Enhanced Image Steganography System based on Discrete Wavelet Transformation and Resilient Back-Propagation

Reyadh Naoum, Ahmed Shihab, Sadeq AlHamouz

Middle East University, College of Information Technology, Computer Science Department Amman, Jordan

Summary
Image hiding is a form of steganography that works by embedding data into a digital media for the purpose of identification, annotation, and copyrighting. This paper introduces a novel image steganography system, which embeds (RGB) secret image within (RGB) cover image chosen by an enhanced resilient back propagation neural network. The proposed system includes embedding and extraction phases. Three main stages are included within the embedding phase, which are; best cover image selection and processing stage, secret image selection and processing stage and best embedding threshold selection stage respectively. Best cover image is performed using SOM and ERBP algorithms. Secret image is processed by separating it into (Red, Green, Blue) color layers and DWT is then applied. The color layers are then converted to bit streams; modified FLFSR in turns will be used to encrypt these streams to get more secure system. ERBP is again used to select the best embedding threshold values. The extraction phase will be performed the stego image result from embedding process. The performance has been evaluated during embedding and extraction stages considering using several cover and secret images and considering several sizes. Experiments show that (PSNR) is improved efficiently.

Key words:
Steganography, Neural Networks (NNs), Enhanced Resilient Back-Propagation (ERBP), discrete Wavelet Transformation (DWT), "Fibonacci Linear Feedback Shift Register (FLFSR)", Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MES).

1. Introduction

In a line with the recent development in communication filed, several techniques occurred and developed in order to securely and reliably transmit the data between communication process's parities. It is based on dimming the content of information by encrypting them, yet sometimes this kind of techniques can be insufficient. In some cases, it is better to hide the communication existence to stay away from any doubt from adversaries.

The techniques of information hiding are applied in many fields, e.g.; Digital media applications such as Audio, Video and pictures. These kinds of Digital media would hide some unnoticed information, copyright information or serial numbers. Sometimes such media would restrain unauthorized copying. Another living example of applying the information hiding techniques is the military communication systems which encrypt their messages to hide the communication existence or any part of the communication by applying the traffic security techniques (PETITCOLAS et al., 1999).

The term "information hiding" is related to the digital watermarking and Steganography. Watermarking are the methods of hiding any identifying data in a data object to keep the information strong against any kind of modification. Steganography is hiding the existence of any communication or information transferring attempt (STAMP, 2006).

Steganography can be viewed as akin to cryptography. Both have been used to add elements of secrecy to communication. Cryptographic techniques scramble a message so that if it is intercepted, it cannot be understood. This process is known as encryption and the encrypted message is sometimes referred to as ciphertext. Steganography, in essence, camouflages a message to hide its existence and make it seem invisible thus concealing the fact that a message is being sent altogether. A ciphertext message may draw suspicion while invisible messages will not (JOHNSON et al, 2001).

A general Steganography framework, it is assumed that the sender wishes to send, via steganographic transmission, a message to a receiver. The sender starts with a cover message, which is an input to the stego-system, in which the embedded message will be hidden. The hidden message is called the embedded message. A steganographic algorithm combines the cover message with the embedded message, which is something to be hidden in the cover (JALAB et al, 2010).

The algorithm may, or may not, use a steganographic key (Stego-key), which is additional secret data that may be needed in the hidden process. The same key is usually needed to extract the embedded message again. The output of the steganographic algorithm is the stego message. The cover message and stego message must be of the same data type, but the embedded message may be of another data type. The receiver reverses the embedding process to extract the embedded message. Figure 1 below shows a general Steganography framework (JALAB et al, 2010).

Manuscript received January 5, 2016
Manuscript revised January 20, 2016

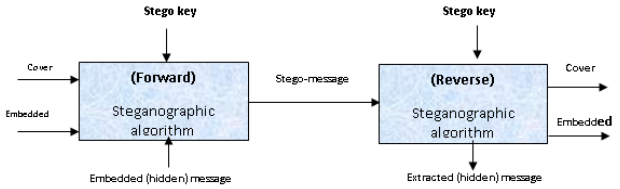

Fig. 1 General Steganography Framework (JALAB et al, 2010).

A novel steganography scheme will be implemented during this paper considering different algorithms to improve the performance as much as possible. The first section from this paper introduced an introduction to the steganography topic and information hiding. The remaining of the paper is organized as follow; the research scope is introduced in section 2, section 3 highlights some of the previous studies and researches related to steganography, section 4 introduces the system methodology in details, the steganography system's performance is evaluated in result and discussion in section5 and finally the summary and conclusion remarks of the whole work is introduced in section.

2. Research Scope

This paper aims to introduce a new robust and secure steganography system, based on a combination of two powerful algorithms (DWT and ERBP), this model can be used to hide full color secret image inside full color cover images without affecting them, in such a way that avoid drawing suspicion to the stego-image.

