International Journal of Advanced Trends in Computer Applications
www.ijatca.com

A Review: Genetically Modified Neural Network Used For Image Steganography

Hafsa Zargar[1], Harpreet Kaur[2]

[1] Hafsa Zargar
Shaheed Udham Singh College of Engineering and Technology
Tangori (Mohali)
Research Scholar, Department of CSE
hafsazargr8@gmail.com

[2] Harpreet Kaur
Shaheed Udham Singh College of Engineering and Technology
Tangori (Mohali)
Assistant Professor, Department of CSE
harpreetk857@gmail.com

Abstract: *Steganography is the enhancement of the historical approach in which messages were transmitted by hiding its existence. Steganography emphasizes on concealing the data in some carrier medium. During communication process typical lsb steganography is not a secure way for message transmission. So a first level secure DWT based steganographic technique is proposed in integration with neural network which is further optimized with genetic algorithm using a fitness function. The second level encryption is provided to the text which uses 2 fish algorithm for generating key and elgamal algorithm for encrypting text using key generated by 2 fish. This algorithm provides more security and better image quality. The effectiveness of the proposed method can be estimated by calculating the peak signal to noise ratio (psnr) and mean square error(MSE).*

Keywords: *steganography, dwt, neural network, 2 fish, elgamal*

1. Introduction

Since the rise of internet proffering security is the point to be focused on. Cryptography was the technique which was created for concealment of private data. Unfortunately it is infeasible enough to keep the contents of the message secret, however conformity of its existence differs .The technique used to implement this, is called steganography[1].Steganography differs from cryptography in their triats. Cryptography has the power of retaining a message secret, whereas steganography has the power of retaining the existence of a message secret[4].Steganography and cryptography are conjunctively used for guarding information from third parties but neither technology alone is substantial and can be compromised. Once the revelation of hidden information is made or even doubtful, the purpose of steganography is partly subjugated [4]. The strength of steganography can thus be boasted by uniting it with cryptography. In this approach steganography and cryptography are aggregated together. Steganography is done by aggregating DWT with genetically optimized neural network and cryptography is done by encrypting text using elgamal algorithm using the key generated by 2 fish.

2. MOTIVATION AND BACKGROUND

Information security is nowadays a point of concern due to the fast growth of internet and technology. Data integrity and confidentiality are the two main aspects in the field of information security systems. Black hat hackers' increases day by day and their capability of breaking the encryption algorithms also increase. Thus there comes the need of steganography. Image steganography is the most popular type in which image is the carrier. Image steganography is divided into spatial and transform domain. In spatial domain messages are embedded in the intensity of image pixel like in LSB. In transform domain the images are first transformed using dct or dwt based transformations.

3. DWT TRANSFORMATION

A first level dwt is obtained in our approach which is done by scanning the pixels first in right to left in horizontal direction and then from top to bottom in vertical direction. Addition and subtraction operation are performed on the neighboring pixels. Sum is stored in the right and difference in the left for horizontal scanning; this process is repeated until horizontal scanning is traced. The pixel sum represents the low frequency part and the pixel difference represents high frequency part. For the pixels scanned in vertical direction again addition and subtraction is performed for the neighboring pixels. Sum is stored on the top and difference on the bottom of the pixels. This operation is repeated until all columns are processed. Finally we will obtain 4 sub bands denoted as LL, HL, LH, and HH respectively. In the proposed approach all the lsb's of the pixels are obtained from LL sub band.

From the previous studies it has been summarized that DWT is a better approach than DCT. They belong to the wavelet families. The psnr and mse values for different threshold have been carried for the sample images. High psnr for DWT summarizes that DWT is better approach to be used than DCT.

Figure 1: carrier image LENA

For the image LENA the parameters for DWT and DCT are calculated which will define the image quality as shown in table 1.on different threshold values different values for specific transforms are obtained. PSNR and MSE values are which will define the corresponding image quality.

