Eng. & Tech. Journal, Vol.30, No.20, 2012

Text Hiding Using Artificial Neural Networks

Haider Tarish Haider
Engineering College, University of Al-Mustansiriyah /Baghdad
Emasil:hth.1977@yahoo.com hth.1977@yahoo.com
Faiq Sabar Baji
Engineering College, University of Al-Mustansiriyah /Baghdad
Ahmad Saeed Mohammad
Engineering College, University of Al-Mustansiriyah /Baghdad

Received on: 23/11/2011 & Accepted on7/6/2012

ABSTRACT

The growth of information technology and data transfer led to increase the data attacks, so that information security becomes an important issue to keep the data saved during information exchanges in computer networks. Steganography techniques used to protect the information from being detected. The art of steganography will hide secret information into cover data, which will be sending without any change so the attack does not recognize any change into cover image. This paper use the Steganography and artificial neural networks to presents an information hiding procedure for hiding text in cover image, the secret text will be converted to binary code, also the cover image will be converted to the binary data in form of vectors. The supervised learning of neural networks will use binary patterns of hidden text as set of input values, and the corresponding cover image data as target that used as teacher signal to neural network. The generated weights from neural network and the coordinate of data block of cover image have been saved and then used to extract hidden text data.

Keywords: Information Technology, Steganography, Digital Watermarking, Information Hiding, Artificial Neural Network**.**

اخفاء النص بأستخدام الشبكات العصبية الاصطناعية

الخلاصة

ان تطور تكنولوجيا المعلومات وتناقل البيانات ادى الى زيادة الهجمات على البيانات، لذلك اصبح امن المعلومات اواً مهماً لابقاء البيانات آمنه خلال تبادل المعلومات في شبكات الحاسبات. ان تقنيات الاخفاء (steganography) تستخدم لحماية المعلومات من دون كشفها, ان مهارة الاخفاء سوف تخفي المعلومات السرية داخل بيانات الغطاء، والتي سوف ترسل بدون ان تغيير لذلك المخترق لا يميز اي تغيير داخل صورة الغطاء. هذا البحث يستخدام الاخفاء (steganography) وكذلك الشبكات العصبية الاصطناعية (artificial neural networks) ليقدم طريقة لاخفاء نص في صورة الغطاء, ان النص السري سوف يحول الى شفرة ثنائية (binary code) وكذلك صورة الغطاء سوف تحول الى بيانات ثنائية بصيغة متجهات.ان تعلم المراقب للشبكات العصبية سوف يستخدم الانماط الثنائية (binary pattern) للنص السري كمجموعة من القيم المدخلة، وما يقابلها من صورة الغطاء تكون هي الهدف (target) و الذي

https://doi.org/10.30684/etj.30.20.6
2412-0758/University of Technology-Iraq, Baghdad, Iraq
This is an open access article under the CC BY 4.0 license http://creativecommons.org/licenses/by/4.0

يستخدم كاشارة مُدرب للشبكة العصبية، ان الاوزان المتولدة من الشبكة العصبية والاحداثيات لكتلة البيانات لصورة الغطاء قد تم خزنها ومن ثم استخدمت لاسترجاع بيانات النص السري.

الكلمات المرشدة تكنولوجيا المعلومات، الاخفاء, العلامات المائية, أخفاء المعلومات, الشبكات العصبية الصناعية.

INTRODUCTION

The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days [1]. Using the steganography as a solution for this problem. Steganography is a technique of hiding information in digital media. In contrast to cryptography, was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately, it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret [2].

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. Unlike cryptography, where the existence of the message is clear, but the meaning is obscured, the steganographic technique strives to hide the very presence of the message itself from an observer. Steganography simply takes one piece of information and hides it within another [3]. Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object’s use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially compatible with this requirement, while research has also uncovered other file formats that can be used for information hiding as shown in Fig.(1) [2,4].

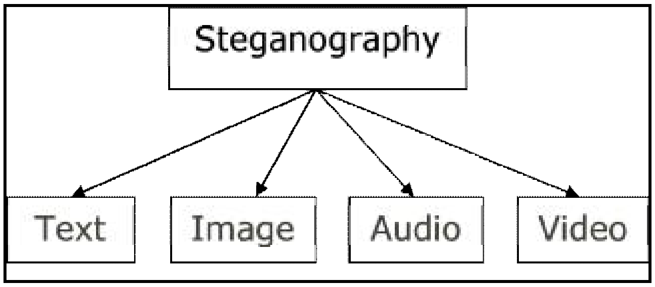


Figure (1) Steganography in Multimedia Files.

