High Secure Image Steganography based on Hopfield Chaotic Neural Network and Wavelet Transforms

B. Geetha vani [1] and **E. V. Prasad** [2]

Research scholar, Dept. of CSE,
JNTU Kakinada. AP, India.

Professor, Dept. of CSE & Rector,
JNTU Kakinada, AP, India

ABSTRACT
Steganography is an art of hiding the information without any change in the external appearance of the cover object. Cryptography is a technique to make the information unreadable for unauthorized users. Making the data unreadable and hiding it, will make the data highly secure. Image steganography allows the user to hide a large amount of data inside an image. On transmission side Steganography is performed by choosing a Cover-Image then hiding the text within the image. On receiving side the secret text is extracted from the stego image. In this paper, High Secure steganography algorithm is proposed. This process contains three stages. In the first stage, the text is encrypted by using a traditional encryption method i.e Caeser method. In the second stage the cipher text is again encrypted by using the chaotic neural network and in the third stage the resulting encrypted text is embedded inside the image using DWT. High security can be achieved by encrypting the text using Chaotic Neural Network. The binary sequence of the encrypted text created by Chaotic neural network is unpredictable making it highly secure.The Proposed algorithm is tested against different gray scale images considering PSNR, MSE and SSIM for evaluation. It is observed that the security is increased with acceptable PSNR compared to other methods.

Keywords:
Steganography, Hopfield Chaotic Neural Network, DWT based steganography, Text Encryption based on Caeser cipher and HCNN.

1. Introduction

Steganography is an art of hiding information inside an image or an audio file secretly without any change in the external appearance of the image or audio file. Cryptography is an art of sending the secret information in the unreadable form. Both Steganography and Cryptography have the same goal of sending the secret message to the exact receiver. In Steganography, the secret message is hidden in any of the cover medium and then transmitted to the receiver, whereas in cryptography, the secret message is made unreadable and then transmitted to the receiver in an unreadable form. The message that is sent to receiver through cryptography, express out that some secret communication is going on between the sender and the receiver. This leads to the main drawback of the cryptography. In steganography, only the sender and receiver know the secret communication. Having the advantage of cryptography of making the text unreadable and then combining with the steganography makes the secret transmission highly secured.

Image steganography is carried out using different techniques. It is broadly classified based on Spatial-domain and transform-domain. In Spatial-domain, the secret messages are embedded directly. In the paper [10], the steganography scheme embeds the secret message by modifying the Gabor coefficients of the cover image. In the paper [11], the data hiding technique using 1-D DWT was performed on both the secret and cover images. In the paper [12], the secret message is embedded in the high frequency coefficients in 2D-DWT performed on cover image. In papers [1,12.14.15] , cryptographic scheme based on delayed chaotic neural networks is defined.

The proposed three level algorithm consists of normal Ceaser Cipher at the first stage, encryption using chaotic neural network at the second stage and embedding the coded text into the image at the third stage. Similarly on the receiving side, the secret text is extracted from the image and then the extracted image is decrypted using chaotic neural network and at the third stage the decrypted text will be made to readable text by applying inverse caeser cipher algorithm.

The rest of the paper is organized as follows. In Section 2, Hopfield Chaotic Neural Network used for encryption is explained. In Section 3, Overview of Discrete Wavelet Transforms is presented. In Section 4, Overview of proposed steganography algorithm is presented. In Section 5, construction and working methods of Proposed Algorithm is described. In Section 6, Simulation results and analysis of proposed approach is discussed. In Section 7, the conclusion of work is presented.

2. Hopfield Chaotic Neural Network for Encryption

Encryption is the process of converting the plain text to cipher text. The cipher text is unreadable and should decrypt to obtain the information readable. The drawback

Manuscript received March 5, 2013
Manuscript revised March 20, 2013

of existing public key cryptography of large computational power, complexity and time consumption during the generation of key can be overcome by using chaotic neural network. The Chaotic neural network, used for encryption consumes less computational power and the sequence generated using this is unpredictable leading to highly secured and efficient in terms of power. In Chaotic Neural Network, the weights and biases are determined by a chaotic sequence, a binary random deterministic sequence, to mask or to scramble the original information.

