International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 18 (2019) pp. 3696-3700

Multi Layer Image Steganography-Encryption mechanism employing DCT-DWT and Chaotic Network

Asutosh Tiwari
UEC, Ujjain
Madhya Pradesh, India.

Prof. Y.S. Thakur
UEC, Ujjain
Madhya Pradesh, India.

Abstract

In the present security scenario, implementing tele-health solutions has become an emerging trend at global level. It primarily focuses on employing latest information and communication technologies (ICT) to cater the requirements of people associated with the health industry, patients, and policy makers Hence there is a need for high end security for tele-health services. In the proposed work, biomedical image security has been addressed using a multi-layer approach. The propose system works on the Discrete Cosine Transform, Discrete Wavelet Transform (DWT) and Chaotic Neural Networks for biomedical image security to implement a steganogrpahy-encryption hybrid. The performance metrics have been chosen as Mean Square Error, Peak Signal to Noise Ratio, structural similarity index measure (SSIM) number of changing pixel rate (NPCR) and unified averaged changed intensity (UACI).

Keywords: Discrete Cosine Transform, Discrete Wavelet Transform, Chaotic Neural Networks, Peak Signal to Noise Ratio, structural similarity index measure (SSIM) number of changing pixel rate (NPCR) and unified averaged changed intensity (UACI).

I. INTRODUCTION

Presently, information and communication technologies are making their presence felt in several domains including healthcare. With widespread data sharing in the tele-health sector, security has become a major concern Cryptosystems have always been an area of active research to secure confidential and classified data. [1] As digital technologies have With a distinct difference in the information content in digital images compared to normal text data, encryption of digital images have evolved from conventional techniques to adaptive and light weight techniques for applications that can run on systems with moderate to low computational capacity. An **image** is a function of two variables and can be defined as *f(x,y)* where x and y are the coordinates in space on which the image values depend. Image pixel values often convey the following information:

1) The brightness at a point or the Gray Scale Value.
2) The color or frequency aspect of the point often referred to as the RGB value.
3) The co-ordinates of a point also convey the spatial information i.e. the values (x,y)

II. FUNDAMENTALS OF IMAGE ENCRYPTION

What is critical to save classified images form attacks is the algorithm that is used to encrypt it. While classical algorithms such as AES [2] or Blowfish [3] do perform the task at hand, but the internal architecture of such algorithms is well known which lets attackers exploit even slightly visible trends in the encrypted image. A second binding factor is the fact that these algorithms were designed typically for textual data which means that the arrangement or permutation of the pixels or picture elements is immaterial. This causes degradations in the image even after decryption. Thus these techniques need considerable amount of space and time complexity to handle digital images. Off late artificial neural networks are being used for image encryption.

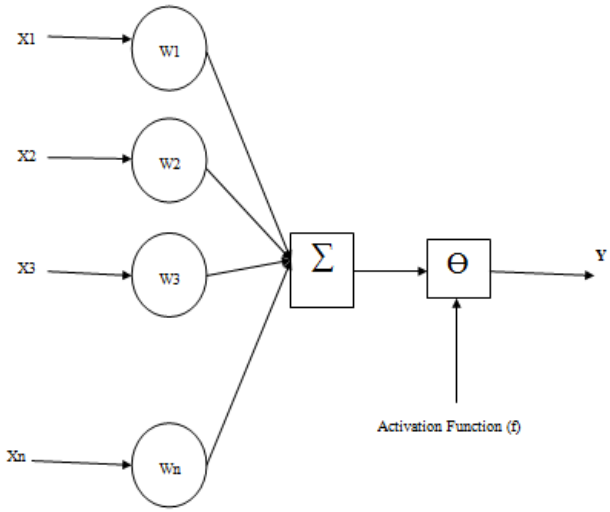

Fig.1 Mathematical model of neural network

The output of the neural network is given by:

$$\mathbf{Y} = \sum_{i=1}^{n} \mathbf{X_i} \cdot \mathbf{W_i} + \boldsymbol{\theta_i} \qquad (1)$$

Here,

X is the input data stream

Y is the output

W is the weight

Θ is the decision logic or bias

f is the activation function

A much sought after algorithm is one in which the values of key and algorithmic parameters change dynamically with the change in the image to be encrypted. The property of chaos can be used to implement such a system**.** [4],[5]. The reason for using sequential machine for implementation is that the output and input can have any type of relationship and the output depends on the starting state. The starting state is used as a key for encryption and decryption.