3. Previous Research

Geetha and Prasad (2010) presented a high secure steganography algorithm using DWT and Hopfield Chaotic Neural network. The proposed system contains three phases. In the first phase, the text is encrypted by using a traditional encryption method (Caeser method). In the second phase, 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 high frequency components of cover image (gray scale), using DWT.

Kumar and Muttoo (2011) presented a steganography techniques based on "Contourlet Transform (CTT)". The proposed technique uses a self-synchronizing variable length code to encode the secret image. The secret image then is embedded in the high frequency sub-bands obtained by applying CTT to the cover-image (gray scale), using rightmost of LSB and threshold methods.

Kumar et al (2011) implemented a "Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques (PCRSMT)". The Cover image as well as payloads is applied with DWT and IWT. "Most Significant Bits (MSB)" of payload IWT coefficients are embedded into "Least Significant Bits (LSB)" IWT coefficients of cover image.

Mandal (2011) presented a novel embedding approach termed as, FDSZT based on Z- transformation for gray scale, images where concept of median has been used to select the coefficient for embedding in Z-Transformed domain. One bit of the secret image is inserted into byte of the cover image in 2×2 mask. Insertion is done in the rightmost fourth LSB bit of the byte cover image

Kumar et al (2011) propose hybrid steganography, which is an integration of both spatial and transform domains. The cover image as well as the payload is divided into two cells each. The RGB components of cover image cell I are separated and then transformed individually from spatial domain to frequency domain using DCT/DWT/FFT and embedded in a special manner, whereas the components of cell II of cover image are being retained in spatial domain itself. Embedding Process, based on, the four MSB bits of each pixel in the payload cell 1 and cell 2 are embedded in the second and fourth LSB positions of cover image cell I and cell II respectively to increase the security of the payload and generate stego image in transform domain.

Singh & Siddiqui (2012) proposed a new robust steganography algorithm based on DCT, Arnold transform and chaotic system. The chaotic system is used to generate a random sequence to be used for spreading data in the middle frequency band DCT coefficient of the cover image. The security is further enhanced by scrambling the secret image using Arnold Cat map before embedding.

Bhattacharya et al (2012) proposed Steganographic technique for hiding multiple images in a color image based on DWT and DCT. The cover image is decomposed into four sub-bands using DWT. DCT is applied in each HH band separately to get corresponding DCT coefficients. Secret binary images are dispersed among the selected DCT coefficients using a pseudo random sequence and a Session key.

Hemalatha et al (2013) provide a novel image steganography technique to hide both image and key in color cover image using DWT and Integer Wavelet Transform (IWT). The cover is 256x256 color image. The secret information is grey scale image of size 128 x128. To transfer the secret image confidentially, the secret image

itself is not hidden, instead a key is generated and then the key is encrypted

Naoum, et al. (2013) proposed hiding color images in another color images. It uses the transform domain technique in the steganography process to increase its robustness against the changes and treatments done for the cover image. In this work, DCT applying smart block matching method between the embedded image and cover image to find locations to hide information blocks. The use of block matching in the DCT method implies some restriction and difficulties although it offers a great opportunity to retain the embedded information blocks.

Parul et al (2014) presented a new approach for image steganography using DWT and Arnold transformation is used to improve security. DWT is applied on color cover images are divided into higher and lower frequency sub-bands. Secret images are transformed using Arnold transformation (chaotic map). Embed the secrete images components into higher frequency sub band.

Naoum, et al (2014) suggested to hide a color image inside another larger color image. The research aims to use transformation domain methods to deal with complexity, security and robustness. The proposed Steganography scheme uses a DWT method to provide better imperceptibility, in harmony with the human visual system, and with higher robustness against signal processing attacks. The DWT method is implemented for storing the embedded image in the cover image, while finding locations to hide information is realized on using a threshold method.

Nitin, et al (2014) present a novel image steganography method that is based on LSB and DCT coefficients that provide randomized bits embedding inside the cover image. Firstly the DCT apply on the cover image and then hiding the secret image in LSB of the cover image in random locations based on threshold value.

Vijay & Vignesh (2014) proposed work, Integer "Wavelet Transform (IWT)" is performed on a gray level cover image and in turn embeds the secret image bit stream into the LSB's of the integer wavelet coefficients of a the image . The main purpose of the proposed work is to focus on improving embedding capacity and bring down the distortion occurring to the stego image.

4. Research Method

The proposed system consists of two main phases: the embedding phase and extraction phase. In the embedding phase, the combination of (ERBP) and (DWT) algorithms take the secret image and the cover image as inputs, and the stego image will be created, whereas, in the extraction phase, the stego image will be decomposed to extract the secret image once again.