Two other technologies that are closely related to steganography are watermarking and fingerprinting. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized use of the data set back to the user [1].

RELATED WORKS

Kensuke Naoe and Yoshiyasu Takefuji, "Damageless Information Hiding Technique using Neural Network" Five neural networks are used to hide a classification of 32 secret patterns. and each pattern has five bits using one network to represent one binary digit for corresponding secret codes this method is used for small amount of data, since its very difficult to achieve that hiding[5].

E. Ashish Bansal and S. Singh Bhadauria, "watermarking using neural network and hiding the trained network within the cover image",

This paper based on Backpropagation Neural Network to train a given cover image to produce a desired watermark image. At the end of the training, the entire trained neural network weights have been hiding within the cover image itself [6]**.**

STEGANOGRAPHIC TECHNIQUES

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in an image in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are including:

i. Least significant bit insertion (LSB)
ii. Masking and filtering
iii. Transform techniques

Least Significant Bits (LSB) a simple way of steganography is based on modifying the least significant bit layer of image, In this technique, the least significant bits of the pixel is replaced by the message which bits are permuted before embedding[7]. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, find the significant areas where, the hidden message will be more integrated to cover the image and finally the data will be embed in that particular area.

Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants [1].

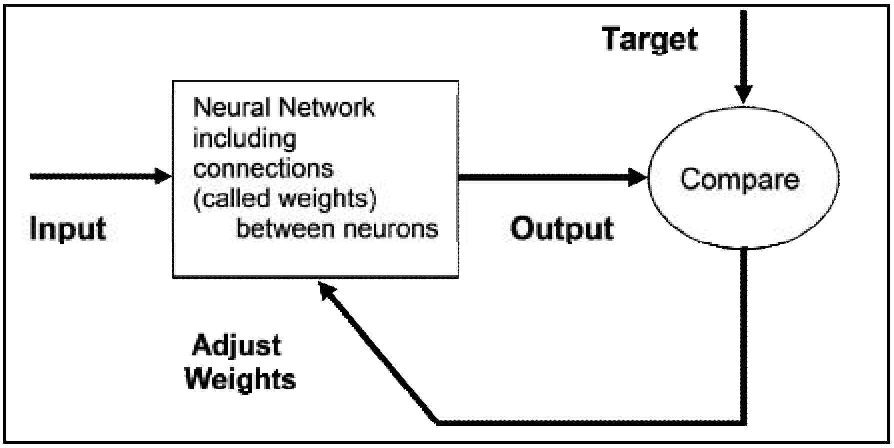
ARTIFICIAL NEURAL NETWORKS

Artificial Neural networks are composed of simple elements operating in parallel. These elements are inspired by biological nervous systems. As in nature, the network function is determined largely by the connections between elements.

PDF created with pdfFactory Pro trial version www.pdffactory.com

The training neural network to perform a particular function by adjusting the values of the connections (weights) between elements.

Commonly neural networks are adjusted, or trained, so that a particular input leads to a specific target output as shown in Fig.(2). The network is adjusted, based on a comparison of the output and the target, until the network output matches the target. Typically many such input/target pairs are used, in this supervised learning, to train a network.


Target
Neural Network including connections (called weights) between neurons
Compare
Input
Output
Adjust Weights

Figures (2) Supervised Learning In Neural Network.

Batch training of a network proceeds by making weight and bias changes based on an entire set (batch) of input vectors. Incremental training changes the weights and biases of a network as needed after presentation of each individual input vector. Incremental training is sometimes referred to as “on line” or “adaptive” training.

Neural networks have been trained to perform complex functions in various fields of application including pattern recognition, identification, classification, speech, vision and control systems [8].

PROPOSED TECHNIQUE

The proposed technique is mainly include, neural network model, embedding process and extraction process.

Neural network model

The proposed method has been used a feed-forward back-propagation with adaptive learning rate for artificial neural network (ANN).The ANN has been designed with three layers. The inputs, hidden and output layers that have been fully connected, as shown in Fig (3).

