Eng. & Technology, Vol.25, No.9, 2007

A Secure Invisible Watermarking Using Rijndael Algorithm and Wavelet Transform

Dr. Saleh M. Al-Qaraawy* Dr. Imad H. Al-Hussaini* Khalid F. Shubair*

Received on: 23/3/2005
Accepted on: 12/7/2006

Abstract

Digital watermarking hides secret or personal information in host digital data to demonstrate and protect the copyrights of digital products, to authenticate the contents of digital data, or to convey side information such as access control or annotations. There are several fundamental requirements for watermarking such as: Perceptual invisibility. For robustness, a watermark should be resistant to a variety of manipulations, either unintentional or malicious. The detection should be accurate and especially the mean square error rate should be very small. To help protect the copyright and data security, Rijndael algorithm will be used using many mathematical operations like (Byte Substitution, ShiftRow, MixColumn and AddRound Key). The wavelet transform or wavelet analysis is probably the most recent solution to watermarking Rijndael code. Meaning by factoring technique for invisible watermarking Rijndael code is calculated and inputted in random locations. At the end, a detection process based on back propagation neural network will be used to detect watermarking string.

العلامة المائية السرية غير المرئية باستخدام خوارزمية رايندال وتحويل المويجة

الخلاصـــــــــة

إن الغرض من إخفاء البيانات الرقمية في العلامة المائية الرقمية هو إما لحماية المنتج الرقمـــي ، للتأكد من محتوى المعلومات الرقمية أو لإيصال جزء من المعلومات مثل السيطرة علـــى الوصـــول. هنالك الكثير من المتطلبات الأساسية للعلامة المائية منها: الإدراك الحسي بأنه غير مرئية. وللمتانة يجب أن تكون العلامة المائية مقاومة للمناورة المتغيرة المقصودة وغير المقصودة. يجب أن يكون الكشف تام وخاصة معامل معدل مربع الخطأ (MSE) والذي يجب أن يكون صغير جدا. وللمســـاعدة في حماية النشر أو البيانات السرية تستخدم خوارزمية رايندل (Rijndael) باستخدام عدة عمليـــات حسابية مثل (إحلال بايت ، تزحيف صف ، مزج عمود ، وغيرها) . إن تحويل المويجـــة أو تحليـــل المويجة قد يعتبر الحل الأمثل لشفرة العلامة المائية لرايندل. تعرض في هذا البحث تقنيـــة المعامـــل كتطوير لشفرة رايندل للعلامة المائية. ان عملية الكشف عن سلسلة العلامة المائية ستتم باســـتخدام الشبكات العصبية.

1. Introduction

Information hiding represents a class of processes used to embed data into various forms of media such as images [1]. The embedded data should be invisible to a human observer. The term hiding can refer to either making the information imperceptible or keeping the existence of the information secret. Depending on what

* Control and Systems Engineering Dept. - University of Technology

https://doi.org/10.30684/etj.25.9.1
2412-0758/University of Technology-Iraq, Baghdad, Iraq

information and in which form it is hidden in the media one can select robust watermarking using Rijndael ciphering algorithm. Wireless LANs have gained strong popularity in a number of vertical markets, including the health-care, retail, manufacturing, warehousing, and academia [2]. These fields have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today, wireless LANs (WLANs) are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers. Wireless LAN products, based on the different flavors of 802.11, are available from many different vendors. Depending on transmission scheme, products may offer bandwidths ranging from 1 Mbps up to 22Mbps [3].

Discrete wavelet transform techniques (DWT) can be used to distribute invisible Watermarking Rijndael code. It will be shown that the watermarking string code can be ciphered by Rijndael algorithm and any different attack like noise, clipping and compression have not effects on detecting watermarking Rijndael binary code. Back propagation neural network (BPNN) is used for training the neighborhood pixels in two dimensional images. So, BPNN has been designed to detect and reconstruct watermark Rijndael binary code.