4.1 Embedding Phase

The embedding phase is proceeded by three main stages: best cover image selection and processing stage, secret image selection and processing stage and best embedding threshold selection stage.

4.1.1 Best Cover Image Selection and Processing Stage

The selection of the best cover image that will be used to hide the secret image will be conducted using hybrid system built upon two different types of artificial neural networks, the first is SOM neural network which is an unsupervised artificial neural network, and the second network, is the enhanced resilient back propagation neural network, SOM will be trained to obtain the desired outputs of the enhanced resilient back propagation neural network. The histograms of all the cover images database is obtained first, then they are used as inputs for the SOM neural network. SOM will categorize the histograms into pre-defined classes, ([1 0 0 0], [0 1 0 0], [0 0 1 0], [0 0 0 1]), these classes will be used as desired outputs of the enhanced resilient back propagation, whereas the histograms will be used as training patterns. The resilient back propagation neural network can be enhanced to achieve less "Minimum Square Error (MSE)" in less number of iterations by adding a learning parameter ξ that affects the speed of convergence. This parameter and its impact is proved by (NAOUM, et al., 2012). And can be explained as following.

The general learning rule formula is identified as.

$$w^{(m+1)} = w^m + \xi(t^m - d^m)z^m \dots\dots\dots (1)$$

Where;

$w^{(m+1)}$ is the new weight,

w^m is the previous weight,

ξ is a positive learning parameter, t^m is the target (desired)output.

d^m is the neural output and finally z^m is a training pattern.

The optimal factor w^* which is the correct weight solution will be used to improve the convergence speed where the neural network will settle in the global minima instead the local. Using the above equation w^* is subtracted at both sides of the equation. Adding the parameter ξ in the weight update equation as illustrated below;

$$w_{ij}(t+1) = w_{ij}(t) + \xi \Delta w_{ij}(t) \dots . (2)$$

where $0 < \xi < 1$

In order to find the optimal value of ξ, we use the trial and error approach, however, a local searching algorithm may be used, Using (ξ) (NAOUM, 2011). The pseudo code for the enhanced resilient back-propagation becomes (RIEDMILLER and BRAUN, 1993):

$For\ all\ weights\ and\ biases\{$
$if\left(\frac{\partial E}{\partial w}(m-1) * \frac{\partial E}{\partial w}(m) > 0\right) then\ \{$
$\Delta(m) = minimum(\Delta(m-1) * \eta^{+}, \Delta_{\max})$
$\Delta w(m) = -sign\left(\frac{\partial E}{\partial w}(m)\right) * \Delta(m)$
$w(m+1) = w(m) + \xi \Delta w(m)$
$\}$
$else\ if\ \left(\frac{\partial E}{\partial w}(m-1) * \frac{\partial E}{\partial w}(m) < 0\right) then\ \{$
$\Delta(m) = maximum(\Delta(m-1) * \eta^{-}, \Delta_{\min})$
$w(m+1) = w(m) - \xi \Delta w(m-1)$
$\frac{\partial E}{\partial w}(m) = 0$
$\}$
$else\ if\ \left(\frac{\partial E}{\partial w}(m-1) * \frac{\partial E}{\partial w}(m) = 0\right)\ then\ \{$
$\Delta w(m) = -sign\left(\frac{\partial E}{\partial w}(m)\right) * \Delta(m)$
$w(m+1) = w(m) + \xi \Delta w(m)$
$\}$
$\}$

Learning parameter ξ is used in (ERBP) training for both: (ERBP) training to get best cover image, and (ERBP) training to get the best embedding threshold. In the former one, the enhanced resilient back propagation neural network (ERBP) is trained to choose best cover image, where the network is first built without using ξ (i.e. set ξ =1 in equation $w(m+1) = w(m) + \xi \Delta w(m)$) with initial weights set to : -0.5 ≤ weights ≤ 0.5 and MSE = 0.0733 on average is obtained. Then (ξ) parameter is set a value between 0 and 1 ($0 < \xi < 1$) in the equation ($w(m+1) = w(m) + \xi \Delta w(m)$), where an optimal value of ξ = 0.6 is obtained in case of the enhanced resilient back propagation neural network that used to choose the best cover image, and optimal ξ = 0.7 in case of the enhanced resilient back propagation neural networks that used to choose the best embedding thresholds for each color layer (rT, gT ,bT), and for both cases, a better average MSE is gotten.

After the best cover image is chosen by the trained enhanced resilient back propagation neural network, then it will be divided into its (R,G,B) layers, After the cover image and secret image has been divided into three color layers (R,G,B) then the next step is to apply 4 level-Discrete Wavelet Transform separately to each color layer. Each channel (R,G,B) of cover-image will be decomposed into four levels and each level with various multi-resolution sub bands (Approximate, Horizontal ,Vertical and Diagonal), using Haar function as mother wavelet. The aim of decomposition is to separate the low frequency components, which has the most energy of the image (Approximation), from high frequency components (Details).

