



A novel Image Steganography System based on Hybrid Artificial Neural network with Haar-Discrete Wavelet Transform

KEYWORDS

Steganography, Neural Networks (NNs), Enhanced Resilient Back-Propagation (ERBP), Self Organizing Mapping (SOM), Discrete Wavelet Transformation (DWT), "Fibonacci Linear Feedback Shift Register (FLFSR)", Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Red Threshold (rT), Green threshold (gT), Blue Threshold (bT).

Prof. Reyadh Naoum

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

Ahmed Shihab

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

Dr. Sadeq AlHamouz

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

ABSTRACT *Steganography was emerged as a common process for hiding data that are needed to be exchanges between two communication parties within several critical applications; especially security ones. A new steganography scheme is introduced in this paper. An (RGB) secret image is embedded into (RGB) cover image. Enhanced resilient back propagation neural network and Self Organizing Mapping were employed to select the best cover image compatible with the secret image. Two main phases are included within the proposed steganography scheme; the embedding and extraction phases. The secret image is firstly separated into (Red, Green, and Blue) color layers; each layer is then processed by applying DWT. The color layers are then converted to bit streams; these bit streams are encrypted using modified FLFSR to increase the security level of the proposed system. The threshold values during the embedding and extraction phases were selected employing ERBP algorithm. The results ensured the effectiveness of the proposed steganography scheme in terms of low MSE and high PSNR in comparison with the steganography systems introduced and implemented in the literature.*

1. Introduction

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data. The word steganography, as derived from Greek, literally means covered or hidden writing and includes a vast array of methods of secret communications that conceal the very existence of the message. Though steganography is an ancient craft, the onset of computer technology has given it new life. Computer-based steganographic techniques introduce changes to digital covers to embed information foreign to the native covers. Such information may be communicated in the form of text, binary files, or provide additional information about the cover (JOHNSON et al, 2001).

Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of that message being detected. If the message is also encrypted, then it provides another layer of security (TAQA et al., 2009). Therefore, some steganographic methods combine traditional cryptography with steganography; the sender encrypts the secret message prior to the embedding process. Such a combination increases the security of the overall communication process, as it is more difficult for an attacker to detect embedded ciphertext in a cover (KATZENBISSER and PETITCOLAS, 2000).

Steganographic techniques embed a message inside a cover. Various features characterize the strengths and weaknesses of the methods. The relative importance of each feature depends on the application; these features are introduced below;

A. Capacity

The notion of capacity in data hiding indicates the total number of bits hidden and successfully recovered by the steganographic system (VIJAYAKUMAR, 2011).

B. Robustness

Robustness refers to the ability of the embedded data to remain intact if the stego-image undergoes transformation, such as linear and non-linear filtering; addition of random noise, scaling, rotations and loss compression (YADAV et al., 2011).

C. Undetectability

The embedded information is undetectable if the image with the embedded message is consistent with the model of the source from which the cover images are drawn. For example, if a steganographic method uses the noise component of digital images to embed a secret message, it should do so while not making statistically significant changes to the noise in the carrier. Undetectability is directly influenced by the size of the secret message and the format of the content of the cover image (RAFIQUL, et al., 2009).

D. Security

It is said that the embedded algorithm is secure if the embedded information is not subject to removal after being discovered by the attacker and it depends on the total information about the embedded algorithm and secret key (VIJAYAKUMAR, 2011).

E. Invisibility (Perceptual Transparency)

This concept is based on the properties of the human visual system or the human audio system. The embedded information is imperceptible if an average human subject is unable to distinguish between carriers that do contain hidden information and those that do not. It is important that the embedding occurs without a significant degradation or loss of perceptual quality of the cover (RAFIQUL et al., 2009).

Steganography encompasses methods of transmitting secret messages in such a manner that the existence of the embedded message is undetectable. Carriers of such mes-

sage may resemble innocent sounding text, disks, network traffic, and protocols, the way software or circuits are arranged, audio, images, video, or any others digitally represent code or transmission. These provide excellent carriers for hidden information and many different techniques have been introduced (JOHNSON et al, 2001).

