IMAGE STEGANOGRAPHY USING 2-LEVEL DWT AND ARTIFICIAL NEURAL NETWORK

Harpreet Kaur[1], Jyoti Saxena[2], Sukhjinder Singh[3]
[1]Giani Zail Singh Campus College of Engineering & Technology, MRSPTU, Bathinda-151001 (Punjab),India
[2]Giani Zail Singh Campus College of Engineering & Technology, MRSPTU, Bathinda-151001 (Punjab),India
[3]Giani Zail Singh Campus College of Engineering & Technology, MRSPTU, Bathinda-151001 (Punjab),India
(E-mail: kaurharpreet07733@gmail.com)

Abstract— Steganography plays an important role in the field of information hiding. It is used in a variety of applications such as Internet security, authentication, copyright protection and information protection. In this research, image steganography model is designed to provide the security while transmitting the information in the form of an image. To provide high-security, different processes are implemented such as pre-processing that is used to resize the image, convert a color image into gray scale image and image decomposition. Histogram technique is used to determine the pixel values of the image and the pixels are optimized by using Genetic Algorithm (GA) by adjusting the fitness value of and hence obtained the optimal pixel group. Also, Artificial Neural Network (ANN) is used to train the system as per the cover image pixels and provide the pixels with less information loss. At last, the parameters such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI) and information Entropy are measured and compared with the existing work.

Keywords— *Image Steganography, Genetic Algorithm, Artificial Neural Network, Mean Square Error, Peak Signal to Noise Ratio, Number of Pixels Change Rate and Unified Average Changing Intensity.*

I. INTRODUCTION

Presently we live in the highly digital world in which computers help to convert analog data to digital data before storage and applying any processing [1]. At the same time, the Internet is developing very fast, so it has become an essential medium for transmitting digital data. However, as a completely open medium, the Internet not only brings us convenience but also brings some dangers and risks [2]. If the data to be transmitted is kept secret, it is convenient for some malicious users to illegally copy, demolish or change the data on the Internet [3]. Therefore, information security has become an important issue. Various data hiding schemes have recently been developed. According to the purpose of data hiding, these schemes fall into two categories named as watermarking and steganography [4]. Watermarking is a protection technique that protects user's property regarding images through some hidden watermarks. Conversely, steganography techniques use some cover images to protect confidential data from unintentional Internet users. There are two methods related to steganography, namely spatial and frequency domain methods. In the spatial domain method, the secret message is embedded in the least significant pixel of the cover image [5]. This method is very fast but sensitive to image processing attacks. The frequency domain method involves transforming the overlay image into frequency domain coefficients before embedding the secret message there in [6]. The conversion can be a Discrete Cosine Transform (DCT) and Discrete Wavelet Transforms (DWT). Although these methods are more difficult and slower than the spatial domain, in spite of this, it has the benefit of being more secure and noise tolerant [7]. In the proposed work, we present the very user friendly and robust Image Steganography using Artificial Neural Network with optimization. For the selection of suitable region from the cover image, we use Artificial Neural Network (ANN). Also, Genetic algorithm (GA) has been used to resolve the problem of optimization. Therefore, the image region that is noisier is ignored [8].

The remainder of this research paper is organized as follows. Section 2 demonstrates the related works. Section 3 presents proposed techniques that are used to enhance the efficiency of the proposed Steganography approach. Section 4 shows the experimentation and results followed by conclusion in section 5.