4.1.2 Secret Image Selection and Processing Stage

In this stage, the secret image is chosen manually and then processed to get the encrypted bit streams that will be embedded in the cover image. The first step of secret image processing is to separate it into (Red, Green ,Blue) color layers. Discrete wavelet transform of first level is applied to each color layer of secret image. After the DWT is applied to each color layer of secret image then each color layer will be processed separately. Color layer sub bands will converted to bit streams, and that will yield four bit-streams (bit stream for each sub band) where each coefficient is transformed into 16 bits and the bits of all coefficients of a sub band are concatenated to compose the whole bit stream. Once the bit stream of each sub band is available, the encryption step starts. The encryption will cipher the bit stream using key produced by modified "Fibonacci Linear Feedback Shift Register (FLFSR)" (GORESKY and KLAPPER, 2002). The modified FLFSR model is illustrated below in the following figure.

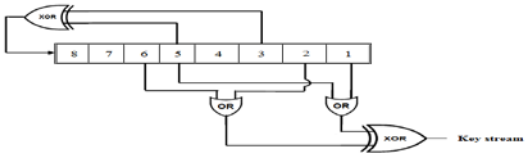

Fig. 2 An 8-bit Modified Fibonacci Linear Feedback Shift Register.

Initial state of the register is set using the first pixel of each color layer, and this 8-bits pixel is considered the seed value of the register, where a separate seed is used for each color layer, so there is a separate encryption key for each color layer and this increases the security level of our proposed system. Then the operation of shifting each time produces new bit key. The key bits are generated key bits as much as needed to form a stream of ciphering key matches in length of sub band bit stream.

4.1.3 Best Embedding Threshold Selection Stage

In this stage of pre-embedding phase, the best embedding threshold parameter (T) is selected using the enhanced resilient back prorogation neural network once again. This parameter is considered the reference level that determines the availability to use the coefficients of sub bands in

cover image to hide sub band bit streams coming from the secret image without loss of information in the extraction process. The embedding threshold determines the size (the space) of the redundancy in the best cover image coefficients that can be used to embed the secret image. And this embedding threshold can be obtained analytically by using statistical equation (3)

$$T = \frac{\alpha}{N}\sum_{i=0}^{N}\left|C_i\right| \tag{3}$$

But our proposed embedding and extraction algorithm depend on using same threshold value in both embedding and extraction stages without using further locations in the DWT coefficients to store the indices of the locations that used to store the bit streams of secret image sub bands. It is proposed to use the learning power of the enhanced resilient back-propagation neural network to approximate the appropriate best threshold parameter that suits our proposed embedding algorithm without returning to equation 5.1 and without playing in (α) value. Our resilient back-propagation neural network was trained using the Normalized DWT coefficients as inputs and the best threshold value as the desired output for each layer of the cover image, the best threshold value (T) is determined after multiple of trials and errors to determine the best threshold for each cover image of database contains (100) cover images, and MSE down to (1.4525x10-4) in (100) epochs of training is obtained. Once the results coming out of pre-embedding stages being ready, then the embedding phase can take place. In this phase, the bit stream of each sub band in the secret image will be embedded in the (DWT) coefficients of the cover image such that, the coefficients of one layer are embedded in the secret image in the corresponding layer in the cover image and the bit stream of one sub band in the secret image will be embedded in the corresponding sub band in the cover image. Now, the coefficients of each sub band in the cover image are converted to a vector that composed of the coefficients coming out of all levels and in a concatenated way. Each coefficient is compared with the embedding threshold (T). if it is greater than threshold, then it is neglected and it will not be involved in the embedding process, however if the value of the coefficient is less than or equal to the embedding threshold (T), then the coefficients is converted to 16 bits binary number and then the least four significant bits (LSB) `of this binary number are used to store four bits block coming out the bit stream of secret image. After the substitution is done, the coefficient that used in embedding is transferred to its float value once again. After the whole bit stream of secret image sub bands is embedded in the available coefficients that lies under threshold of cover image then "Inverse Discrete Wavelet Transform (IDWT)" is applied.

However, our proposed embedding model have a drawback from the elapsed time perspective, where the training process of three neural networks used to get the best embedding threshold for each color layer, leads to massive time and computational power consumption, which force us to use the statistical equation 3 to calculate the embedding threshold instead of training scarified three neural networks, although the accuracy and the smartness yielded by using the neural networks at the same time, the using of Equation (3) keeps the objective tests values (PSNR and MSE) at satisfying levels.