There are many different methods for hiding information in images. In images, we can modify properties such as contrast, colors or luminance to hide secret messages. Proposed methods hide data in images with virtually no impact to the human sensor system. When considering an image in which to hide information, one must consider the structure of the image as well as the palette. The most popular method to hide information in the image is least significant bit (LSB) insertion or manipulation. This is a common, simple approach to embedding data in a cover. Unfortunately, this approach is vulnerable to even a light image distortion. When we want to hide an image in the LSBs of each byte of a 24-bit image, we can store 3 bits in each pixel. To the human eye, the resulting stego-image will look identical to the cover image (PEJAS and PIEGAT, 2006).

2. Research Scope

The aim from this paper is to introduce and implement a new steganography system that mainly depends in two main algorithms, which are; ERBP and DWT algorithms. The paper will consider hiding color secret images into another color cover 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 (Caesar 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.

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.

Ghaleb et al. (2012) proposed a new approach of image steganography that conceals a gray scale secret image into colored (BMP) image. This approach has two stages, in the first stage they compress the secret image using artificial neural network technique (Back-propagation algorithm) and in the second phase, they hide the secret image using the Least Significant bit substitution method.

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.

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.

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.

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.

Nain & Bansal (2014) suggests merging text into color cover image based on Block-DCT vector quantization method, where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain. Here the artificial neural network will help to find pixels to merge the data bits without much affecting the original pattern. A technique based on Least Significant Bits replacement considering DCT coefficient value of pixels.

Naoum, et al (2015) 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 in-

cludes 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.

4. Research Method

The methodology that will be applied during this paper can be summarized as illustrated below in the following figure.

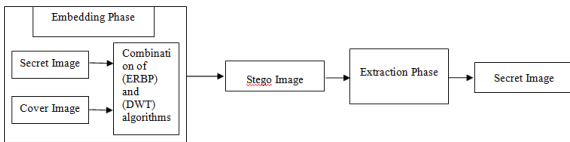


Figure 1: The main idea for the proposed steganography scheme.

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.

A. 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 were proved by (NAOUM, et al., 2012). This stage is illustrated in figure below.

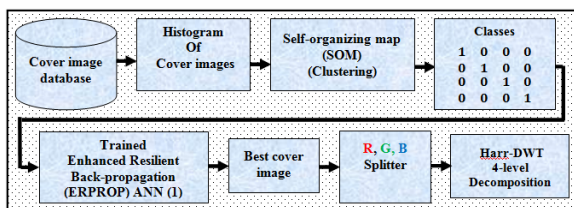


Figure 2: Best cover image selection and processing using hybrid of (SOM) and (ERPROP)

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 $\xi = 1$ in equation) with initial weights set to : $-0.5 \leq \text{weights} \leq 0.5$ and $\text{MSE} = 0.0733$ on average is obtained. Then (ξ) parameter is set a value between 0 and 1 ($0 < \xi < 1$) in the equation, where an optimal value of $\xi = 0.6$ is ob-

tained in case of the enhanced resilient back propagation neural network that used to choose the best cover image, and optimal $\xi = 0.7$ 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).

B. 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. Figure 3 demonstrates the bit stream conversion of sub bands coefficients of the red layer and this approach applied for the rest layers. As another case study, it is possible to convert the coefficients to 24 bits instead of 16-bits and it gives better PSNR values, however it consumes much time and computational power especially in extraction process.

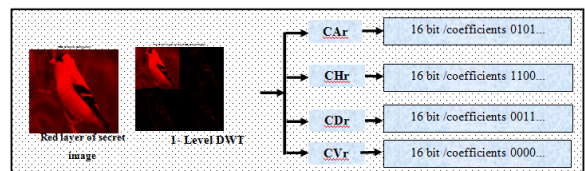


Figure 3: Bit stream conversion of secret image coefficient of red layer

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). 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.

C. 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 propagation 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. 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. 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 (1.4525×10^{-4}) in (100) epochs of training is obtained. Figure 4 demonstrates the best embedding threshold selection stage.