Table 1: PSNR (in DB) and MSE values at different threshold values for LENA image sample

Threshold	Transform type	DCT	DWT
10	PSNR	37.5321	37.7149
	MSE	11.4781	11.0050
20	PSNR	33.2485	33.4413
	MSE	30.7771	29.4409
30	PSNR	30.8452	31.1016
	MSE	53.5249	50.4569
40	PSNR	29.2907	34.9446
	MSE	71.7549	20.8268
50	PSNR	28.3884	34.0183
	MSE	94.2415	25.7782

4. GENETICALLY MODIFIED NEURAL NETWORK (GANN)

Neural network in this approach is used for training the lsb's of the image after applying dwt transformation. The idea of combining genetic algorithm with the neural network paved its way out in the field of research. The problem with the neural network is that the number of parameters has to be calculated before any training section can begin in its way. However there is no such clue of setting these parameters [2].By combining genetic algorithm with neural network, the genetic algorithm is used to find these parameters.

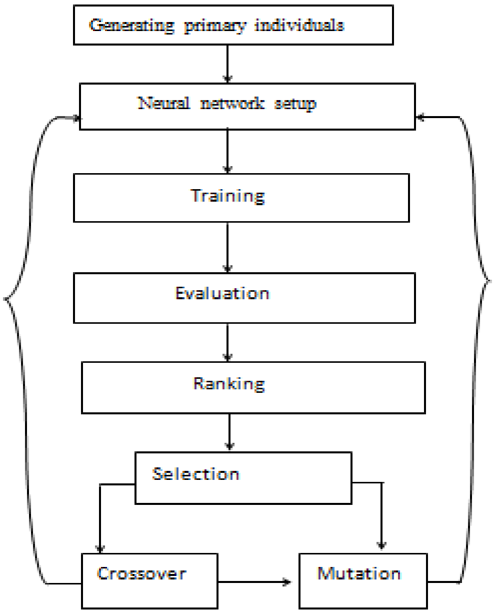

Figure 2: Principle approach to GANN

Training neural network propounds inquisitor with innumerable credits. Artificial neural network channelizes with grains of information and makes it possible for the information to be generalized. Neural network memorize to diagnose templates on the data set. Neural network replaces programming by learning approach. This will greatly reduce time consumption as programming is much more time consuming than learning. Gnome-stationed system is applicable to certain rules for which programming is done incorporated with model based rules. These are biased, when rule is changed due to certain circumstances the model is no more applicable and need to be changed. On the other hand neural network plays its controversy as it is a pliable approach. Although it takes some time to grasp the changes but at the same time has the power of molding the desired changes.

The startup procedure of neural network is by making use of relevant neural model which are nothing but the multi-neurons[6]. These can be illustrated by underlying architecture and memorizing algorithms. For a neural network model there is a set of input and an output layer and some hidden layers between these two input and output layers. This forms the basic model of multi-layer feed-forward neural network (MLFF).fig 3 gives the description of feed-forward neural network.

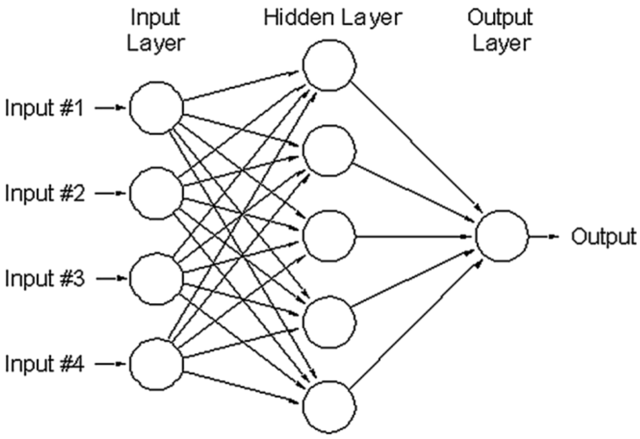

Figure 3: Multilayer feed forward neural identifier architecture.

There are no such criteria as to the count on the hidden layers. The number of hidden layers depends on the weight adjustment factor, and the weights are adjusted according to the error incorporating in the model. Selection, crossover and mutation are the criteria that are met by the genetic optimizer. Genetic algorithms are an evolutionary approach. The selection is based on the survival of fittest rule. Those who met with the above rule donatetheir chromosomes to their descendants and those who don't extinct automatically.

