Efficient Encryption and Password Protected Multi-Neuron Approach For Data Hiding In Image Steganography

Hafsa Zargar, Er. Harpreet Kaur, Dr. Dheerendra Singh
[1]Mtech (CSE) Student, [2] Assistant Professor, [3] Professor & Head (CSE)
SUS College of Engineering and Technology, Tangori, Mohali
hafsazargr8@gmail.com, harpreetk857@gmail.com, professordsingh@gmail.com

Abstract: Our research work center point is on building an algorithm that helps in transmitting information and protecting and keeping them safe from any eavesdrop or cruel third party by using the concept of steganography. Steganography is one of the approaches used to secure information. It is the art of forming hidden messages such that the planned receiver is the only party attentive of the existence of the message. Steganography algorithms use different cover media such as text, images, sounds and video. The proposed method encodes the secret message in least significant bits of the novel image by first using DWT technique, where the pixels values of the encrypted message are adapted by the hybrid approach of neural network and genetic algorithm to preserve their sign characters, thereby making the discovery of secret of message not easy. The planned work has been implemented using MATLAB.

Keywords: stego image, DWT, neural network with genetic algorithm (GANN), GANN model.

1. Introduction

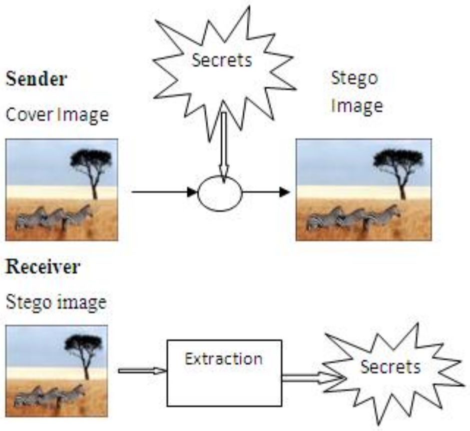
Globalization has led to the speedy growth of the internet through which customers can send and receive large amount of data (e.g., manuscript, auditory, video, and images). In recent communication systems, securing data is of extreme importance [1]. Until now sending and receiving covert files over the internet is still insecure, and therefore hiding data in an effective method protects this secret information [2].

1.1. **Data hiding using image Steganography**

Data is significant to any association. They must be sheltered from the illegal access. Data should only be visible to the sender and receiver of transmitted data, and they should be hidden from hackers [3]. Hiding data is nothing more than defensing the data in some intermediate or encrypting the data. There are many techniques that use the concept of hiding data; cryptography and steganography are among them. In our approach use of cryptography and steganography has been established to provide a two level security. Steganography is done by aggregating DWT with genetically optimized neural network and cryptography is done by encrypting text using 2 fish algorithm using the key generated by elgamal.

1.2. Mechanics of steganography

The crux of the steganography requires encapsulating the secret message inside the cover image. The first and foremost step is to select a cover image. It would seem most appropriate to select an innocent looking and an unsuspicious image. The next step is to select, install, and run a steganographic tool to plunge the secret in the cover image. Once embedding is done, we refer to this file as a stego file which is made ready to be sent to a receiver. Once the stego file is received, the intended recipient should be well framed with its reverse process, so that the information in the received end is achieved inauspiciously. The same steganography tool is used to extract the concealed message from the stego file. Figure depicts the layout of the secret communication.



3. GANN MODEL

Genetic algorithms and artificial neural networks work in conjugation with each other. Both of these evolved from biological systems. Neural networks are generally evolved from the examples, while GAs are deduced by means of analytical functions. Thus there comes the need of evolutionary neural network in which both techniques run hand in hand in order to increase the performance.GA limits its use for task domain. They may just find its way out in task domain which arises problem for training algorithms. For generalized structure/parameter learning in neural systems GA has revealed its importance. This type of learning has the property to act complimentary for inductive as well as synaptic weight adjustments. The use of deductive

DOI: 10.141079/IJITKM.2015.811

learning has adapted the system knowledge of domain environment. Such hybrid systems have ability of finding both the weights and the architecture of a neural network, which includes number of layers, the processing elements per layer and their connectivity.

4. Methodology

The proposed method is implemented in MATLAB platform using standard cryptography and steganography algorithm [9].Encryption Algorithm hybrid cryptography is used along with Genetic algorithm and neural Network. Below Figure shows the working of proposed information security scheme.