2. Simulation Techniques

In this paper, two keys are used for this simulation:

1) Pseudo random sequence for watermarking code.
2) A Rijndael secret key (password Rijndael key).

The locations, for watermarking code between sender and receiver via wireless LAN network, depend on the designer. The transmitter applies pseudorandom sequence code and Rijndael secret key (password key). The location for watermarking code is then scaled by a new technique called meaning by factoring method which depends on a mean value around watermark location. Discrete Wavelet Transform (DWT) is then repeatedly adding watermark Rijndael code to the sub bands (LH, HL and HH). This new technique gives a good invisible watermarking Rijndael code by using the above method.

3. Meaning By Factoring Method

In this section, a new watermark embedding and extraction system is presented, in an attempt to capture the various systems and configurations that have been presented. Many different types of watermarks have been proposed for a variety of applications, e.g., copyright image protection, broadcast monitoring, owner identification, proof of ownership, copy control and covert communication. The watermarking range lies between:

$$\mathbf{W = \{w(r,c),\ 0 \le r \le 255;\ 0 \le c \le 255\},}$$

where r and c are the length and width of the image , is embedded into the original image:

$$\mathbf{H = \{h(r,c),\ 0 \le r \le 255;\ 0 \le c \le 255\ \},}$$

To create a watermarked image, H' should be visually close to

H. A secret key, K, may be used as shown in Fig.1.

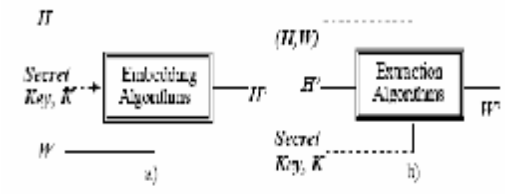

Figure 1 Embedding and extraction Block diagram

In watermark detection process, the watermark W' is extracted from the 'tested' image then W' is compared with the original signature W, see Fig.1. The most common watermark embedding rules are the following:

$$H_{new}' = H_{old}' + \{(code(Rijndael) * (Hold' - average))\}$$

where the summation of all pixels around watermark is divided by the number of locations, called the average, as shown in Fig.2.

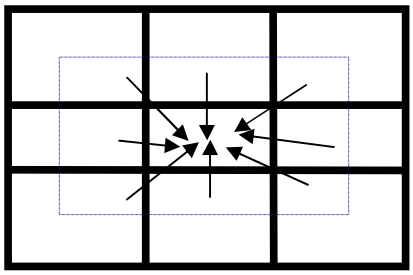

Figure 2 Neighborhood pixels

The first row, first column, final row and final column should be avoided for watermarking location because there is no mean values (average values) at these locations. This new technique is called meaning by factoring, see Fig. 3.

No	**No**	**No**	**No**	**No**	**No**
No	**Yes**	**Yes**	**Yes**	**Yes**	**No**
No	**Yes**	**Yes**	**Yes**	**Yes**	**No**
No	**Yes**	**Yes**	**Yes**	**Yes**	**No**
No	**Yes**	**Yes**	**Yes**	**Yes**	**No**
No	**No**	**No**	**No**	**No**	**No**

Figure 3 Avoiding first row, first column, final row and final column

In its simplest form, such a process has three inputs, the pseudorandom key, Rijndael password key and watermarking string as shown in the Fig. 4-. This process may be represented as blocks and this is called an encoder or embedding process.

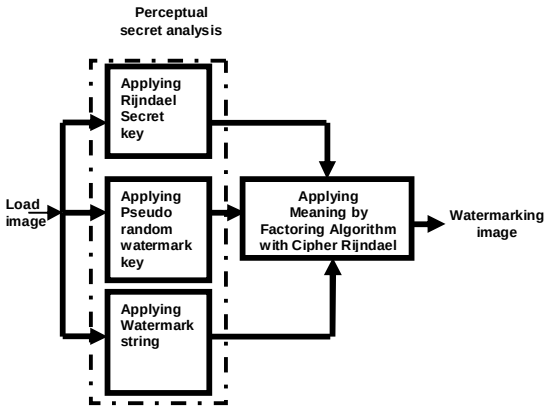

Figure 4 A block diagram for transmitting invisible watermarking image after applying meaning by factoring methods

In the former, watermark data is converted into a form suitable for applying watermarking Rijndael secret

key to the image. It is clear from the above illustration that the extraction procedure is almost an inverse of the embedding process.