Chaotic System possess many interesting properties of good cryptosystem such as ergodicity, mixing and sensitivity to initial conditions.[1] Yu et al. designed a delayed chaotic neural network based cryptosystem[2].This cryptosystem makes use of the chaotic trajectories of two neurons to generate basic binary sequences for encrypting plaintext. The cryptosystem using Hopfield Neural Network, is discussed as below.

$$\begin{pmatrix} \frac{dx1(t)}{dt} \\ \frac{dx2(t)}{dt} \end{pmatrix} = -A\begin{pmatrix} x1(t) \\ x2(t) \end{pmatrix} + W\begin{pmatrix} \tanh(x1(t)) \\ tanh(x2(t)) \end{pmatrix} + B\begin{pmatrix} \tanh(x1(t-\tau(t))) \\ tanh(x2(t-\tau(t))) \end{pmatrix} \quad \text{--} \quad \text{Eq.1}$$

Where $\tau(t) = 1+0.1\sin(t)$, the initial condition of differential equation (Eq.1) is given $x_i(t) = \Phi_i(t)$ when $-r \leq t \leq 0$, where
$r = \max_t\{\tau(t)\}$, $\Phi_i(t) = (0.4,0.6)^T$.

The set of delayed differential equations is solved by the fourth-order Runge–Kutta method with time step size h = 0.01. Suppose that x1(t) and x2(t) are the trajectories of delayed neural networks. The ith iterations of the chaotic neural networks are $x_{1i} = x1(ih)$, $x_{2i} = x2(ih)$.

An approach proposed in [3] was adopted to generate a sequence of independent and identical (i.i.d.) binary random variables from a class of ergodic chaotic maps. For any x defined in the interval I = [d, e], we can express the value of (x - d)/(e - d) belongs to [0, 1] in the following binary representation

$$\frac{x-d}{e-d} = 0.\ b_1(x)\, b_2(x) \ldots\ldots.\ b_i(x) \ldots.., \ x € [d,e], \quad b_i(x) € \{0,1\} \quad \text{---} \quad \text{Eq.2}$$

The ith bit $b_i(x)$ can be expressed as

$$b_i(x) = a_0 + \sum_{r=1}^{2i-1} (-1)^{r-1}\, \Phi_{(e-d)(r/2i)+d}(x) \quad \text{---} \quad \text{Eq.3}$$

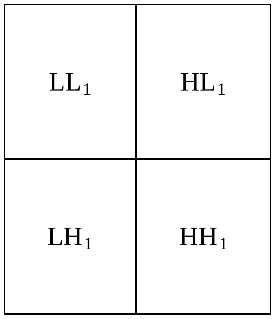
where $\Phi_t(x)$ is a threshold function defined by

$$\Phi_t(x) = \begin{cases} 0, x < t \\ 1,\ x \geq t \end{cases} \quad \text{---} \quad \text{Eq.4}$$

The above said four equations enable to generate the basic binary sequence. These binary sequences are used for encryption as stated by Yu et al [1]. Chaotic neural networks offer greatly increase memory capacity. Each memory is encoded by an Unstable Periodic Orbit (UPO) on the chaotic attractor. A chaotic attractor is a set of states in a system's state space with very special property that the set is an attracting set. So the system starting with its initial condition in the appropriate basin, eventually ends up in the set. The most important to be noticed is that the existence of the system in nearby states of the attractor leads to the divergence from each other exponentially fast and small amounts of noise is noticeably amplified.

3. Discrete Wavelet Transforms

The simplest of DWT is Haar - DWT where the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. For 2D-images, applying DWT will result in the separation of four different bands. LL is the lower resolution approximation of the image. HL is the horizontal, LH is the vertical, HH is the diagonal component. These bands are shown in Figure 1.



LL_1	HL_1
LH_1	HH_1

Figure 1. Components of 1 level 2 dimensional Discrete Wavelet Transform

With the DWT, the significant part (smooth parts) of the spatial domain image exist in the approximation band that consists of low frequency wavelet coefficients and the edge and texture details usually exist in high frequency sub bands, such as HH, HL, and LH. The secret data are embedded to the High Frequency components as it is difficult for the human eye to detect the existence of secret data.

4. Proposed Steganography Method using DWT and Chaotic Neural Network

Algorithm for embedding

1. The Text is ciphered using Ceaser Cipher.
2. The ciphered text is encrypted using Chaotic Neural Networks
3. The encrypted text is embedded into the image using DWT.