PDF created with pdfFactory Pro trial version www.pdffactory.com

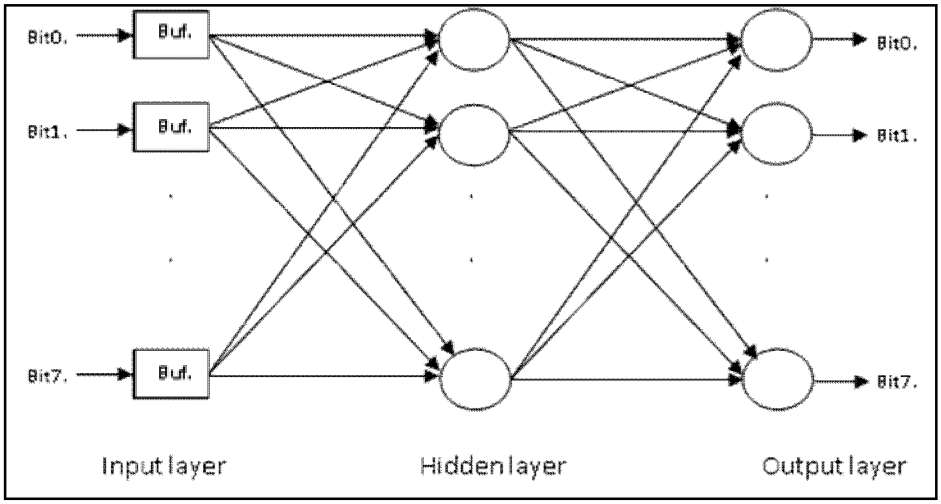


Figure (3) The Proposed ANN.

The final weights and biases have been saved to be used in the receiving side to reconstruct the secret message from the cover image. The inputs for this ANN have been applied from the secret codes of the text message; therefore, eight inputs buffers neurons have been implemented for input layer of ANN, as shown in Table(1).

Table (1) ANN System Model.

Layer	**No. of Nodes**	**Transfer Function**
Input	**8**	**---**
Hidden	**8**	**Log-Sigmoid**
Output	**8**	**Log-Sigmoid**
Training Function	**Gradient Descent Back-propagation with adaptive learning rate**	
Performance	**Mean Square Error (MSE)**	
Epochs	**48000**	
No. of Patterns	**229**	

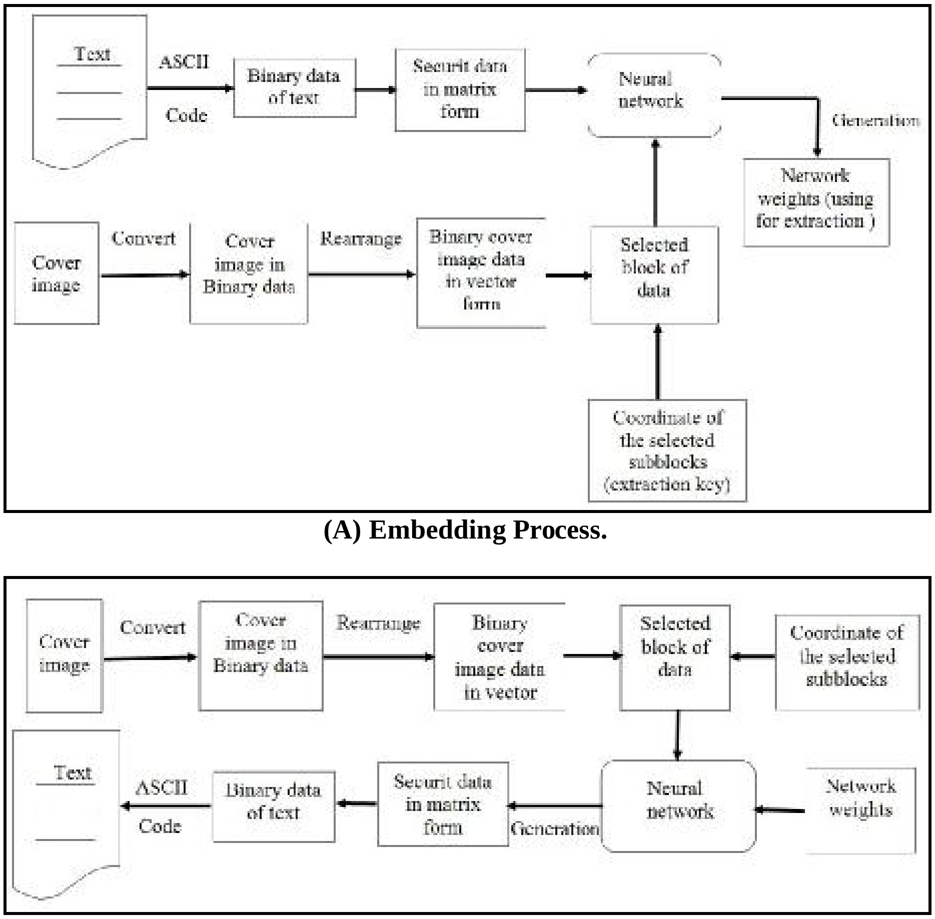
The ANN has been trained and tested for different patterns (code of the text message) to select the best performance with minimum memory capacity which