The basic idea behind designing a neural network which would perform encryption is to render a high level of randomness in the cipher text so as to hinder attacks from adversaries. For that purpose, a special type of neural network called the chaotic neural network is designed which follows the following conditions.

$$\boldsymbol{CT(x) = f(PT)} \quad \textbf{(2)}$$

$$\boldsymbol{PT = f^{-1}CT(x)} \quad \textbf{(3)}$$

but,

$$\boldsymbol{CT(x + \Delta x) \neq f(PT + \Delta PT)} \quad \textbf{(4)}$$

The take away from the above discussion is the existence of chaos in the system.

In the above equations,

P.T. stands for plain text

C.T. stands for cipher text

f stands for the function mapping the plain text and the cipher text

f^{-1} stands for the inverse mapping function from the cipher text to the plain text.

The basic concept of chaos is the fact the output for a given input is deterministic by a particular function f but as the input changes by an amount Δ, the deterministic function **f** ceases to exist. This creates an extremely large amount of randomness in the cipher text and the system is said to possess the property of chaos.

The aim of such an algorithm is to design high amount of randomness in the image and also make the algorithm light weight so as to make it practically feasible for widespread applications.

III. DEGRADATION MODEL FOR DIGITAL IMAGES

Digital images undergo several types of degradations while storage and transmission through channels. The most common sources of noise and blurring effects affect the image under consideration while passing through the communication medium which is termed as the channel or while storage in electronic storage systems. As the degradations are highly random in nature, therefore they are typically designated as random variables described by their statistical parameters. It is crucial that we know about the statistical parameters of the degradations so that we can revert the effects caused by the sources. Thus we need to have the degradation model design for removal of the detrimental effects.

Sources of Noise Affecting Digital Images

Several sources of noise affect signals passing through the communication media or the channel. Our interest lies in that noise and blurring mechanisms that degrade digital images the most. A description of the same is given below.[6]

Common Noise Types Affecting Digital Images

As described earlier, the different noise types which degrade images are given below. It should be noted though that they are characterized by their statistical properties.[7],[8]

1) Gaussian Noise
2) Speckle Noise
3) Salt and Pepper Noise
4) Poisson Noise.

Gaussian Noise

It is typically encountered in electronic amplifier systems which are essential for boosting the strength of the image signals while they wean down.

Gaussian is described statistically by

1) Mean
2) Variance

Salt & pepper Noise or Impulsive Noise

It is encountered majorly in the in built analog to digital converters or ADCs in the devices that convert the analog information into digital information. It can be caused by inappropriate or corrupt values of the picture elements or pixels. It can also be caused by spikes of currents or surges in voltage in the ADCs.

It is statistically described by;

1) Mean
2) Variance
3) Noise Density

Speckle Noise or Multiplicative Noise

It exhibits a multiplicative nature wherein the original image values are M and the one after the impact of noise is M'

$$\mathbf{M' = IM + k*M} \quad \textbf{(5)}$$

It can be seen that the noise would have a high effect for higher values of M or for a simultaneous high value of 'k'.

It is statistically described by the following statistical parameters:

1) Mean
2) Variance
3) Noise Density

Poisson Noise or Shot Noise.

It is encountered if the sensor capturing the digital image gets lesser number of pixel values than what is necessary for it.[9],[10] The absence of such pixel values often a noise

termed as Poisson noise which follows the Poisson distribution for the noise random variable.