Algorithm for extraction

1. From the stegano image the embedded text is recovered using DWT.
2. The extracted text is decrypted using Chaotic Neural Networks
3. The decrypted text is a cipher text and this in turn is converted into readable text by applying the inverse Caeser.

5. Construction and Working of Proposed Algorithm

This has been executed using MATLAB 7.14.0.739.

Caeser Cipher

Caeser Cipher is the well-known and widely used simple encryption technique. This will just shift the text based on the key.

Algorithm for Ceaser Cipher is as follows
Input : Plain Text
Output : Cipher Text

1. Read the message
2. Select the key
3. Shift the number of characters based on the key.
4. Cipher text is obtained.

Encryption using Chaotic Neural Networks

Algorithm for Chaotic Neural Network

Input : Plain Text
Output : Encrypted Text

1. Read the message.
2. Calculate the length of the message and divide the message into subsequences of 8 bytes.
3. Set the Parameters, μ and the initial point x(0).
4. The chaotic sequence x(1), x(2), x(3)…. X(M) is evolved using the formula

   X(n+1) = μx(n)(1-x(n))

5. Create b(0),b(1)…b(8M-1) from x(1),x(2)….x(M) by the generating scheme that b(8m-8)b(8m-7)…b(8m-1)… is the binary representation of x(m) for m= 1,2,…M.
6. For n = 0 to (M-1),

```
For i= 0 to 7
    j = {0,1,2,3,4,5,6,7}
    Wji =  1   if j=i and b(8n + i) = 0
          -1   if j=i and b(8n + i) = 1
           0   if j≠i
    $\Theta_i$ = - ½  if b(8n+i)=0
           ½  if b(8n+i)=1
End
For i=0 to 7, $d_i$ is calculated using
        $d_i = f(\sum_{i=0}^{i=7} w_{ij} d_i + \theta_i)$
        where f(x) is 1 if x>=0
End
$g(n) = \sum_{i=0}^{i=7} d_i \, 2^i$
End
```

Thus the encrypted signal *g* is obtained.

Embedding the Data

The DWT of the image is obtained using Haar Wavelet transform. In Haar Discrete Wavelet Transform, the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels.

Input : Cover Image
Output : Stegano Image

Algorithm for DWT embedding

1. The DWT of the image is taken.

2. Insert the encrypted text in the DWT coefficients of the selected sub-band.
3. The inverse of DWT is applied resulting the stego image.

Extracting the Data

*A*lgorithm for extracting the encrypted data from stego image

Input : Stegano-Image
Output : Secret message in encrypted form

1. Apply the DWT of the stegano image.
2. Extract the encrypted text from the DWT coefficients

Decryption using Chaotic Neural Networks

Decryption is the process of converting the crypted text to plain text. Chaotic Neural Network performs the similar technique used in encryption process. The inverse of Encryption is performed by providing the input to the network with the encrypted text.

Input : Encrypted Text
Output : Plain Text

Algorithm for Ceaser Cipher to obtain the plain text is as follows

Input : Cipher Text
Output : Plain Text

1. Read the cipher text
2. Inverse Shift is performed based on the number of characters based on the key.
3. Plain text is obtained.

6. Simulation Results and Analysis

Some experiments have been conducted to prove the efficiency of the proposed algorithm. A GUI was developed using Matlab 7.14.0.739. Figure 2 shows the GUI performing Embedding and Extracting in the Barbara image. The Quantitative performance of the proposed algorithm is evaluated based on Peak signal to noise ratio (PSNR), Mean Square Error (MSE) and Structural Similarity of Image(SSIM) which are given in equations 5,6,7 respectively.

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad \text{--- Eq.5}$$

$$\text{MSE} = \frac{\sum_i \sum_j (r_{ij} - x_{ij})2}{M \times N} \quad \text{--- Eq.6}$$

$$\text{SSIM}(x,y) = [l(x,y)]^{\alpha}.\ [c(x,y)]^{\beta}.\ [s(x,y)]^{\gamma} \text{ -Eq.7}$$

Where *r* refers to Original image, n gives the corrupted image, *x* denotes restored image, M x N is the size of Processed image.
SSIM[5] is based on luminosity, contrast and structural similarity.
The qualitative performance of the proposed algorithm is tested on various images such as Lena, Cameraman, Barbara, Boat, Pepper, House (Images are chosen as per the details of the image). The secret text of length 2500 bytes is taken for testing. Performance of the method has been evaluated in terms of PSNR, MSE and SSIM. Results are given in Table 1.