Cover image: It is the carrier image which is to be transmitting to the receiver side. It will carry the covered data.

Transformed image: It will denote the probabilistic symphony of the frequencies for the cover image. Thus the image will be composed of DWT coefficients.

Optimized LSB: The hybrid approach GANN of neural network training and genetic algorithm will find the optimized empty LSB coefficients from the actual part of DWT, which are responsible for concealing the data.

Encrypted text: It will denote the encrypted form of data that is the important message to be concealed inside LSB. It is done using hybrid approach of 2 fish and elgamal algorithm.

Embedding process: It will embed the stego key, password, cipher text inside the trained LSB unit using sum rule. Thus our carrier image will be embedded with encrypted secret message which is concealed within the carrier image.

Stego image: The final processed image concealing secret data inside the cover image will be called as the stego image.

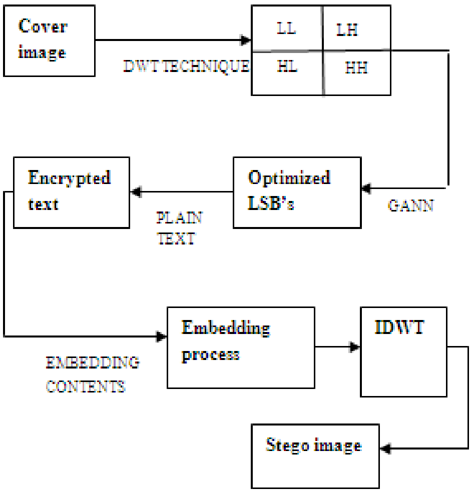


Figure no: 4(a) Sender Side Process

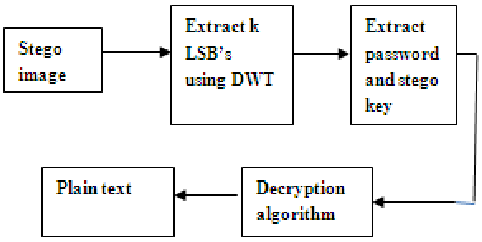


Figure no: 4(b) Receiver Side Process

5. Proposed work

Embedded algorithm:

The embedding process works as follows:

- Partition the cover image into 4 *4 pixels.
- Evaluate the frequency entities of blocks by means of 1D Haar Discreet Wavelet Transform and four sub bands LL1, HL1, LH1, and HH1 are formed.
- Train the neural network by inputting the features extracted from LL1 band and find the blank locations.
- Genetic algorithm is used by optimizing the neural network. Encrypt the message using hybrid algorithm using hybrid approach of 2 fish and elgamal algorithm.
- Calculate the length of the text to determine the no of lsb's used for embedding.
- Embed the encrypted message bits, password and key in empty LSBs which are trained by genetic algorithm with neural network functioning.

Extracting Algorithm:

The extraction algorithm works according to the four steps as follows:

- Separate the stego image into 4x4 blocks.
- Infuse transform domain coefficient by means of calculating 1D HDWT of each 4x4 block.
- Find the pixel sequences for extraction by utilizing the obtained function in the embedding phase
- Infuse k-LSBs in each pixel.

6. Results and discussions

A. RESULTS

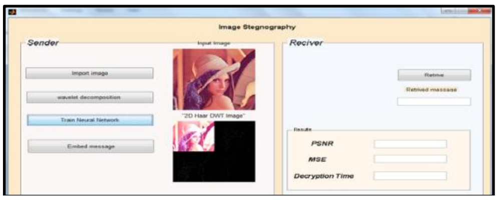


Figure no: 6.1 Sender and receiver side interface

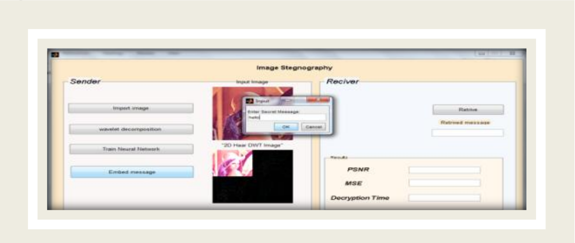
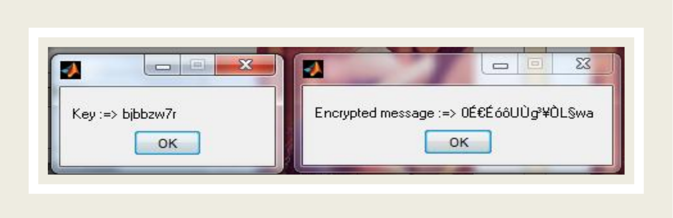


Figure no 6.2: Message to be embedded inside image


Key :=> bjbbzw7r

OK

Encrypted message :=> 0É€ÉóôUÙg³¥ÒL§wa

OK

Figure no 6.3: stego key and encrypted message for secret image

The optimization using fitness function will follow a number of iterations .When the iterations are complete stego image is created in which encrypted message and key will be embedded. The stego image formed will entirely look like input image thus avoiding suspicious communication.