PDF created with pdfFactory Pro trial version www.pdffactory.com

represents the eight neurons of hidden layer. The output layer has been designed with eight neurons, because the target of the ANN is selected from the cover image, which is a compatible size to secret code message.

Text hiding description

After neural network structures are constructed, Figure (4) illustrates the block diagram of embedding and extracting text process.


Text
ASCII
Code
Binary data of text
Securit data in matrix form
Neural network
Generation
Network weights (using for extraction)
Cover image
Convert
Cover image in Binary data
Rearrange
Binary cover image data in vector form
Selected block of data
Coordinate of the selected subblocks (extraction key)
Cover image
Convert
Cover image in Binary data
Rearrange
Binary cover image data in vector
Selected block of data
Coordinate of the selected subblocks
Text
ASCII
Code
Binary data of text
Securit data in matrix form
Generation
Neural network
Network weights

(A) Embedding Process.

(B) Extracting Process.

Figure (4) Text Embedding And Extracting Process.

EMBEDDING PROCESS

A text of any English string text has been input with compatible size for the selected block of data from the cover image. This text has been converted to ASCII code (binary data) of 8-bit. The result secret data have been arranged into a matrix form to prepare these data as an input to the ANN.

Another hand, the cover image will be converted in two stages, in the first stage; the cover image has been converted into binary data, in the second stage, the binary data will be arranged into vector form. A block of the result vector has been

PDF created with pdfFactory Pro trial version www.pdffactory.com

selected according to the secret data size, also the selected block of cover image are taken according to pseudo random selection to make strong hiding. Therefore, the matrix of secret data (which is input to the ANN) and the vector of selected block (which is the target of ANN) will be input to the ANN to generate the weights that will be used in extraction process.

Extraction process

Three stages will be done to cover image to prepare it as input to the ANN. At the first stage, the cover image has been converted into binary data. In the second stage, the binary data has been rearranged into the vector. At the final stage of preparing a block of data has been selected according to the extraction key. The ANN will be generate the secret data according to the selected block of data (from cover image) and the previous weight of training. Finally, the secret data (binary ASCII data) has been converted into plain text.

EXPERIMENTAL RESULTS

Three images are taken as cover images (camera man, vegetables and rice) with different pixels size (256*256 and 512*384).

The secret message has content 229 different patterns and each pattern has 8 bits (1 byte) as input to the designed ANN, the target vector was taken from cover image according to the pseudo random with the same size of secret message has been fed to the ANN.

The training process is repeated until the output value satisfies a certain learning threshold value.

Figure (5) shows the application of this procedure for (camera man) which has been divided into six parts.

Part (A) show the original cover image before hiding the secret message, part (B) show the cover image after hiding the secret message, part(C) shows the curve fitting (linear regression) between target values and training values.

On other hand, part (D) shows the most important parameter of ANN which is the performance of ANN training with respect to mean square error (MSE), part (E) shows ANN training state of gradient, validation checks and learning rate values, part (F) shows ANN training window which is includes ANN view, the algorithms (for training and performance), training parameters of ANN and the plots of ANN (performance, training state and regression).

The same procedure has been applied for vegetables image as shown in figure (6) and for rice image as shown in Fig(7).