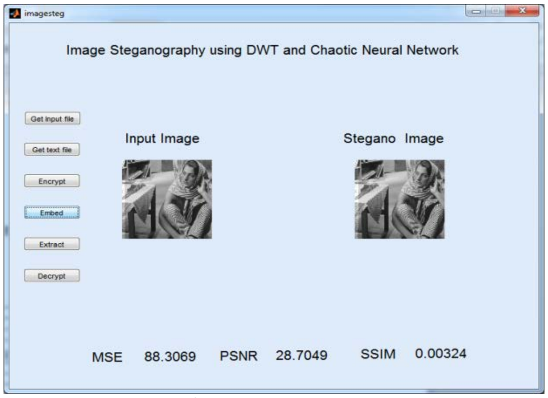


Image Steganography using DWT and Chaotic Neural Network

MSE 88.3069 PSNR 28.7049 SSIM 0.00324

Figure 2. GUI of the Proposed algorithm in Matlab

TABLE 1: PERFORMANCE OF PROPOSED ALGORITHM ON VARIOUS IMAGES

IMAGE	MSE	PSNR	SSIM
Barbara (512*512)	88.3069	28.7049	0.00324
Boat (512*512)	92.8255	28.4881	0.0037
LENA (512*512)	91.6927	28.5414	0.0041
Camera man(256*256)	359.0346	22.6134	0.0100
House (256*256)	368.0820	22.5054	0.0051
Peppers (256*256)	354.1158	22.6733	0.0044

Figure 3, shows the PSNR and MSE of various images of size 512*512. Figure 4, shows the PSNR and MSE of various images of size 256*256.Figure 5, shows the SSIM of various stegno images with their original images.

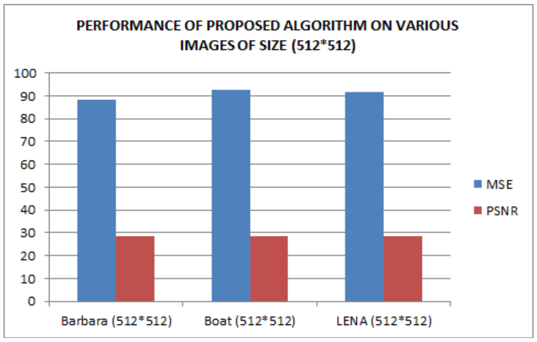


Figure 3.PSNR, MSE of Proposed Algorithm on various images of size 512*512

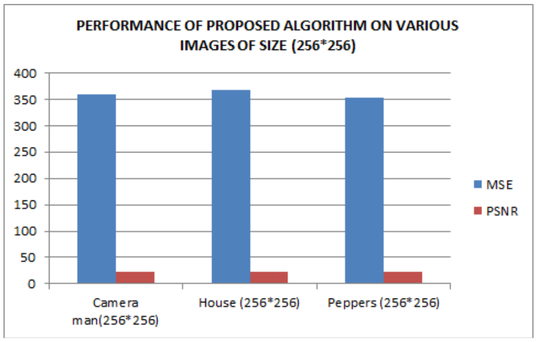


Figure 4.PSNR, MSE of Proposed Algorithm on various images of size 512*512

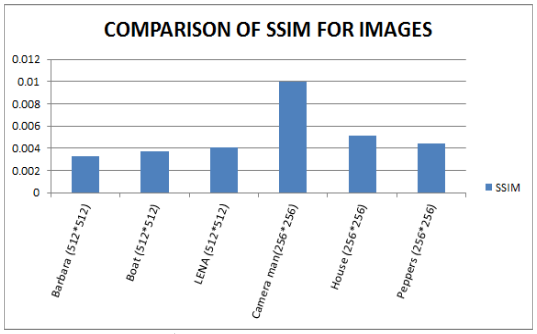


Figure 5. SSIM of Proposed Algorithm on various images

From the above Figures, we can notice that better results are obtained for the High dimension images.