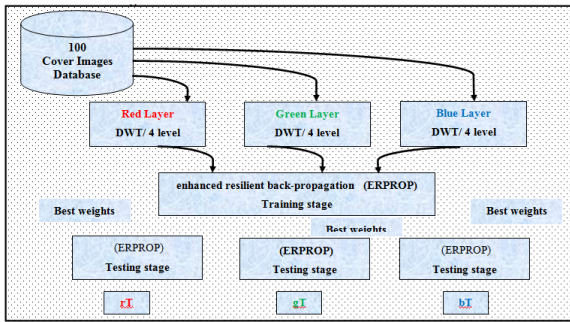


Figure 4: Enhanced resilient back propagation training process to select best embedding threshold

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.

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 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).

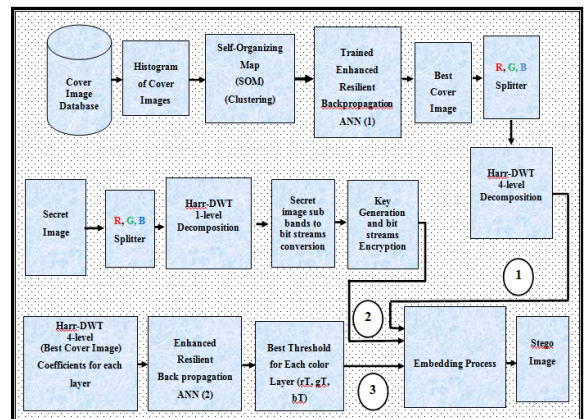


Figure 5: Proposed steganography scheme flow chart.

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. Mat-Lab 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 three cases of cover and secret images: first case hides full color (100x100) secret images inside full color (256x256)

cover images, second case hides full color (128x128) secret images inside full color (512x512) cover images and finally the third case hides full color (150x150) secret images inside full color (512x512) cover images. The following figure illustrates both the secret and the best cover images that were used during the system implementation and evaluation.

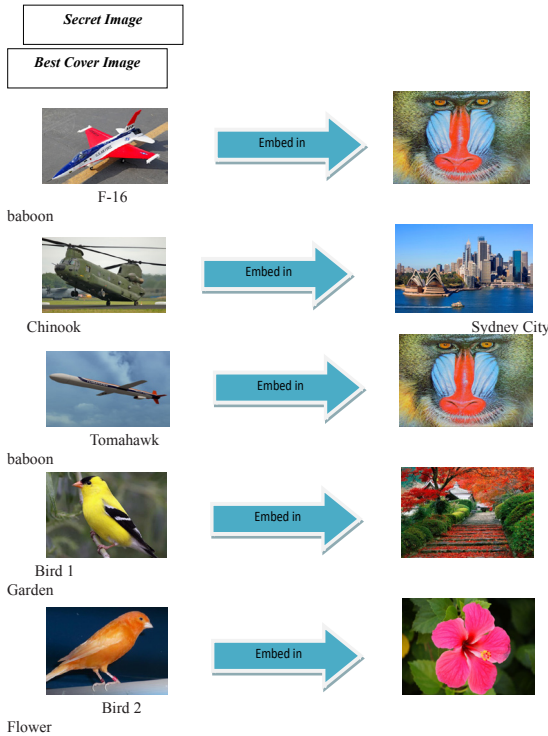


Figure 6: The selected secret images and the corresponding best covers images chosen by (ERBP)

The results of hiding (150x150) secret image inside (512x512) cover image will now be introduced and investigated as an example to evaluate the performance of the proposed scheme. 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 hiding (150x150) secret image inside (512x512) cover image during the embedding stage

Secret-image (150x150)	Cover-image (512x512)	Stego-image	PSNR/dB	MSE
F-16	Baboon	Baboon + F-16	120.5261	5.8293e-06
Chinook	Sydney City	Sydney City + Chinook	121.8677	5.0974e-06
Tomahawk	Baboon	Baboon + Tomahawk	119.4119	6.5164e-06

Bird 1	Garden	Garden + Bird	115.1675	9.9618e-06
Bird 2	Flower	Flower + Bird 2	133.3082	1.6237e-06

Furthermore; the histogram for the cover and the stego images were also obtained and compared in order to ensure that the steganography process does not affect the histogram characteristics of the cover images. The following figures illustrate an example for the histogram results for each one of the three cases considering for different images for the both cover and stego images before and after hiding the secret image best cover image.