II. RELATED WORK

D. Baby et al., [9] proposed a data securing method that has been used for hiding manifold colour images into a solitary colour image by utilizing the concept of DWT. The cover image has been divided into R, G and B planes. The performance in terms of PSNR and SSIM value has been measured that shows the robustness of the research. D. K Srivastava et al.,[10] used advanced encryption standard (AES) technique to encrypt secret image at the initial stage. Later then, the encrypted image is hidden into the cover image using Haar DWT and alpha blending approach. The parameters such as PSNR, MSC and NCC have been measured. M. Hashim, et al., [11] presented an image steganography technique, the performance of which is measured on the basis of hiding capacity, security and distortion measure. Also, the authors have demonstrated various steganography tools like as RS and pixel difference histogram that is used to measure security parameter. R. Vijayarajeswari et al.,[12] has proposed a compression scheme that has been based on both level and integer matrix which enhance the compression level extensively. The performance of the proposed system has been evaluated in the form of computation parameters such as peak signal to noise ratio (PSNR), mean square error (MSE), a number of pixels change rate (NPCR) and unified average changing intensity (UACI). The proposed method obtained 42.65% PSNR, 27.16% MSE, 99.9% NPCR and 30.99% UACI. R. Karakış et al.[13] presented a Fuzzy logic algorithm along with a similarity index to select the Least significant bit (LSB) of the image pixel. For the security of the message, lossless compression along with encryption algorithm is used. The proposed work reduced the data repository as well as the transmission capacity of MR and EEG signals. S. Hemalatha et al.,[14] proposed a steganography approach by utilizing transform domain using wavelet transform to hide an audio signal in the image. The authors have considered audio signal format such as MP3 or WAV that is encrypted and the signal is transmitted to the medium along with the image. The analysis has been performed with different attacks and observed that the proposed technique is robust enough and also has the capability to withstand attack.

III. METHODOLOGY

This work proposes a data securing technique that is used for hiding multiple color images into a single color image using the concept of DWT with optimized artificial neural network. In this research, mainly three techniques are used namely DWT, GA and ANN.

A. DWT

DWT technique is used for decomposition of a cover image into 4 bands according to the pixels. The cover image is split up into LL, LH, HL and HH planes using the DWT decomposition technique and find out the best pixels group for hiding the secret image. Secret images are embedded into these planes based on their position using an artificial neural network. A 2-level DWT decomposition of the cover image and the secret images are done and some frequency components of the same are combined.

B. Genetic Algorithm

A genetic algorithm is an optimization algorithm that is used to determine the appropriate and optimal pixel group. The algorithm of GA is written as follows.

Algorithm 1: Genetic Algorithm

Input: Pre-processed pixels and Fitness Function

Output: Optimized Pixel Sets

```
1 Define: Fit Fun – Fitness Function: Fit Fun=
```

$$Fit\ Fun = \begin{cases} True; & if\ P_{val} < Threshold_{val} \\ False; & Otherwise \end{cases}$$

Where P_{val}: is value of pixel which are pre-processed and $Threshold_{val}$, is the threshold value of pixels which define on the basis of the mean of all pixel values.

```
2 Calculate, R as row and C as columns of pre-processed pixels (Img)
Initialize GA parameters    – Iterations (T)
                            – Population Size (P)
                            – Crossover function
                            – Mutation function
                            – Selection function
.
   (    $P_{val}$ and $Threshold$val
Optimized Pixel = []
5 for i = 1→R
6     for j = 1→C
          $P_{val} = \sum_{i=1}^{P} \text{Img (i)}$
8                    =
9         $Threshold_{val} = \frac{\sum_{i=1}^{P} \text{Img (i)}}{Length\ of\ Img}$
10        $Fit\ Fun = Fit\ Fun\ (P_{val}, Threshold_{val}))$
11
          $Optimized\ Pixel = GA\ (Fit\ Fun, Initialize\ Parameters)$
12    end
13 end
14 Returns: Optimized Pixel Sets
15 end
```

C. ANN

ANN is used as a classification algorithm that comprises three layers, input, hidden and output layer respectively. The optimized pixels are passed to the input layer. In the hidden layer, the input value of pixels is modified as per the sigmoid function. The error generated is measured by the MSE values.