B. CALCULATION OF PARAMETERS:

Some of the input images are taken and there corresponding PSNR, MSE decryption time and accuracy values are generated.

Figure no 6.4: Some carrier images used (Barbara, leena, polar bear, and jellyfish)

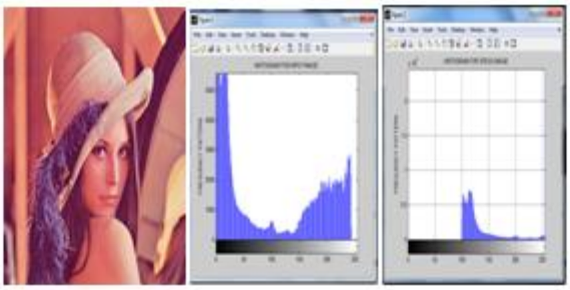
The image quality of stego image is compared with the original image by means of calculating PSNR and MSE. The accuracy rate and decryption time are also specified in the below table.

Table 6.5: PSNR, MSE, ACCURACY and decryption time of color images

COVER IMAGE	MESSAGE	PSNR	MSE	ACCURACY	DECRYPTION TIME
Barbara	“hello”	89.4769	0.000024	97.30	0.16ms
Leena	“hi”	89.4261	0.000025	97.6	0.38ms
Polar bear	“seema”	89.409	0.000022	97.6	0.28ms
jellyfish	“see”	89.8921	0.000021	97.66	0.83ms

From the above table the various parameter results have been generated. Increased psnr shows high image quality and further decrease in mse shows high image quality. Thus PSNR and MSE are inversely proportional to each other.

C. COMPARING HISTOGRAM OF ORIGINAL IMAGE AND STEGO IMAG

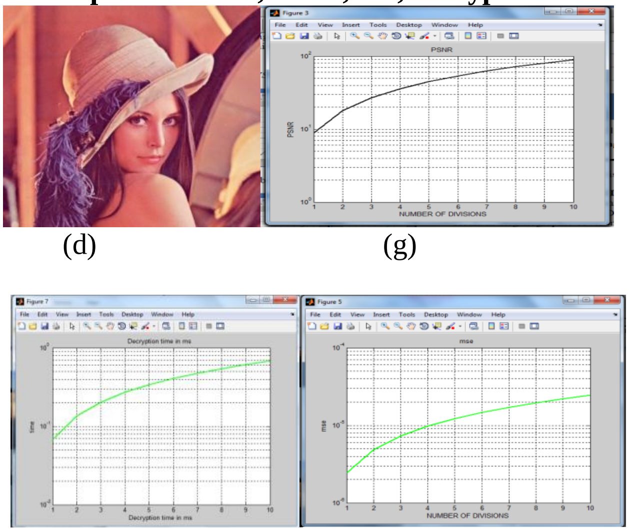


(a) (b) (c)

Figure no: 6.6 Cover image and their corresponding histograms (a) Leena (b) Histogram of original image (c) Histogram of Stego image

Histogram of stego image formed is different from that of the histogram of the original image. This is due to the fact of adding extra bits to the image and the changes incorporated in the original image.

D. Graphs of PSNR , MSE ,and, decryption time



(d) (g)

(e) (f)

Figure no: 6.7 PSNR, MSE and decryption time graph of image

(d) Leena (g) PSNR graph (e) decryption time graph (f) MSE graph

E. COMPARISON TO THE PREVIOUS APPROACH

The below table shows the comparison of our proposed technique with the previous technique for an input image “leena” of size 256 *256 color image. The value obtained for the proposed technique in genuine and high which has resulted in an efficient steganographic technique.