It is statistically described by:

1) Variable Mean or expectation value
2) Value of Standard deviation or value of variance.

Images undergo several random degradations such as noise and blurring effects. Although the effects are random in nature, yet they can be modelled statistically using parameters such as mean, variance, standard deviation etc.[7]Its essential though that the restoring mechanism does not introduce non-linearity of its own. Hence is necessary to filter out noise effects to restore the image. [11],[12]

IV. SYSTEM DESIGN

The multi layer security is mathematically modelled as:

Start

1. Choose the original secret image Is and also a cover image Ic.
2. Apply the discrete wavelet transform (DWT) on the cover image Ic. Discrete Wavelet Transform (DWT) is capable to separate the image into different spectral bands. The mathematical description of the wavelet transform can be given by: [1]

$$\boldsymbol{C\,(S,\,P)} = \int_{-\infty}^{\infty} \boldsymbol{f}(\mathrm{t})\;((\boldsymbol{S},\boldsymbol{P},\boldsymbol{t}))\;\boldsymbol{dt} \qquad \textbf{(6)}$$

Here S stands for scaling

P stands for position

t stands for time shifts.

C is the Wavelet Transform

Apply the Discrete Cosine transform on the secret image to re-arrange the pixels into a DCT matrix with inner elements containing maximum information. The DCT is defined as:

$$\boldsymbol{y(k) = w(k)\sum_{i=1}^{N} x(n)\cos\left(\frac{\pi(2n-1)(k-1)}{2N}\right)} \qquad \textbf{(7)}$$

Here

$$\boldsymbol{w(k) = 1/\sqrt{N}} \ \textbf{for k=1} \qquad \textbf{(8)}$$

and

$$\boldsymbol{w(k) = \sqrt{2/N}} \ \textbf{for 2< k<N} \qquad \textbf{(9)}$$

The main benefit of the Discrete Cosine transform is the fact that it breaks down the signal into spectral bands and separates frequency components.[13],[14] The redundant components can be removed or other co-efficients can be inserted without making distinct difference in the perceptibility. The result is lesser redundant information in the signal. Thereby the information content in the signal is more, and can be given by:

$$\boldsymbol{I = log_2 \frac{1}{P_i}} \qquad \textbf{(10)}$$

3. Now, apply the DCT and DWT decompositions to the obtain co-efficients.
4. Design an ANN based on Chaos governed by:

$$\boldsymbol{Y(i) = f\{X(i)\} \quad \nabla\ X(i)} \qquad \textbf{(11)}$$

But Y (i) is random for X (i+Δ);

Here,

Δ stands for a change in X.

Such a mathematical condition can be generated by what is called a **'chaotic neural network'** i.e. a neural network that exhibits the property of chaos. Chaos is the property that makes it extremely complicated for the attackers to break the encryption algorithm and decipher the cipher text. The requirement for such a chaotic neural network is the adaptive nature of the path weights for different conditions. As the path weight variable changes adaptively, the design of the neural network changes for various inputs thus making it infeasible for the attacker to decipher the cipher text. The above condition can be mathematically expressed as:

$$\boldsymbol{W(i) = f'\{X(i)\}} \qquad \textbf{(12)}$$

Here,

f ' represents the function or condition that keeps changing the path weight according to the input available to the chaotic network.

Since the path weights change according to the available inputs, therefore the encryption taking place through the chaotic neural network keeps changing dynamically

5. Simulate the Neural network for a

   2-20-20-20-1 model.

   Here,

   2 represents the two neurons for the lain text image and the key

   Hidden layer 1 controls the encryption algorithm

   Hidden layer 2 controls the decryption algorithm

   Hidden layer three optimizes the outputs of two layers.
6. Compute the IDCT and IDWT to get back image form co-efficients.

Stop

The performance evaluation parameters are:

1) Peak Signal to Noise Ratio

2) Mean Square Error

3) Structural similarity index measure (SSIM)

4) Number of changing pixel rate (NPCR)

5) Unified averaged changed intensity (UACI).