Depending on the intended application, two additional steps may be performed during the embedding and extraction process from perceptual secret analysis. These include pseudo random watermark key and Rijndael password key generation. Note that the attacker is not able to detect watermark code because of a good security achieved through design as will be shown in the results. The block diagram of the extraction process is shown in Fig. 5.

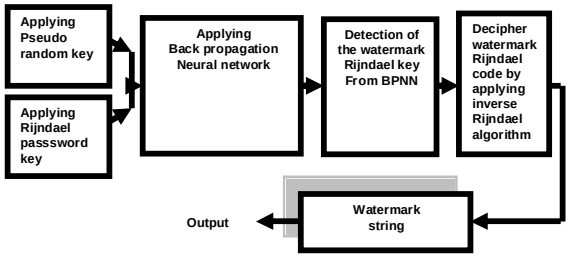

Figure 5 A block diagram for receiving image after applying typical extraction method using BPNN.

4. Rijndael Algorithm Specification

Rijndael algorithm is an iterated block cipher with variable block length and variable key length [4]. The block length and the key length can be independently specified to 128, 192 or 256 bits with the constraint that the input and the output have the same length. Internally Rijndael operations are performed on a two dimensional array of bytes called the state. All the intermediate cipher and inverse cipher results are stored in the state. This array has four rows. The number of columns represents the data block length to be encrypted divided by 32 and is denoted by Nb. At the start of the cipher and inverse cipher operations, the input block is copied into the state array; the cipher or inverse cipher operations are then conducted on this state array. Fig. 6 shows many mathematical operations within Rijndael ciphertext algorithm.

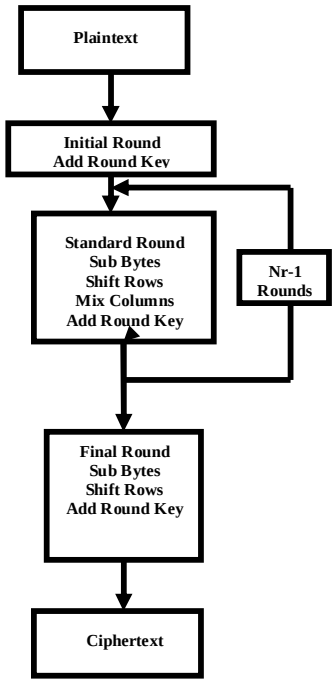

Figure 6 Rijndael ciphertext algorithm

The cipher key is similarly considered as a rectangular array with four rows. The number of columns is equal to the key length divided by 32, and denoted by Nk. These representations are illustrated in Fig.7

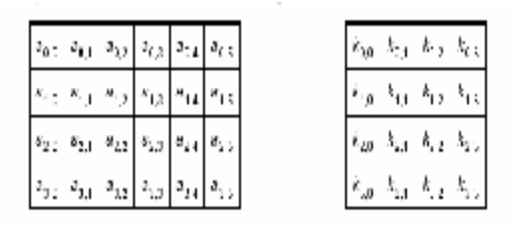

Figure 7 Example of a state with Nb=6 and cipher key with Nk=4

The number of rounds is denoted by Nr, and depends on the values of Nb and Nk as given in Table (1). For example when Nk=4, Nb=6, then Nr=12.

Table (1) Number of rounds Nr as a function of the block and key length

Nr	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

i. The ShiftRow Transformation

In ShiftRow, the rows of the State are cyclically shifted over different offsets. Row 0 is not shifted, Row 1 is shifted over C1 bytes, row 2 over C2 bytes and row 3 over C3 bytes. The shift offsets C1, C2 and C3 depend on the block length Nb. The different values are specified in Table (2). The operation of shifting the rows of the State over the specified offsets is denoted by: ShiftRow (State).