4.2 Extraction Phase

The first step of extraction process is to separate the stego image into its color layers (R,G,B) and then each color layer will be processed separately to get the color layers of secret image, then these color layers will be combined together to get the full (RGB) recovered secret image and this is considered the first security layer of our proposed system. Then each color layer of stego image is decomposed into 4 level/ DWT to get the stego image sub bands that hide the secret image bit streams. Starting with the approximate sub band, where the secret key which consists of embedding threshold is extracted; seed value and secret image size that are embedded in the first three coefficients of approximate sub band coefficients vector.
Each coefficient is compared with the extracted embedding threshold; if the coefficient is greater than the threshold, ignore it. If it is less or equal to threshold then convert it to binary number and extract the 4 Least Significant Bits. This process is repeated this process for each coefficient less or equal to the threshold until the whole bit stream of secret sub bands is extracted. Now, the same operation is performed for the other sub bands where each sub band bit streams of secret image is hidden in its corresponding sub bands of the cover image and this add another security level to our proposed system. Now, there are 4 encrypted bit streams of the secret image sub bands and need to be decrypted. The decryption is performed in the same steps mentioned above in the embedding phase. Hiding the encrypted bit streams of the secret image is considered another security layer for our proposed system. Once the encrypted bit streams is gotten the decrypted, then it will be divided to 16-bits blocks and they are converted back to vectors of float numbers .One level IDWT is applied to get one color layer of the recovered secret image and then apply the same procedure above to get the other layers. Finally, the color layers are combined together to get the full color (RGB) secret image. The proposed scheme flow chart is illustrated below followed by the selected secret images and the corresponding best covers images chosen by (ERBP).

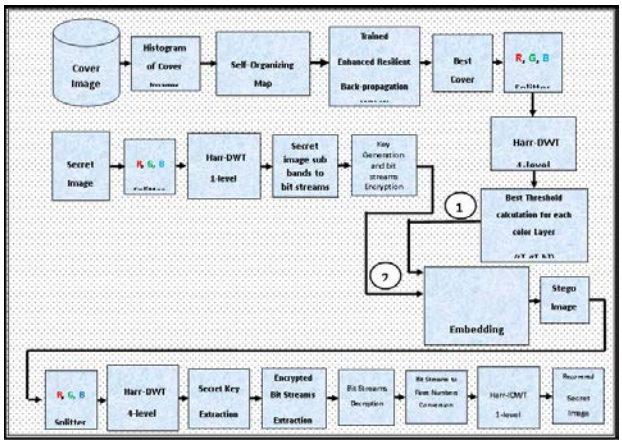

Fig. 4 Proposed Stenography Scheme.

5. The Results and the Discussions

The proposed system is tested with different cover images and secret images. Both, the secret image and the cover image are in the '.jpg' format. MatLab 2012a running on a Windows 7 platform was used to implement the proposed steganography scheme. The best cover image that will be used in the embedding process was selected using (ERBP), trained using a database composed of (305) full color (RGB) images. Figure 3 shows the set of selected secret image and the corresponding best cover images selected by the (ERBP). The proposed system hide two sets of cover and secret images: first set hide full color (64x64) secret images inside full color (256x256) cover images and the other set hide full color (128x128) secret images inside full color (512x512) cover ima

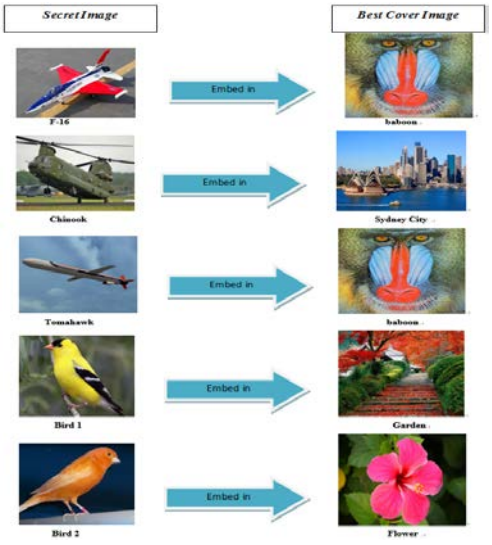

Fig. 5 the selected secret images and the corresponding best covers images chosen by (ERBP)

As a case study; the results of 64x64 secret images in 256x256 cover image will now be introduced and investigated. The first part of the results is the MSE and PSNR for stego and cover images during the embedding stage as tabulated in tables 1.

Table 1: PSNR and MSE for (64x64 secret image in 256x256 cover image) during the embedding stage

Secret-image (64X64)	Best cover-image (256X256)	Stego-image	PSNR/dB	MSE
F-16	Baboon	Baboon + F-16	105.6812	2.5723e-05
Chinook	Sydney City	Sydney City + Chinook	105.7266	2.5607e-05
Tomahawk	Baboon	Baboon + Tomahawk	104.9983	2.7541e-05
Bird 1	Garden	Garden + Bird	103.0899	3.3332e-05
Bird 2	Flower	Flower + Bird 2	121.1390	5.4828e-06

To highlight the important characteristics of our proposed system, a histograms comparison between the resulted stego image and the cover image is presented now. The histogram test shows that the modified image (stego image) is not affected by the hidden image. The histogram of the cover image is approximately the same as the histogram of stego image as shown in the Figures below that illustrates Hiding (bird 2 of 64x64) secret image inside (flower of 256x256) cover image.