Algorithm 2: Artificial Neural Network

Input: Optimized Pixel Sets as training data (T), Types of pixels (G), and Neurons (N)

Output: Embedding Pixel Sets

Training:

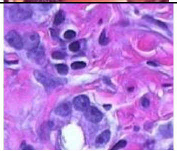
```
1 Initialize the basic parameters of ANN
      • Number of Epochs (E) // Iterations used by ANN
      • Number of Neurons (N)
      • Performance parameters of training: MSE
      • Technique: Levenberg Marquardt
      • Data Division: Random
2 for i = 1 → T
3     if T belongs to 1st type's pixel group
```

```
        Group (1) = Pixels of training data according to the lower bit
    else if T belongs to 2nd type’s pixel group
        Group (2) = Pixels of training data according to the higher bit
    else
        Group (3) = Pixels of training data which are extra (Some Cases)
    end
end
Initialize the ANN using Training data and Group
Net = Newff (T,G,N)
Set the training parameters according to the requirements and train the system
Net = Train (Net, Training data, Group)
Testing:
Test data = Pixels of Cover Image
Embedding Pixel Sets = simulate (Net, Test data)
Return; Appropriate pixel sets as an Embedding Pixel Sets
end
```

D. Database

The dataset taken from R. Vijayarajeswari et al., [12] paper Figure 1 represents the used database in the proposed image steganography module. The figure comprises of different figures (a) Baboon, (b) Fruits, (c) Lena, (d) Hestain and (e) Football. These images are used to simulate the proposed work and find out the efficiency of image steganography module. The description of database is given in table 1

TABLE I. DATABASE DESCRIPTION

No.	Image	Name	Format	Size
1		Baboon	jpg	109.12 KB (1,09,120 bytes)
2		Fruits	jpg	14.95 KB (14,950 bytes)
3		Lena	jpg	117.3 KB (1,17,300 bytes)
4		Hestain	jpg	78.21 KB (78,210 bytes)
5		Football	jpg	185 KB (1,85,000 bytes)

The parameters evaluated in the proposed work are defined below.

i. PSNR

This shows the correctness of the decoded hidden secret image as compared to the original secret image.

$$PSNR = 20 \log_{10} \frac{P_n}{\sqrt{MSE}}$$

Here, P_n signify the number of pixels in the secret image.

ii. mean square error (MSE)

This indicates the error rate measured while decoding the original secrete image and mathematically can be represented as:

$$SE = \frac{1}{y \times z} \sum_{0}^{b-1} \sum_{0}^{a-1} |f(i,j) - g(i,j)|^2$$

Here, f(I,j) defined the original secrete image, g(I,j) denotes the extracted secrete image, y and z represents the width and height of the secrete image.

iii. Number of pixels change rate (NPCR)

It is used to measure the different pixel percentage of two images (original image and decoded image). The formula can be written as:

$$NPCR = \frac{1}{y \times z} \sum P(i,j)$$

Let, p1 (I,j) signify the original secret image, p2 9i,j) defines the decoded image, therefore,

$$p(i,j) = \begin{cases} 1 & if\ p1(i,j) = p29i,j) \\ 0, & else \end{cases}$$

iv. unified average changing intensity (UACI)

It evaluates the average intensity of dissimilarity between the two images like original secret image and decoded image. It is represented as:

$$UACI = \frac{1}{y \times z} \sum_{0}^{b-1} |p1(i,j) - p2(i,j)|$$

v. Information entropy

This parameter represents that how much information is provided by the source image or the embedded image hence the information provided by the source image is termed as source information entropy (SI) entropy and the information provided by the embedded image in known as EI (embedded information) entropy.

IV. RESULT ANALYSIS

The test has been conducted on the above dataset and the following results are obtained after simulating the code in MATLAB tool. The parameters like PSNR, MSE, NPCR, UACI, EI entropy (entropy of embedded image) and SI entropy (entropy of source image) are measured to determine the performance of the proposed work. The parameters have been compared with the R. Vijayarajeswari et al. work. The average values of the proposed work along with the existing work are depicted in table 2.