V. ANALYSIS OF OBTAINED RESULTS

The test images taken for this study are standard biomedical images for the MRI of the brain. The images are used to implement the multi layer security approach and finally the results are computed in terms of the evaluation parameters.

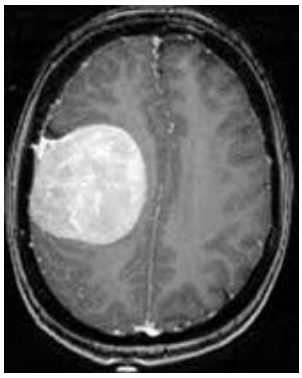

Fig.2 Original Bio-Medical Image

Fig.3 Cover Image

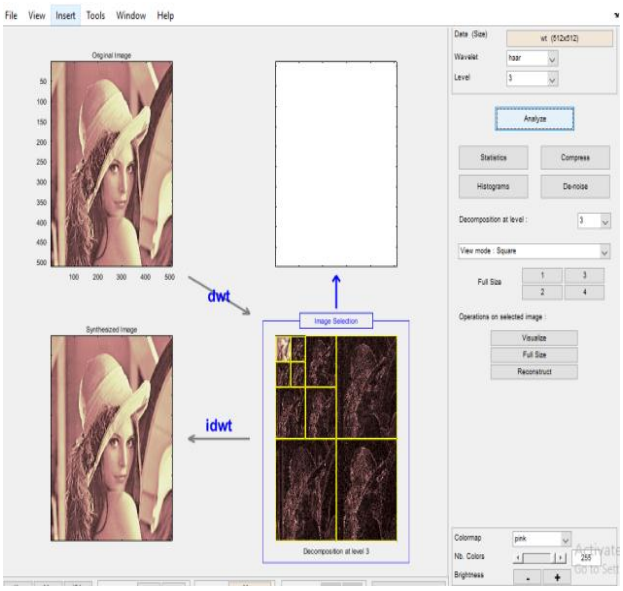

Fig.4 Wavelet Decomposition of cover image

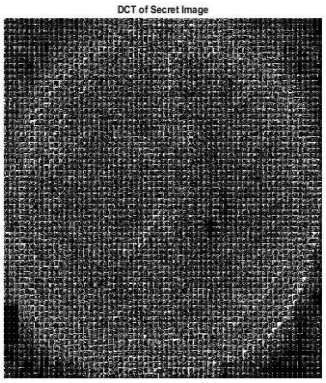

Fig.5 DCT of Secret image

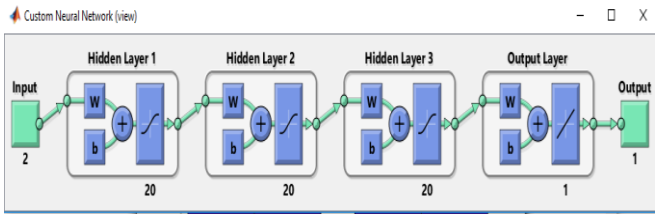

Fig.6 Neural Network Design

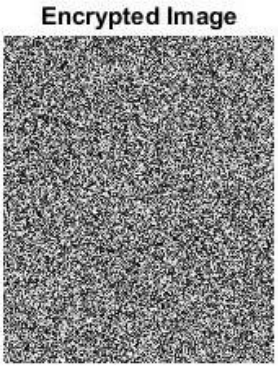

Fig.7 Encrypted Image

Fig.8 Degraded image and Salt & Pepper Noise

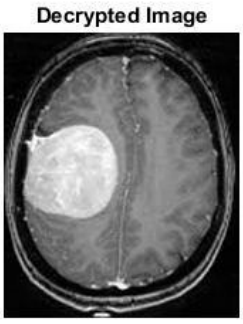

Fig.9 Decrypted Image

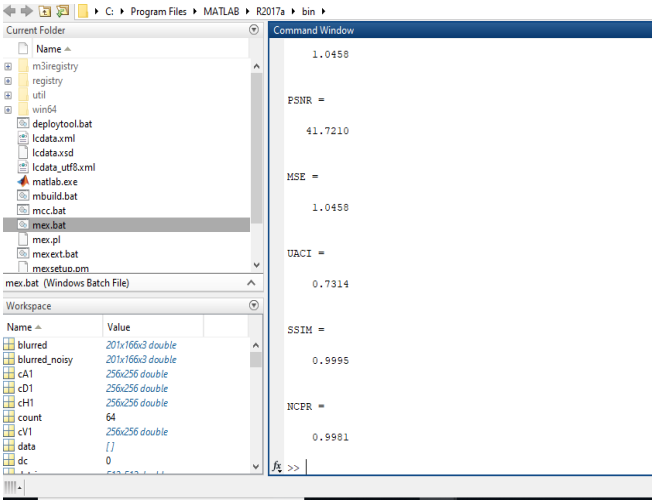

Fig.10 Screenshot of Command Window

Table 1. Comparative Analysis with Previous Work [1]

S.No	Parameter (MRI Image)	Previous Work [1]	Proposed Work
1.	PSNR	35.52	41.72
2.	MSE	-	1.0458
3.	SSIM	0.9973	0.9995
4.	NPCR	0.9962	0.9981
5.	UACI	0.3447	0.7314

CONCLUSION:

It can be concluded from the previous discussions that biomedical images can be thought of as requiring multi layer security with increasing tele-medical applications. The propose system works on the Discrete Cosine Transform, Discrete Wavelet Transform (DWT) and Chaotic Neural Networks for biomedical image security. The performance metrics have been chosen as Mean Square Error, Peak Signal to Noise Ratio, structural similarity index measure (SSIM) number of changing pixel rate (NPCR) and unified averaged changed intensity (UACI). It has been found that the proposed system achieves better results compared to contemporary and previous work. [1]

REFERENCES