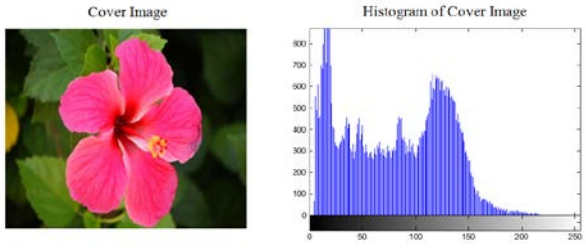

Fig. 6 cover image with histogram

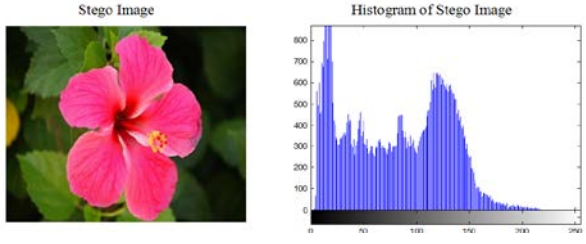

Fig. 7 stego image with histogram.

Figure 8, and 9 show hiding (tomahawk) secret image inside (Baboon) cover image example.

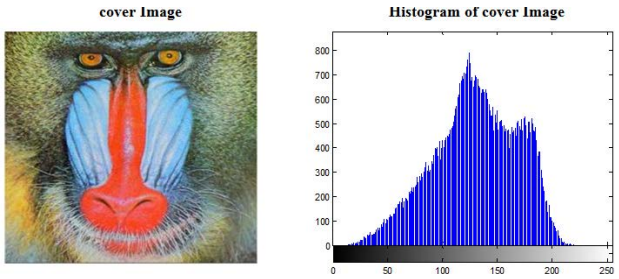

Fig. 8 Cover image with histogram

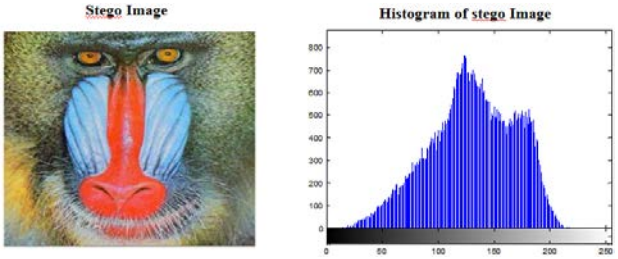

Fig. 9 Stego image with histogram

The MSE and PSNR were also evaluated during the extraction stage for original secret and extracted secret image as tabulated in table 2.

Table 2: PSNR and MSE for (64x64 secret image in 256x256 cover image) during the extraction stage

Stego-image (256x256)	Original Secret-image (64X64)	Recovered secret image (64X64)	PSNR (dB)	MSE
Baboon + F-16	F-16	F-16	88.3651	1.4533e-04
Sydney City + Chinook	Chinook	Chinook	86.6446	1.6724e-04
Baboon + Tomahawk	Tomahawk	Tomahawk	80.6842	2.1858e-04
Garden + Bird 1	Bird 1	Bird 1	92.5407	9.5721e-05
Flower + Bird 2	Bird 2	Bird 2	92.6455	8.8155e-05

The histogram test is also applied to the secret image and recovered secret image. In the extraction stage, the experimental results show that the recovered secret image has almost the same histogram of the original secret image. The following figures illustrate the results of extracting (bird 2 of 64x64) secret image out of (flower of 256x256) stego image.

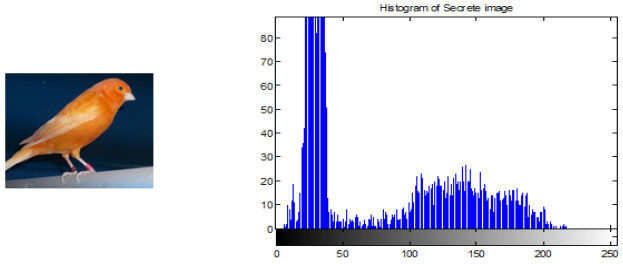

Fig. 10 original secret image with histogram

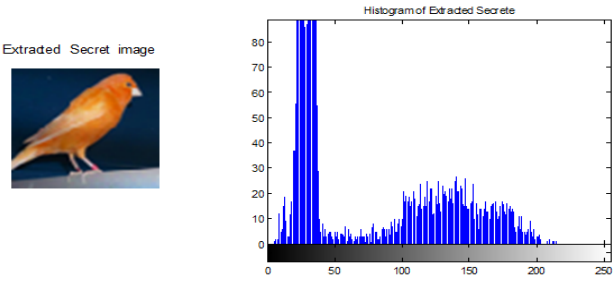

Fig. 11 extracted secret image with histogram.