TABLE II. Comparison of performance parameters with the existing work

	PSNR (dB)	MSE	NPCR (%)	UACI (%)	EI Entropy	SI Entropy
Proposed Work	60.38	5.67	98.74	16.10	7.34	7.36
Existing Work [12]	41.9	28.45	99.9	30.99	7.99	7.23

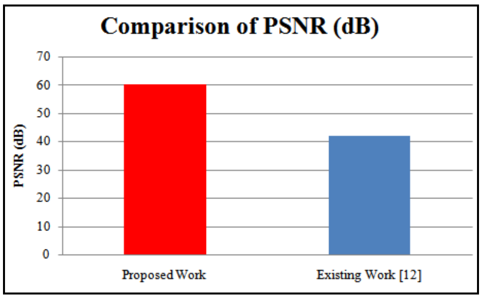


Figure 2: Comparison of PSNR

Figure 2 depicts the PSNR graph that comprises of average values of PSNR obtained after simulating the proposed work in MATLAB as well as with the values found in the base paper R. Vijayarajeswari et al., From the above graph, it is clear that the PSNR measured for the proposed work is more than the existing work and there is an increment of 44.11% in the PSNR value from the existing work.

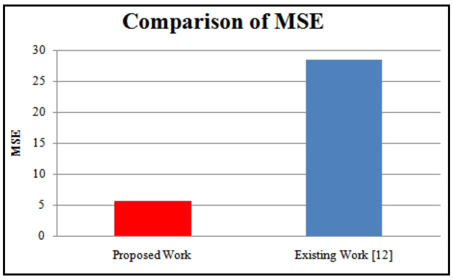


Figure 3 Comparison of MSE

Figure 3 displays the average values of MSE in graphical form. The red bar and the blue bar represent the average values of MSE observed for proposed and existing work respectively. From the graph, it has been observed that there is a decrement of 80.07% while comparing the MSE value with the existing work.

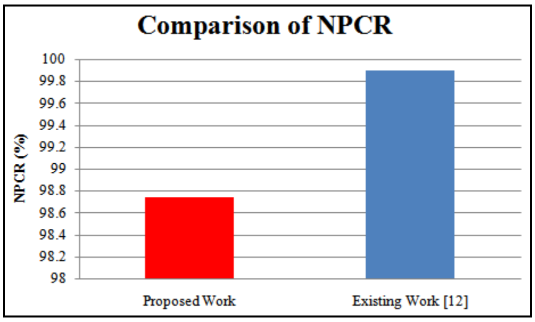


Figure 4 Comparison of NPCR

Figure 4 represents the comparison of average values of NPCR parameter for the proposed and existing work respectively. From the graph, it has been observed that the NPCR values have been decreased from the existing work by 1.16%.

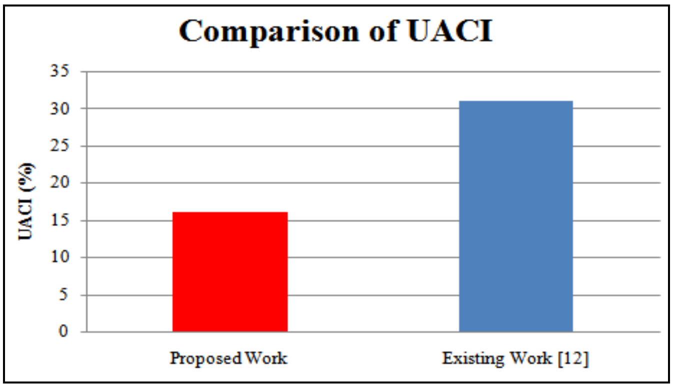


Figure 5 Comparison of UACI

The comparison of UACI measured in percentage has been depicted in figure 5. The graph shows that the UACI of proposed work is less than that of existing work and a decrement of 48.05% has been observed while comparing the proposed value with the existing one.