7. Conclusion

In this Paper, a high Secure Image Steganography algorithm using Chaotic Neural Network for encryption of the text file is presented. The embedding process is done using the DWT transformation of the cover image. Chaotic Neural Network is highly secure technique in cryptography, since the chaotic sequence is unpredictable. The secret data of length 2500 bytes is embedded into the cover image and the qualitative performance of the proposed system is shown in Figure 3 and Figure 4. The PSNR, MSE varies depending on the amount of data embedded in the image and the size of the image. The proposed system is evaluated for Image Quality which is measured by image metric 'SSIM' and it is shown in Figure 5. Better results are noticeable for the 512*512 size images.

References

[1] Yu W, Cao J. "Cryptography based on delayed neural networks". PhysLetter A ;356:333–8. 2006

[2] Wu Xiaogang, Hu Hanping, et al. "Analyzing and improving a chaotic encryption method. Chaos", Solitons & Fractals; 22: pp 367–73, 2004.

[3] Chan, C.K. and Cheng. L.M. "Hiding data in image by simple LSB substitution". Pattern Recognition, 37: pp 469 – 474, 2003.

[4] Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh, "Image Quality Assessment: From Error Visibility to Structural Similarity" IEEE Transactions On Image Processing, VOL. 13, NO. 4, pp. 600-612, April 2004.

[5] H. Arafat Ali. "Qualitative Spatial Image Data Hiding for Secure Data Transmission". GVIP Journal, 7(1): pp 35-43,2007.

[6] Chen, T.S., Chang C.C., and Hwang, M.S. "A virtual image cryptosystem based upon vectorquantization". IEEE transactions on Image Processing, 7,(10): pp 1485 – 1488, 1998.

[7] Chung, K.L., Shen, C.H. and Chang, L.C. "A novel SVD- and VQ-based image hiding scheme. Pattern Recognition Letters" 22: pp 1051 – 1058, 2001.

[8] Iwata, M., Miyake, K., and Shiozaki, A. "Digital Steganography Utilizing Features of JPEG Images, IEICE Transfusion Fundamentals". E87-A(4): pp 929 – 936, 2004.

[9] Mythreyi S and Vaidehi V. "Gabor Transform based Image Steganography", IETE Journal of Research, 53(2): pp 103 – 112,2007

[10] A.A. Abdelwahab, L.A. Hassan. "A discrete wavelet transform based technique for image data hiding", Proceedings of 25th National Radio Science Conference, Egypt, 2008

[11] Chen, P.Y. and Wu, W.E. "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, 4,3: pp 275 –290.

[12] Harpreet Kaur and Tripatjot Singh Panag, 'cryptography using chaotic neural network' , International Journal of Information Technology and Knowledge Management July-December 2011, Volume 4, No. 2, pp. 417-422.

[13] Miles E. Smid and Dennis K. Branstad.'The Data Encryption Standard: Past and Future', proceedings of the ieee, vol. 76, no. 5, , pp 550-559, May 1988.

[14] Ilker Dalkiran, Kenan Danisman. 'Artificial neural network based chaotic generator for cryptography', Turk J Elec Eng & Comp Sci, Vol.18, No.2, pp, 225-240, 2010.

[15] Shweta B Suryawanshi and Devesh D.Nawgaje, "A Triple key chaotic neural network for cryptography in Image processing" International journal of Engineering sciences & Emerging technologies, vol 2,No 1, pp 46-50, April 2012.

B.GeethaVani has received the B.Tech degree in Computer Science and Engineering from JNTU Hyderabad in 1993 and M. Tech degree in Computer Science and Engineering from JNTU Hyderabad in 2003. Currently pursuing Ph.D from JNTU Kakinada, India. Research interests include Theory of Computation, Artificial Neural Networks, Image Processing and Network Security.

Dr.E.V.Prasad has received Ph.D degree in Computer Science and Engineering from I.I.T, Roorke. He is having 34 years of experience in teaching. He joined in JNTU College of Engineering in the year 1979 and served in various positions like Head of the Department, Vice Principal, Principal, Director of IST, Registrar and presently Rector. He has taught over 16 courses in CSE and has guided 6 Ph.D students successfully and presently supervising 9 Ph.D candidates. He is the Co author of six books and published more than six dozen papers in national and International journals and conferences. His research interests include Parallel Computing, Data Mining, and Information Security.