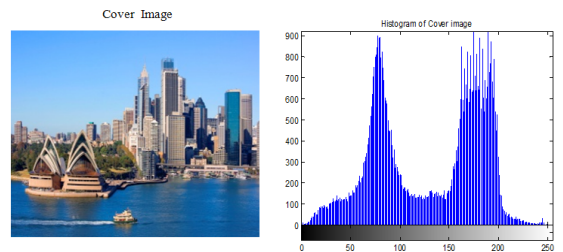


Figure 7: Sydney City cover image with its histogram for the first case.

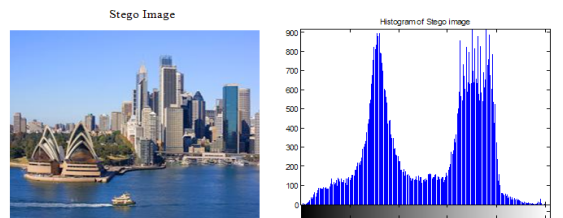


Figure 8: Sydney City stego image with its histogram for the first case.

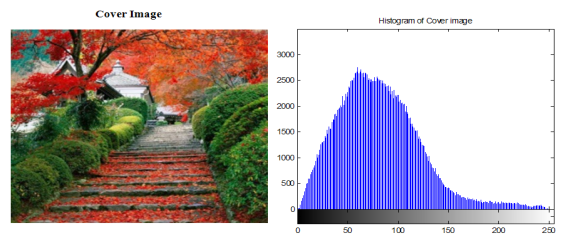


Figure 9: Garden cover image with its histogram for second case.

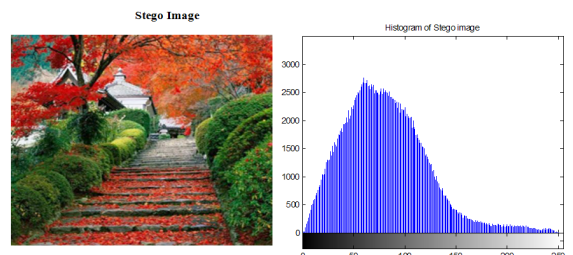


Figure 10: Garden stego image with its histogram for second case.

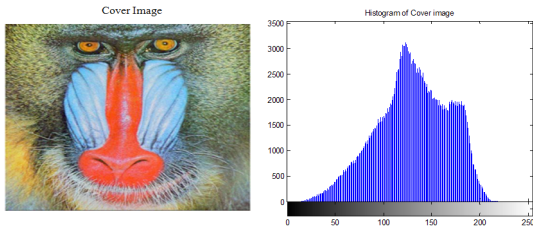


Figure 11: Baboon cover image with its histogram for third case.

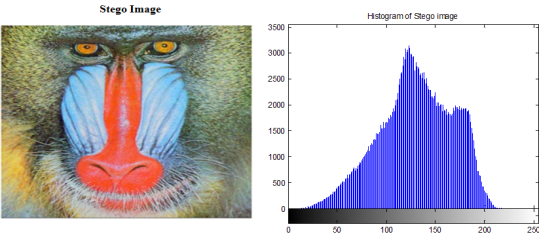


Figure 12: Baboon stego image with its histogram for third case.

As shown; the stego image and the cover image have identical histogram characteristics, which in turns confirmed the effectiveness of the proposed scheme since if no noticeable change occurred during the embedding phase. The system performance was also evaluated during the extraction phase; the MSE and PSNR for original secret and extracted secret image as tabulated in table 2.

Table 2: PSNR and MSE for hiding (150x150) secret image inside (512x512) cover image during the extraction stage

Stego-image (512x512)	Original Secret-image(150X150)	Recovered secret image (150X150)	PSNR/dB	MSE
baboon + F-16	F-16	F-16	88.2296	1.4731e-04
Sydney City + Chinook	Chinook	Chinook	87.0785	1.6528e-04
baboon + Tomahawk	Tomahawk	Tomahawk	81.3334	2.1261e-04
Garden + Bird 1	Bird 1	Bird 1	92.9127	9.1504e-05
Flower + Bird 2	Bird 2	Bird 2	93.3504	8.6211e-05

Again; the histogram test was also applied during the extraction phase; this was achieved via comparing the histogram for the original secret image and the extracted one. The following figures illustrate the results of extracting the secret images out of stego images.