PDF created with pdfFactory Pro trial version www.pdffactory.com

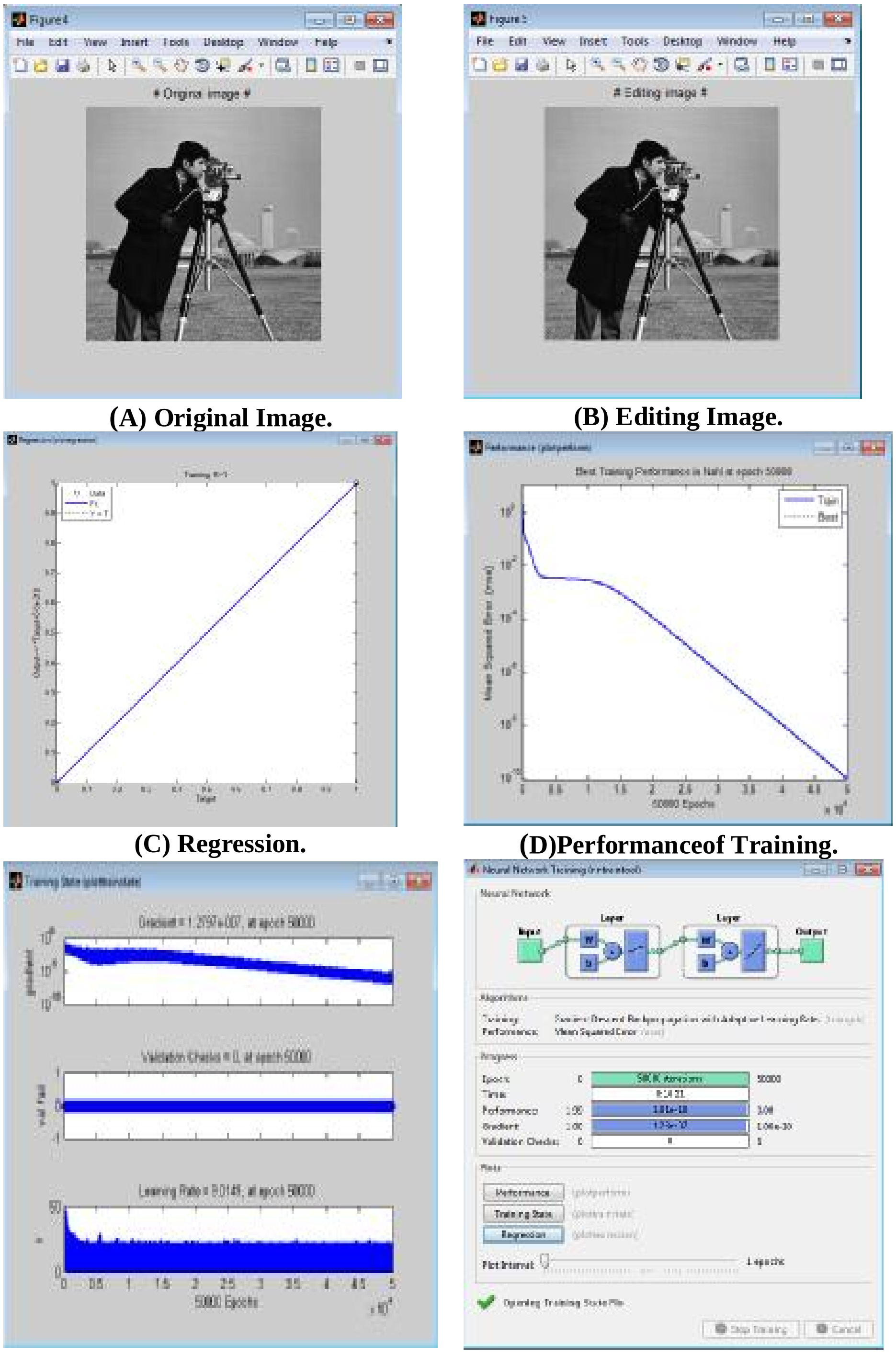


Figure 4
File Edit View Insert Tools Desktop Window Help
# Original image #
Figure 5
# Editing image #
Training: R=1
Data
Fit
Y = T
Target
Best Training Performance is NaN at epoch 50000
Train
Best
Mean Squared Error (mse)
50000 Epochs
Training State (plottrainstate)
Gradient = 1.2797e-007, at epoch 50000
gradient
Validation Checks = 0, at epoch 50000
val fail
Learning Rate = 0.0148, at epoch 50000
lr
50000 Epochs
Neural Network Training (nntraintool)
Neural Network
Input
Layer
Layer
Output
W
b
Algorithms
Progress
Plots
Performance
Training State
Regression
Stop Training
Cancel