V. CONCLUSION

The goal of this research is to increase steganographic potential and increase the quality of stego image. Also, this research is to find a way or method to hide confidential information securely based on the optimized ANN classifier has been proposed to enhance the security level of the transmitted image. The compression technique has been used to integrate the secret binary image into the test image. The concept of DWT has been used to hide the multiple colour images into a single image. SWT decomposition scheme split the cover image into LL, LH, HL and HH planes and hence determine the best pixel to hide the image. The proposed design mainly focused on to achieve high entropy (secret image and embedding image) that shows the security of the system. From the experiment, it has been analyzed that the difference between the information entropy of secret image and information entropy of embedding image are very small as compared to existing work entropy. Also, the average value of PSNR about 60.38dB and average MSE approximately 5.67 has been achieved. The number of pixels change rate (NPCR) and the unified average changing intensity (UACI) of 98.74 and 16.10 have been measured.

In future, the research work can be extended by considering audio or video with an increase in security level. Also, the performance of the work can be increased by utilizing an artificial bee colony (ABC) as an optimization algorithm in hybridization with a genetic algorithm.

REFERENCES

[1]. A. V. Oppenheim, R. W. Schaffer, Digital Signal Processing, Engelwood Cliffs, N.J:Prentice Hall, 1975.

[2]. A. Z. Aos, A. W. Naji, S. A. Hameed, F. Othman, & B. Zaidan,, "Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File,"*International Association of Computer Science and Information Technology - Spring Conference*, Singapore, 2009, pp. 437-441.

[3]. A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images,"*IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, 2015, pp. 1-4.

[4]. A. Chaudhary and J. Vasavada, "A hash based approach for secure keyless image steganography in lossless RGB images," *IV International Congress on Ultra Modern Telecommunications and Control Systems*, St. Petersburg, 2012, pp. 941-944.

[5]. A. G. Ranade, S. Dargad and K. Mistry, "RGB Model Based Image Enhancement Technique for Steganography," *9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Bangalore, 2018, pp. 1-4.

[6]. A. Procházka and O. Vyšata, "History and biomedical applications of digital signal and image processing," *International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM)*, Paris, 2014, pp. 1-5.

[7]. L. R. Rabiner, & B. Gold, "Theory and application of digital signal processing," *Englewood Cliffs, NJ, Prentice-Hall, Inc., 1975. Pp. 777-786.*

[8]. B. Saha, & Sharma, S., "Steganographic techniques of data hiding using digital images,"*Defence Science Journal*, 2012 pp.11-17.

[9]. D., Baby, Thomas, J., Augustine, G., George, E., & Michael, N. R. (2015). A novel DWT based image securing method using steganography. *Procedia Computer Science*, *46*, 612-618.

[10]. D. K Srivastava & Sharma, V. K., &, "Comprehensive Data Hiding Technique for Discrete Wavelet Transform-Based Image Steganography Using Advance Encryption Standard," In *Computing and Network Sustainability* Springer, Singapore, pp. 353-360.

[11]. M. Hashim, M., Rahim, M. S. M., Johi, F. A., Taha, M. S., & Hamad, H. S, "Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. *International Journal of Engineering & Technology*, 2018, vol. *7, no.*4, pp. 3505-3514.

[12]. R. Vijayarajeswari, Rajivkannan, A., & Santhosh, J., "A Simple Steganography Algorithm Based on Lossless Compression Technique in WSN," 2016 Circuits and Systems, 2016, pp.1341-1351.

[13]. R. Karakış, Güler, İ., Capraz, I., & Bilir, E, "A novel fuzzy logic-based image steganography method to ensure medical data security,"*Computers in biology and medicine*, vol.*67*, pp.172-183.

[14]. S. Hemalatha, Acharya, U. D., & Renuka, A, "Wavelet transform based steganography technique to hide audio signals in image" *Procedia Computer Science*, 2015, vol.*47*, pp.272-281.