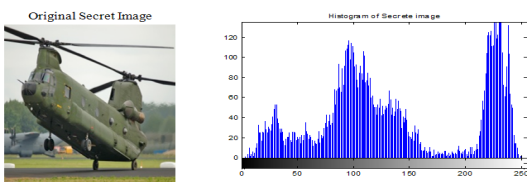


Figure 13: Original Chinook secret image with its histo-

gram for the first case.

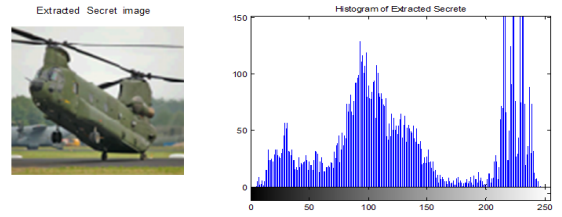


Figure 14: Extracted Chinook secret image with its histogram for the first case.

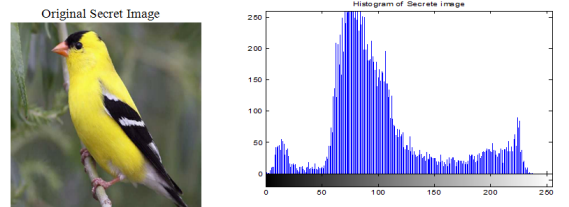


Figure 15: Original Bird1 secret image with its histogram.

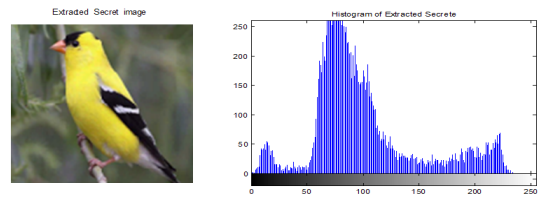


Figure 16: Extracted Bird1 secret image with its histogram.

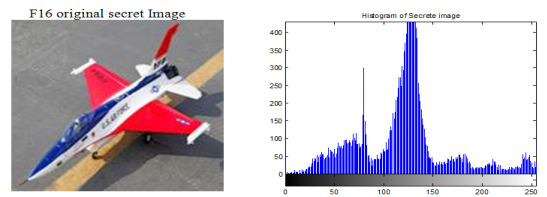


Figure 17: Original F16 image with histogram for the third case.

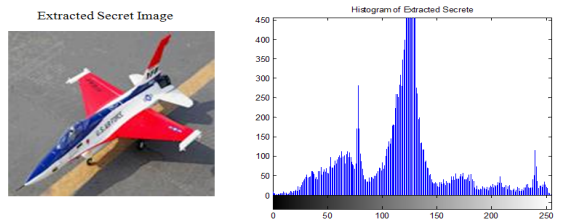


Figure 18: Extracted F16 secret image with histogram for the third case.

6. Comparison our proposed algorithm with other algorithms

To evaluate the performance of our proposed steganography system, several simulations have been performed in order to compare its performance with other existing schemes. Tables 3,4, 5 and 6 illustrate the comparison of PSNR of our proposed method with other methods.

Table 3: PSNR of our proposed method and RDWT method

Method	Secret image	Cover image	PSNR (dB)
Redundant Discrete wavelet transform (RDWT) (Singh & Siddiqui, 2012).	Binary image (64x64)	Gray image (512x512)	39.54
Our Proposed Method	RGB image (64x64)	RGB image (512x512)	135.8903

Table 4: PSNR of our proposed method and DWT method

Method	Secret image	Cover image	PSNR (dB)
Discrete wavelet transform (DWT) (Narasimhalou & Joseph, 2012).	Binary image (128x128)	RGB image (512x512)	33.5325
Our Proposed Method	RGB image (128x128)	RGB image (512x512)	118.7521

Table 5: PSNR of our proposed method and DWT method

Method	Secret image	Cover image	PSNR (dB)
Discrete wavelet transform (DWT) (Naoum, et al., 2014).	RGB image (64x64)	RGB image (256x256)	39.0606
Our Proposed Method	RGB image (64x64)	RGB image (256x256)	101.8378

Table 6: PSNR of our proposed method and DWT method

Method	Secret image	Cover image	PSNR (dB)
Discrete wavelet transform (DWT) (Mahajan & Kranthi , 2014).	Gray image 256x128	Gray image 512x512	75.3945
Our Proposed Method	RGB image 256x256	RGB image 512x512	111.6907

It can be concluded that our proposed method has better results in comparing with other steganographic methods applying to different sizes of cover and secret images.

confirmed through comparing it is results with other steganography schemes that previously introduced in the literature.