Training: Gradient Descent Backpropagation with Adaptive Learning Rate.
Performance: Mean Squared Error

Epoch:	0	50000 iterations	50000
Time:		0:14:21	
Performance:	1.00	3.81e-10	3.00
Gradient:	1.00	1.27e-07	1.00e-10
Validation Checks:	0	0	5

Plot Interval: 1 epochs

✓ Opening Training State Plot

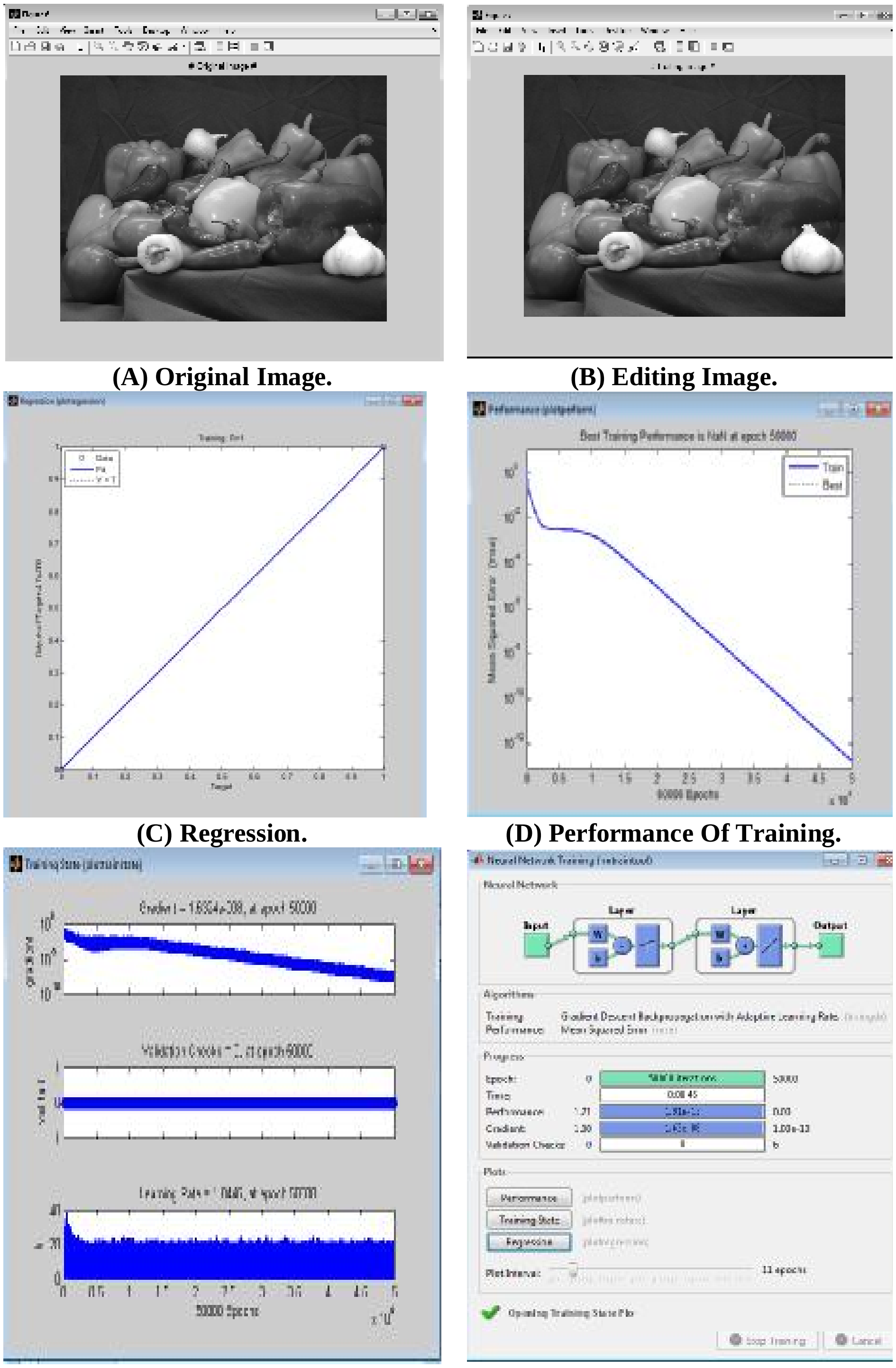
(A) Original Image. **(B) Editing Image.**

(C) Regression. **(D)Performanceof Training.**

(E) Training State. **(F) Ann Training.**

Figure (5) Test No. 1 On Camera Man.