Table(2) Shift offsets for different block length

Nb	C1	C2	C3
4	1	2	3
6	1	2	3
8	1	3	4

Fig. 8 illustrates the effect of the ShiftRow transformation on the State.

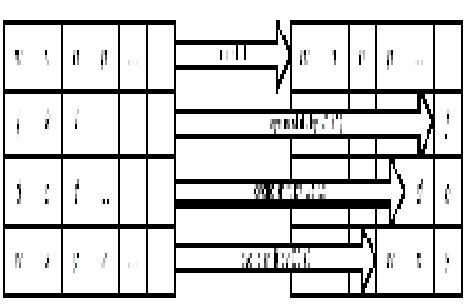

Figure 8 The effect of ShiftRow Transformation

The inverse of ShiftRow is a cyclic shift of the 3 bottom rows over Nb-C1, Nb-C2 and Nb-C3 bytes respectively so that the byte at position j in row i moves to position (j + Nb-Ci) mod Nb [6].

ii.The MixColumn Transformation

In MixColumn, the columns of the State are considered as polynomials over GF(2^8) and multiplied modulo $x^4 + 1$ with a fixed polynomial c(x), given by:

a(x) = '03' x^3 + '01' x^2 + '01' x + '02' .

This polynomial is co-prime to $x^4 + 1$ and therefore invertible. This can be written as a matrix multiplication. Let s'(x) = a(x) $\otimes$ s(x),

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

As a result of this multiplication, the four bytes in a column are replaced by the following:

$$S'_{O,C} = (\{02\} \bullet S_{0,C}) \oplus (\{03\} \bullet S_{1,C}) \oplus (S_{2,C} \oplus S_{3,C}$$

$$S'_{1,C} = S_{0,C} \oplus (\{02\} \bullet S_{1,C}) \oplus (\{03\} \bullet S_{2,C}) \oplus S_{3,C}$$

$$S'_{2,C} = S_{0,C} \oplus (S_{1,C}) \oplus (\{02\} \bullet S_{2,C}) \oplus (\{03\} \bullet S_{3,C})$$

$$S'_{3,C} = (\{03\} \bullet S_{0,C}) \oplus (S_{1,C}) \oplus (S_{2,C}) \oplus (\{02\} \bullet S_{3,C})$$

The application of this operation to all columns of the State is denoted by MixColumn (State). Fig.9 illustrates the effect of the MixColumn transformation on the State [6].

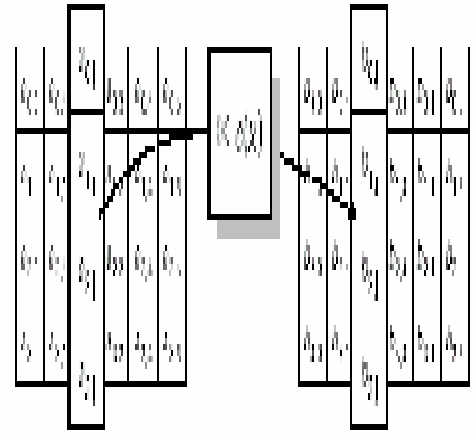

Figure 9 MixColumn Operation.

The inverse of MixColumn is similar to MixColumn.

a(x)=('03' x^3 + '01' x^2 + '01' x + '02')

It is given by:

a^{-1} (x) = '0b' x^3 + '0d' x^2 + '09' x +'0e').

iii. The Round Key Addition

In this operation, a Round Key is applied to the State by a simple bitwise EXOR. The Round Key is derived from the Cipher Key by means of the key schedule. The Round Key length is equal to the block length Nb. The transformation that consists of Exporting a Round Key to the State is denoted by:

AddRoundKey(State,RoundKey).

This transformation is illustrated in Fig. 10.

