Signal & Image Processing, At Zurich, Switzerland, 2015.

[7]. Amsaveni, A., and P. T. Vanathi.(2015) "A comprehensive study on image steganography and steganalysis techniques." International Journal of Information and Communication Technology 7, no. 4-5 406-424

[8]. [8] Mohammad Ali Bani Younes, and Aman Jantan, (June 2008), "A new steganography approach for image encryption exchange by using least significant bit insertion", IJCSNS International Journal of Computer Science and Network Security, Vol. 8 No.6.

[9]. Dr. K. L. Sudha, and Manjunath Prasad, (Aug. 2011)," Chaos image encryption using pixel shuffling with henon map," Elixir Elec. Engg. 38, pp 4492-4495

[10]. [10] N.F. Johnson and S. Katzenbeisser – "A survey of steganograhic techniques". Information hiding, pp. 43-78, 2000.

[11]. [11] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, pp. 1613-1626, 2003.