TABLE 6.8: Comparison of PSNR and MSE between our proposed work, chang’s, lin’s and wavelet method for image “leena” of size 256 * 256

METHOD	AVERAGE	AVERAGE

	PSNR	MSE
Chang's method	40.88	0.000045
Lin's method	39.99	0.000053
Robust steganography using wavelet method	43.11	0.000041
Proposed method	88.52	0.000031

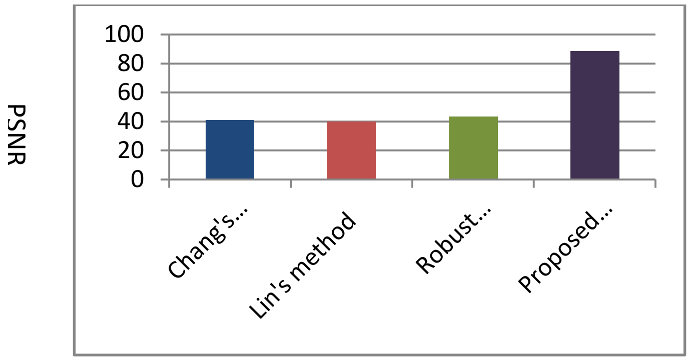


Figure 6.9: Performance analysis in terms of psnr ratio

The information depicted in the above table has been graphically represented by the above graph in order to improve readers understanding.

F. CONCLUSION AND FUTURE SCOPE

A few years, Steganography has become a troubled field of data hiding method. This paper provides a thought of different steganography method that satisfies the most vital factors of steganography design. These are not detectability, and have capacity and strength. Steganography has its place in protection. It is not projected to replace cryptography but enhancing it. There is a provision for non-detectability of message by hiding its contents. However, if that meaning is also encrypted, if exposed, it must also be fractured .There is an infinite number of steganography applications. This paper explores a tiny fraction of the art of steganography. It goes well past simply embed text in an image. The consequences and discussions in the above chapters have clearly shown this idea. The security is added to the method by hybriding an asymmetric cryptography algorithm with the symmetric cryptography algorithm. Thus if somehow there are chances that steganography has been exposed by interloper but the second level security provided to the secret message keeps the contents secret. Thus the proposed technique works both on keeping the contents as well as existence of the message secret.

In the present work genetically modified neural network along with hybrid approach to encryption has been used. Development 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. To add extra security, the prospect focus to on increasing this tool to work in all formats, i.e., hiding digital files in any digital file, as this tool focuses only on hiding text in digital files. In count, tool also gets more security when both the steganography and cryptography concepts are used together.

REFERENCE

[1] M. Niimi, S. Minewaki, H. Noda, and E. Kawaguchi, "A Framework of Text-based Steganography Using SD-Form Semantics Model", Pacific Rim Workshop on Digital Steganography 2003, Kyushu Institute of Technology, Kitakyushu, Japan, July 3-4, 2003.

[2] K. Rabah, "Steganography-The Art of Hiding Data", Information Technology Journal, vol. 3, Issue 3, pp. 245-269, 2004.

[3] Petitcolas, F.A.P., (2000). "Introduction to Information Hiding". In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.

[4] K. Rabah, "Steganography-The Art of Hiding Data", Information Technology Journal, vol. 3, Issue 3, pp. 245-269, 2004.

[5] M.Hassan Shirali-Shahreza, Mohammad Shirali-Shareza, "A New Approach to Persian/Arabic Text Steganography", Proceedings of the 5th IEEE/ACIS International Conference on computer and Information Science, 2006 IEEE.

[6] Pfitzmann, B., Information hiding terminology - results of an informal plenary meeting and additional proposals. In: Proceedings of the First International Workshop on Information Hiding. Springer-Verlag, London, UK, pp. 347–350. (1996).

[7] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[8] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996.

[9] N. Johnson and S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer, pp. 26-34, February (1998).

[10] Mustafa, A. E. A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit. Diss. Mansoura University, 2011.

[11] Silman, J., "Steganography and Steganalysis: An Overview",SANS Institute, gsec 1.2f (august 2001)

[12] Lee, Y.K. & Chen, L.H., "High capacity image, steganographic model", Visual image SignalProcessing, 147:03, June 2000.

[13] Rojalina Priyadarshini, Nillamadhab Dash, Tripti Swarnkar, Rachita Misra," Functional Analysis of Artificial Neural Network for Dataset Classification", Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], 3-5 August 2010.

DOI: 10.141079/IJITKM.2015.811