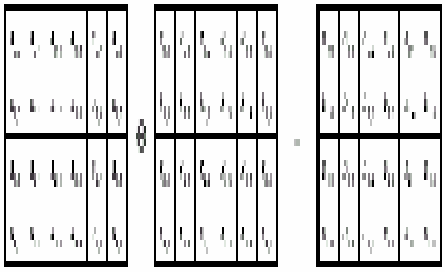

Figure 10 In the key addition the Round Key is bitwise exored to the State. Addroundkey is its own inverse.

5. Watermarking Used in the Wavelet Domain

A subband filtering system allows a signal to be separated into different frequency bands by employing a combination of lowpass, bandpass, and / or highpass filters, along with down sampling of the filtered signals [7]. If certain conditions are meeting the design of the filters, then perfect reconstruction of the original signal can be obtained by using a reconstruction scheme of upsampling

and filtering to remove spectral aliasing effects. In this study, the Discrete Wavelet Transform (DWT) is used to implement subband decomposition and reconstruction filter banks . The DWT can be flexible and extended to work in two and higher dimensions by using separable filters working on separate dimensions. An excellent description of a two-dimensional wavelet filtering scheme can be found in [8,9]. In this paper, the operations of computing the forward and inverse DWT, regardless of dimension, will be denoted DWT and IDWT, respectively. It is possible to state that the most important features of a watermarking technique are that the watermark unnoticeable, robust and blind, i.e., the watermark decoder must not require the original image for extracting the embedded code. The algorithm below explains how an image is loaded and how it is divided by DWT, see the flowchart in Fig. (11). The technique has the ability to locate the region that has been altered. In this paper, watermarks have been embedded into images using wavelet packets in order to fulfill the above characteristics**.**

The new technique (meaning by factoring) is distributed in three bands (LH,HL,HH).The following are the details of these techniques see Fig.(12).

6. Back Propagation Neural Network

The backpropagation (BP) algorithm is also known as error backpropagation or back error propagation or the generalized delta rule[10]. The networks that get trained like this are sometimes known as multilayer perceptrons or MLPs.

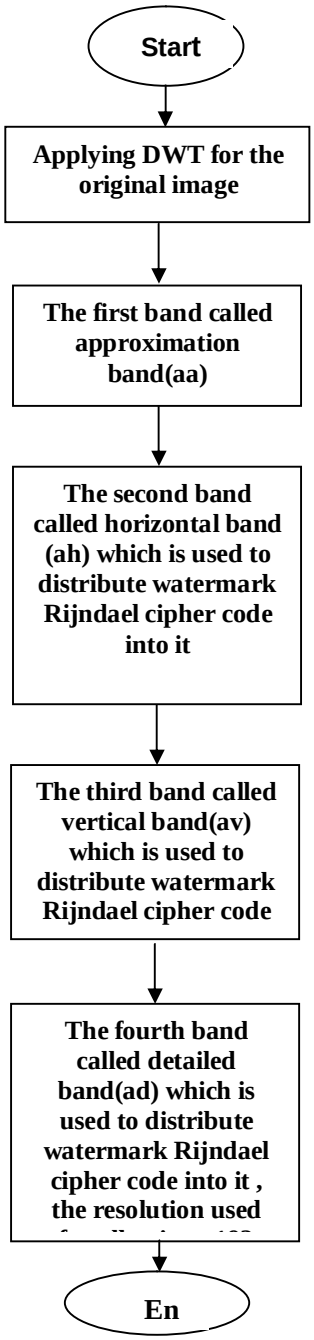

Figure 11 Flowchart illustrate DWT used to distribute watermarking Rijndael Code.