The following figures illustrate the results of extracting (tomahawk 2 of 64x64) secret image out of (baboon of 256x256) stego image.

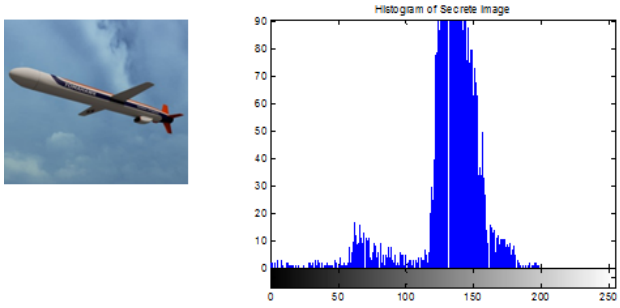

Fig. 12 original secret image with histogram

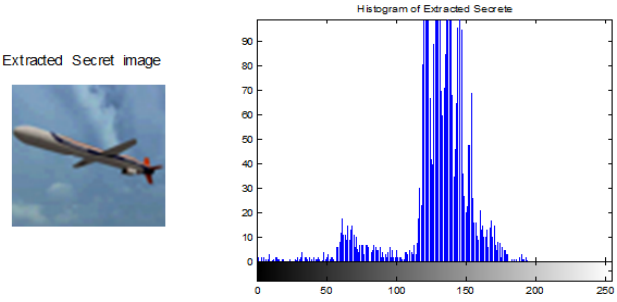

Fig. 13 extracted secret image with histogram.

Table 3 depicts the comparison of PSNR and processing time between proposed model and the modified proposed model.

Table 3 PSNR and Processing time of models (proposed and modified)

Case No.	Secret image	Cover image	PSNR (dB) of Original proposed model	PSNR (dB) of Modified proposed model	Processing time of Original proposed model (minutes)	Processing time of Modified Proposed model (minutes)
Case 1	Bird 2 (64x64)	Flower (256x256)	120.6047	121.1390	12.340	2.373
Case 2	Chinook (100x100)	Sydney City (256x256)	96.6450	97.3686	14.180	4.588
Case 3	Tomahawk (128x128)	Baboon (256x256)	97.3193	98.1081	17.662	7.688
Case 4	Bird 1 (128x128)	Garden (512x512)	118.6205	119.2987	50.623	8.157
Case 5	F-16 (150x150)	Baboon (512x512)	122.2557	122.4483	54.921	11.266

As shown in table 3; the performance of the modified proposed model is enhanced due to using equation 3 to calculate the value of the embedding thresholds rather than using the training process of the three NNs. The performance is measured in terms of the PSNR and processing time; it is clear that the maximum value of PSNR equals to 122.2557dB and 54.921minutes respectively and these two values are improved in the modified model to be 122.4483dB and 11.266minutes. These values are very good considering the system complexity.

6. Summary and Concluding Remarks

To conclude all; a novel steganography model that combine between both DWT and ERBP algorithms. Two main stages are included during the steganography process, which are; embedding and extraction stages. The system implemented using MATLAB software and the performance evaluated in terms of MSE and PSNR criteria in addition to histogram test for both embedding and extraction stages. The result ensured the effectiveness of the proposed scheme in terms of high values PSNR and very low value of MSE. The following are the conclusion remarks regarding to the proposed scheme performance;

The selection of the best cover image using the hybrid artificial neural network (SOM and ERBP) played an important role in improving the overall system performance.

Splitting the secret and cover image into (R, G, B) color layers and different level DWT decomposition led to high perceptual quality in both embedding and extraction phases.

The proposed system hides the secret image in the cover image based on Haar-DWT provides good extracted secret image quality which led to increase the imperceptibility of the system. However, other types of filters to can be used to improve quality of the extracted images.

The approximate and details sub bands in the proposed steganographic technique are used to hide the bit streams of secret image depending on embedding threshold (T) resulted in high embedding capacity. The capacity is about (1/4) of the cover image in worse cases.

Transforming the sub bands of secret image into bits streams and hiding it in the least significant bits of the DWT coefficients of cover image resulted in high PSNR and smaller MSE in both embedding and extraction phases.

The proposed combination between steganography and cryptography improved the security layers of our work to competitive levels in compared with existing modern steganographic systems. So it is difficult to know the original hidden image since it is encrypted before embedded.

Despite of the computational complexity of this system, it is suitable for real time applications because the run time is acceptable (elapsed time =11.266 Minute) in worst cases.