PDF created with pdfFactory Pro trial version www.pdffactory.com



(A) Original Image.

(B) Editing Image.

(C) Regression.

(D) Performance Of Training.

(E) Training State.

(F) Ann Training.

Figure (6) Test No. 2 On Vegetables Image.

PDF created with pdfFactory Pro trial version www.pdffactory.com

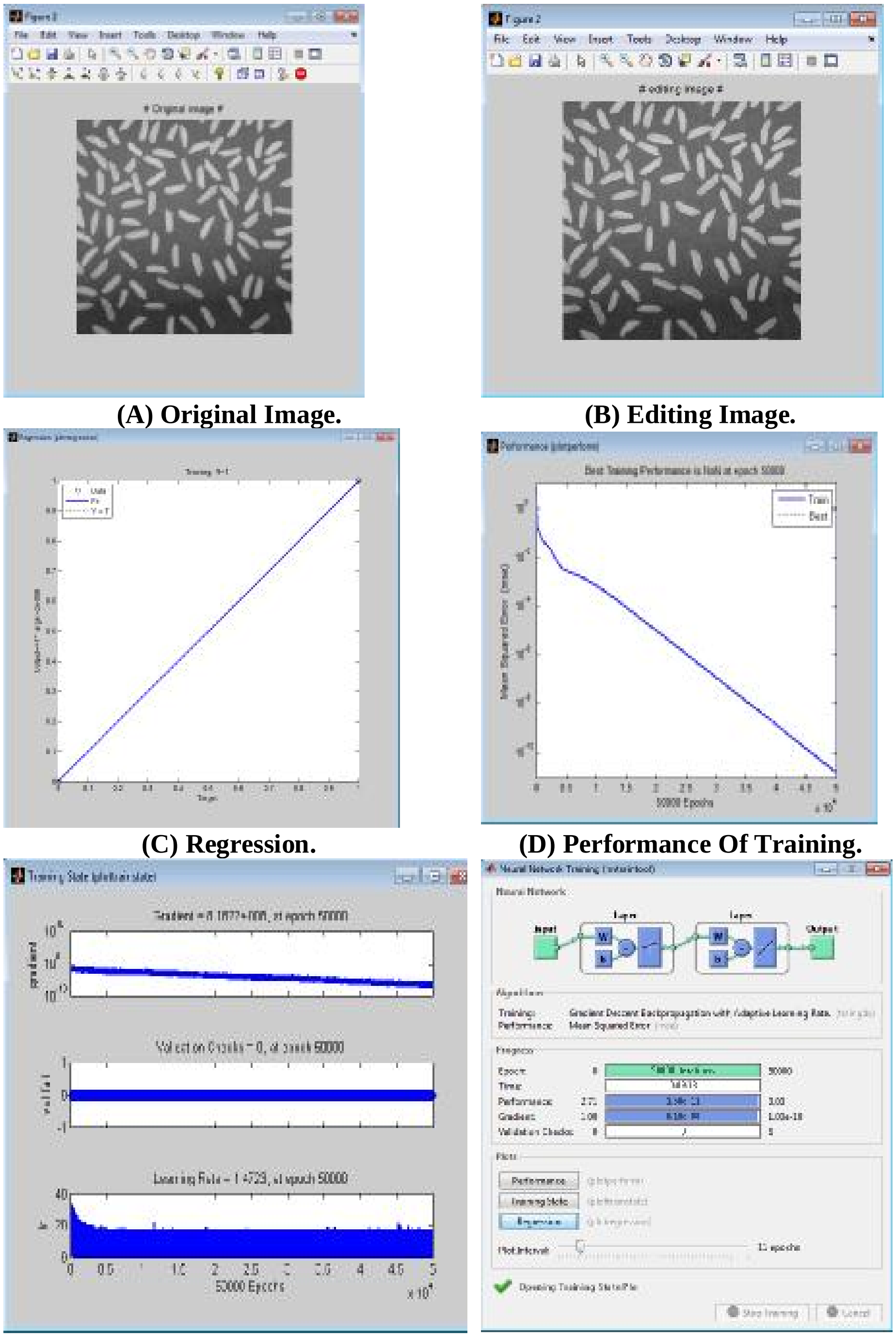


Figure 2
File Edit View Insert Tools Desktop Window Help
# Original image #
Figure 2
# editing image #
Regression (plotregression)
Training: R=1
Data
Fit
Y = T
Target
Performance (plotperform)
Best Training Performance is NaN at epoch 50000
Train
Best
Mean Squared Error (mse)
50000 Epochs
x 10⁴
Training State (plottrainstate)
Gradient = 8.1877e-008, at epoch 50000
gradient
Validation Checks = 0, at epoch 50000
val fail
Learning Rate = 1.4729, at epoch 50000
lr
50000 Epochs
x 10⁴
Neural Network Training (nntraintool)
Neural Network
Input
Layer
Layer
Output
W
b
Algorithms
Training: Gradient Descent Backpropagation with Adaptive Learning Rate.
Performance: Mean Squared Error
Progress
Epoch: 0 50000
Time:
Performance:
Gradient:
Validation Checks: 0 5
Plots
Performance
Training State
Regression
Plot Interval:
epochs
Opening Training State Plot
Stop Training
Cancel

(A) Original Image. **(B) Editing Image.**

(C) Regression. **(D) Performance Of Training.**

(E) Training State. **(F) Ann Training.**

Figure (7) Test No. 3 On Rice Image.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Table (2) shown some of ANN results such as number of iteration, cost time, and MSE.

Table (2) Ann Result

image	Image size	Image type	No. of patterns	No. of iteration	Cost Time	Performance (MSE)
Camera man	**256*256**	**png**	**229**	**50000**	**0:10:21**	**1.01e -10**
pepper	**512*384**	**png**	**229**	**50000**	**0:8:45**	**1.91e-13**
rice	**256*256**	**png**	**229**	**50000**	**0:9:38**	**1,60e-11**

CONCLUSIONS

This paper used the artificial neural network (ANN) and steganography techniques to hide secret message of (299) different patterns into cover image.