7. Summary and Concluding Remarks

As a conclusion; the steganography is now considered essential process in order to hide several type of secret information in other different types, such as; text, audio and images. This paper concentrates on hiding secret images within another cover image. A new steganography scheme was proposed during this research paper. The system includes two main stages; embedding and extraction phases. The cover images are selected carefully employing hybrid artificial neural network (SOM and ERBP). MATLAB software program was used to simulate and evaluate the proposed steganography scheme. 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. Several secret and cover images with different sizes were considered during the evaluation. The PSNR and MSE were used as criteria to estimate the performance. Furthermore; the histogram test was also used to ensure that applying steganography process will not result in any change within the histogram characteristics for the considered images. The effectiveness of the proposed steganography scheme was

REFERENCE

- [1] Johnson, N. F., Duric, Z. and Jajodia, S. 2001. "Information Hiding: Steganography and Watermarking-Attacks and Countermeasures," Kluwer Academic Publishers, USA, Springer, 1. | [2] Katzenbisser, S. and Petitcolas, F. 2000. "Information Hiding Techniques for Steganography and Digital Watermarking," Artech House publisher, Boston, ISBN 1-58053-035-4. | [3] Taqa, A., Zaidan, A. A., & Zaidan, B. B. 2009. "New framework for high secure data hidden in the MPEG using AES encryption algorithm," International Journal of Computer and Electrical Engineering (IJCEE), 1(5), pp. 566-571. | [4] Vijayakumar, M. S. 2011. "Image Steganography based on Polynomial Functions," Journal of Global Research in Computer Science, 2(3). PP. 13-15. | [5] Yadav, R., Saini, R. and Kamaldeep. 2011. "Cyclic Combination Method For Digital Image Steganography With Uniform Distribution Of Message," Advanced Computing: An International Journal (ACIJ), 2 (6). pp. 29-43. | [6] Pejas, J., and Piegat, A. 2006. "Enhanced methods in computer security, biometric and artificial intelligence systems," Kluwer Academic Publishers, Szczecin, Poland, Springer, ISBN 1-4020-7776-9. | [7] Geetha, K. and Muthu, P. V. 2010. "Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy," International Journal of Computer Science and Engineering, 2(4), pp. 1308-1313. | [8] Nain, V. and Bansal, N. 2014. "Performance Upgradation of a Transform Domain based Steganography using Neural Logics," International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014), 2 (1), PP. 150-153. | [9] 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. | [10] Kumar, K. S., Raja, K. B., & Pattnaik, S. 2011. "Hybrid domain in LSB steganography," International Journal of Computer Applications. 19 (7). Pp. 35-40. | [11] 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. | [12] Mandal, J. K. 2011. "A Frequency Domain Steganography using Z Transform (FDSZT)," International Workshop on Embedded Computing and Communication System (IWCECC 2011), pp.1-4. | [13] 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. | [14] 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. | [15] Mahajan, R. & Kranthi, B. 2014. "An Improved Image Steganography Technique Using Discrete Wavelet Transform," International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), 9 (1), PP. 76-82. | [16] Naoum, R., Viktorov, O., Shihab, A., and Shaker, M. 2013. "Image-to-image Steganography Based on Discrete Cosine Transform," European Journal of Scientific Research, 106 (4), PP. 512-522. | [17] Naoum, R. 2011. "Lecture Notes, Artificial Neural Network," Middle East University (MEU), Jordan. | [18] 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). | [19] 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. | [20] 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. | [21] Naoum, R., Shihab, A., & AlHamouz, S. (2015). Enhanced Image Steganography System based on Discrete Wavelet Transformation and Resilient Back-Propagation. IJCSNS, 15(1), 6. | [22] 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. |