[1] Sriti Thakur, Amit Kumar Singh, Satya Prakash Ghrera, Mohamed Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications", Springer ,2018.

[2] C Yu, J Li, X Li, X Ren, BB Gupta, "Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram", Springer 2018

[3] LY Zhang, Y Liu, F Pareschi, Y Zhang, "On the security of a class of diffusion mechanisms for image encryption", IEEE 2018.

[4] Y Li, C Wang, H Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation", Elsevier 2017.

[5] X Chai, Z Gan, Y Chen, Y Zhang, "A visually secure image encryption scheme based on compressive sensing", Elsevier 2017.

[6] A Belazi, AAA El-Latif, AV Diaconu, R Rhouma, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms", Elsevier 2017.

[7] L Xu, Z Li, J Li, W Hua, "A novel bit-level image encryption algorithm based on chaotic maps", Elsevier 2016.

[8] N Zhou, S Pan, S Cheng, Z Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing", Elsevier 2016.

[9] S Trambadia, P Dholakia, "Design and analysis of an image restoration using wiener filter with a quality based hybrid algorithms", IEEE 2015.

[10] J.S. Armand Eyebe Fouda , J. Yves Effa, Samrat L. Sabat , Maaruf Ali , "A fast chaotic block cipher for image encryption", ELSEVIER 2014.

[11] Zhenxing Qian, Xinpeng Zhang, Shuozhong Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream", IEEE 2014

[12] A Bakhshandeh, Z Eslami "An authenticated image encryption scheme based on chaotic maps and memory cellular automata", Elsevier 2013.

[13] K Gu, G Zhai, X Yang, W Zhang, "A new reduced-reference image quality assessment using structural degradation model", IEEE 2013

[14] YW Tai, S Lin, "Motion-aware noise filtering for de-blurring of noisy and blurry images", IEEE 2012

[15] A. Kanso and M. Ghebleh, "A Novel Image Encryption Algorithm Based on a 3D Chaotic Map", Elsevier 2012