The benefit of this method actually, there is no data will be added or modified to the cover image; this will lead to strong information hiding. The block of data form cover image has been selected according to the pseudo random generation to make it another key of hiding. The results of the selected cover images (camera man, vegetables and rise) gives perfect reconstruction of the secret messages.

REFERENCES

[1]. Amin, M.M. S. Ibrahim, M. Salleh, and M. R. Katmin, " Information Hiding Using Steganography", university technology malaysia, Department of Computer System & Communication Faculty of Computer Science and Information system, Universiti Teknologi Malaysia Institutional Repository (UTM-IR, digital collection of the University's intellectual or research output), 2003.
http://eprints.utm.my/4339/1/71847.pdf.

[2]. Hmood,A.K. B.B. Zaidan, A.A. Zaidan and H.A. Jalab," An Overview On Hiding Information Technique In Images", J. Applied Sci., volume:10, issue:18, page no. 2094-2100, 2010.

[3]. Manglem Singh, K. S. Birendra Singh and L. Shyam Sundar Singh," Hiding Encrypted Message in the Features of Images", IJCSNS, VOL.7 No.4, April 2007.

[4]. T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in HS Venter, JHP Eloff, L Labuschagne and MM Eloff (eds), Proceedings of the

PDF created with pdfFactory Pro trial version www.pdffactory.com

Fifth Annual Information Security South Africa Conference *(ISSA2005)*, Sandton, South Africa, June/July 2005 (Published electronically) http://martinolivier.com/open/stegoverview.pdf.

[5]. Kensuke Naoe and Yoshiyasu Takefuji, "Damageless Information Hiding Technique using Neural Network", IJCSNS, VOL.8 No.9, September 2008.

[6]. E. Ashish Bansal and S. Singh Bhadauria, "Watermarking Using Neural Network And Hiding the Trained Network Within the Cover Image", JATIT, 2008, www.jatit.org.

[7]. Motameni,H. M. Norouzi, M. Jahandar, and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, 2007.

[8]. Howard Demuth, and Mark Beale, "Neural Network Toolbox",Math Works Inc.,2002.

PDF created with pdfFactory Pro trial version www.pdffactory.com