5. HYBRID APPROACH TO ENCRYPTION

By hybridizing the cryptographic algorithm the effective power of two algorithms is obtained. These algorithms work in parallel and neither of them will obtain the results alone. In this approach the text is encrypted with the elgamal algorithm which will be done with the help of keys generated by 2 fish.

Two fish is a symmetric block cipher. Two fish distinctive feature is that the key dependent S-boxes are recomputed; in turn it has a complex key schedule. The first half of key is used as actual encryption key and the remaining half of n-bit key is used to make partial changes to the encryption algorithm. It has a 16 rounds fiestal network with non-trivial information in every round.

The algorithm with its key size and block size are illustrated in the below mentioned table. From the performance analysis of data encryption algorithm it has been estimated that blowfish and two fish are the fastest encryption algorithm and DES is the slowest [11].Two fish algorithm eliminates the limitation of blow fish algorithm by not selecting the key dependent s-boxes.

Algorithm	**Key size(bits)**	**Block size(bits)**
DES	64	64
3DES	192	64
Rijndael	256	128
Blowfish	448	64
Two fish	448	128

Table 1: Symmetric block cipher comparison

Elgamal algorithm is based on the difficulty of finding discrete logs because it is much difficult to find the inverse of discrete logs. The Elgamal algorithm can be used instead of RSA algorithm for public key encryption.

Elgamal is the advance version of Diffie-Hell_men key exchange protocol. The cipher text is different from the same plain text each time it is encrypted.

Thus combining the power of two fish and elgamal we can get an effective encryption for the text to be embedded inside an image. If by chance the first level steganography technique breaks, it will still be difficult to break the second level encryption, thus enhancing the security.

6. CONCLUSION

This paper is the review of the steganography technique which will be implemented with genetically modified neural network. The power of this technique will be illustrated by means of psnr value which will be high. Psnr will represent the image quality. The need for enhancing psnr value is to avoid the suspicious images to be known by hackers that will creep in across the network. The abnormality of the image is avoided for acquiring of the confidential data. Improvement of the technique can still be emerged by making neural network work as steganalysis tool, so that there is no need for decryption across the receiver side.

REFERENCES

[1] T. Morkel“Steganography and Steganalysis”, Information and Computer Security Architecture (ICSA) Research Group.

[2] EktaDagar,SunnyDagar ”, LSB Based Image Steganography Using X-Box Mapping” IEEE-2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[3] V.Saravanan, A. Neeraja”, Security Issues in Computer Networks and Steganography” Proceedings of7'h International Conference on Intelligent Systems and Control (ISCO 2013).

[4] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM, 47:10, October 2004.

[5] TandelBhavisha *, Mr.Divyesh Joshi”,Survey on different stenographic technique”http: // www.ijesrt.com © International Journal of Engineering Sciences & Research Technology.

[6] AkshayPhadke, AditiMayekar.”NewSteganography Technique using Neural Network”International Journal of Computer Applications (0975 – 8887) Volume 82 – No 7, November 2013.

[7] Mrs.Archana S. Vaidya, 2Pooja N. More., 3Rita K. Fegade., 4Madhuri A.Bhavsar., 5Pooja V. Raut.,” Image Steganography using DWT and Blowfish Algorithms”IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 8, Issue 6 (Jan. - Feb. 2013), PP 15-19.

[8] Imran SarwarBajwa School of Computer Science University of Birmingham Birmingham, UK imran.sarwar@cs.bham.ac.uk,”A New Perfect Hashing based Approach for Secure Stegnograph”2011 IEEE.

[9] El-Sayed M. El-Alfy,”Detecting Pixel-Value Differencing Steganography Using Levenberg-Marquardt Neural Network” 2013 IEEE.

[10] Mohammad JavadKhosravi • Ahmad Reza Naghsh-Nilchi,”A novel joint secret image sharing and robust steganography method using wavelet”8 October 2013 Springer-Verlag Berlin Heidelberg 2013.

[11] O P Verma”Peformance Analysis Of Data Encryption Algorithms”IEEE-2011