References

[1] Petitcolas, F. A., Anderson, R. J. and Kuhn, M. G. 1999. “Information Hiding- A Survey,” Proceedings of the IEEE, 87(7), pp. 1062-1078.

[2] Johnson, N. F., Duric, Z. and Jajodia, S. 2001. “Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures,” Kluwer Academic Publishers, USA, Springer, 1.

[3] Jalab, H. A., Zaidan, A. A., & Zaidan, B. B. 2010. “New Design for Information Hiding with in Steganography Using Distortion Techniques,” International Journal of Engineering and Technology (IJET)), ISSN, 8236, 2 (1). PP.72-77.

[4] Geetha, K. and Muthu, P. V. 2010. “ Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure

Secrecy," International Journal on Computer Science and Engineering, 2(4), pp. 1308-1313.
[5] Kumar, S. and Multoo, S. 2011. "Steganography based on contourlet Transform," International Journal of Computer Science and Information Security (IJCSIS), 9 (6), PP. 215-220.
[6] Kumar, K. S., Raja, K. B., Chhotaray, R. K., and Pattnaik, S. 2011. "Performance comparison of robust steganography based on multiple transformation techniques," International Journal of Computer Technology and Applications, 2 (4). Pp.1035-1047.
[7] Kumar, K. S., Raja, K. B., & Pattnaik, S. 2011. "Hybrid domain in LSB steganography," International Journal of Computer Applications. 19 (7). Pp. 35-40.
[8] Kumar, K. S., Raja, K. B., Chhotaray, R. K. and Pattnaik, S. 2011. "Performance comparison of robust steganography based on multiple transformation techniques," International Journal of Computer Technology and Applications, 2 (4). PP. 1035-1047.
[9] Mandal, J. K. 2011. "A Frequency Domain Steganography using Z Transform (FDSZT)," International Workshop on Embedded Computing and Communication System (IWECC 2011), pp.1-4.
[10] Singh, S. and Siddiqui, T. J. 2012. " A security enhanced robust steganography algorithm for data hiding," International Journal of Computer Science Issues (IJCSI), 9 (3). PP 131-139.
[11] Bhattacharya, T., Dey, N. and Chaudhuri, S. R. 2012. "A session based multiple image hiding technique using DWT and DCT," International Journal of Computer Applications, 38(5). pp. 18– 21.
[12] Hemalatha, S., Acharya, D. U., Renuka, A. and Kamath, P. R. 2013. "A Secure Color Image Steganography in Transform Domain," International Journal on Cryptography and Information Security, 3 (1). PP. 17-24.
[13] Naoum, R., Viktorov, O., Shihab, A., and Shaker, M. 2013. "Image-to-mage Steganography Based on Discrete Cosine Transform," European Journal of Scientific Research, 106 (4), PP. 512-522.
[14] Naoum, R. 2011. "Lecture Notes, Artificial Neural Network," Middle East University (MEU), Jordan.
[15] Naoum, R. S., Abid, N. A., & Al-Sultani, Z. N. 2012. "An Enhanced Resilient Backpropagation Artificial Neural Network for Intrusion Detection System," International Journal of Computer Science and Network Security IJCSNS, 12(3).
[16] Goresky, M., and Klapper, A. M. 2002. "Fibonacci and Galois representations of feedback-with-carry shift registers. Information Theory," IEEE Transactions on, 48(11), PP. 2826-2836.
[17] Parul, M., and Rohil, H. 2014. "Optimized Image Steganography using Discrete Wavelet Transform (DWT)," International Journal of Recent Development in Engineering and Technology (IJRDET), 2 (2). PP 75-81.
[18] Naoum, R., Shaker, M., Mudhafar.J., and Ahmed. S. 2014. "Discrete Wavelet Transform for Image-to-Image Steganography," European Journal of Scientific Research, Vol. 117, (1). pp 137-152.
[19] Nitin, K., kirit, R., Avalik, R., Vijaysinh, J. and Ashish, N. 2014. "A Novel Technique for Image Steganography Techniques Based on LSB and DCT Coefficients," International Journal for Scientific Research and Development (IJSRD), Vol. 1 (11). PP 2479-2482.
[20] Vijay, M., & Vignesh, V. 2014. "Image Steganography Method Using Integer Wavelet Transform," International Journal of Innovative Research in Science, Engineering and Technology, IEEE International Conference on Innovations in Engineering and Technology (ICIET'14). Vol. 3 (3), PP. 1207-1211.
[21] Riedmiller, M., and Braun, H. 1993. "A direct adaptive method for faster backpropagation learning: The RPROP algorithm. In Neural Networks," IEEE International Conference, PP. 586-591.
[22] Stamp, M. (2006). Information Security Principles And Practice. New Jersey.