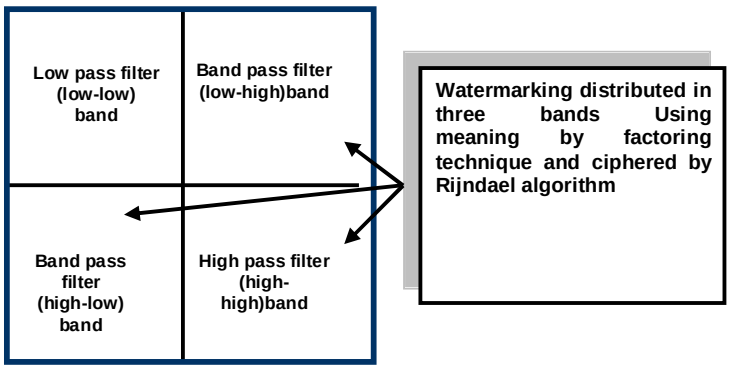

Figure 12 Applying discrete wave let transform and distributed watermarking technique.

In the construction used for back propagation network there are nine input layers, fifteen nodes for the first hidden layer and five nodes for the second hidden layer and one output layer. The input's are called the (neighborhood pixels) wich lies around watermarking Rijndael code, the hidden contain many nodes to train the network and the output to give the actual value. The weights interconnecting the input and the hidden nodes are adjusted and learned, the weights interconnecting the hidden and the output nodes are also trained and adjusted to reach the actual value [11].

Backpropagation algorithm has been used to recognize and detect watermarking Rijndael cipher code. Binary digit code for the watermarking string Rijndael code has been decoded. One of the critical issues in watermarking Rijndael code is the feature selection for the back propagation layers construction and is dependent on the choice of the features for each case used [11,12].

The aim was to recognize all bits for watermark Rijndael cipher code and the goal to create a network that could recognize the inverse cipher to obtain the watermarking characters correctly though there were some attacks like noise and others which make errors in any bit but increase the number of copies for watermarking Rijndael which will defeat any attacking appearing in image.

7. Simulation Results

A) For Wbarb Image:

i) At Sender:

Number of copy:	20
Watermark key:	12
Rijndael key password:	2004
Watermark string:	KHALID
Wavelet kind:	Db2

The achieved DWT for wbarb image is

shown in Fig. (13).

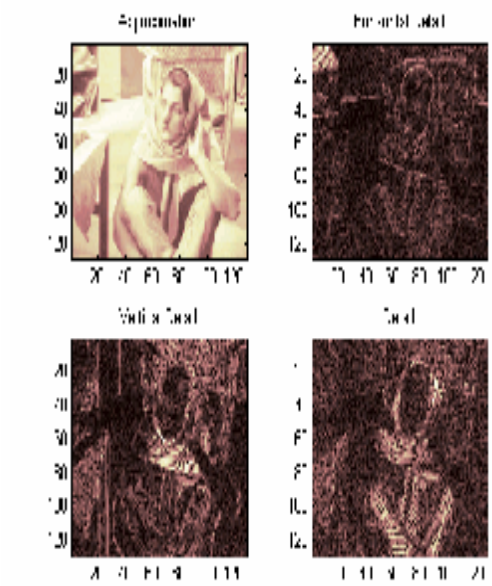

Figure 13 Applying DWT for 2-D image

The original image and invisible watermark image are shown in Figs.(14) and (15) respectively.

Figure 14 The original image

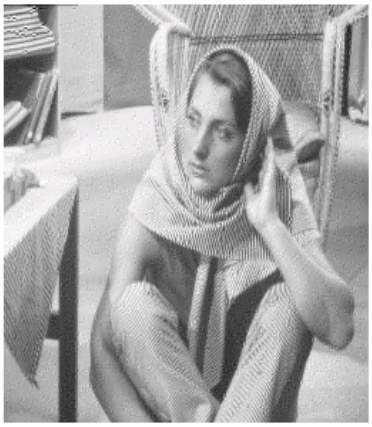

Figure 15 Invisible watermarking with Rijndael cipher code

ii) At Receiver: Enter Two Keys To obtain Watermark String By BPNN:

Watermark key:	12
Rijndael key password:	2004
Number of first hidden layer:	15
Number of second hidden layer:	5
Number of output:	1

The received image with watermarking Rijndael cipher code is shown in Figure (16).

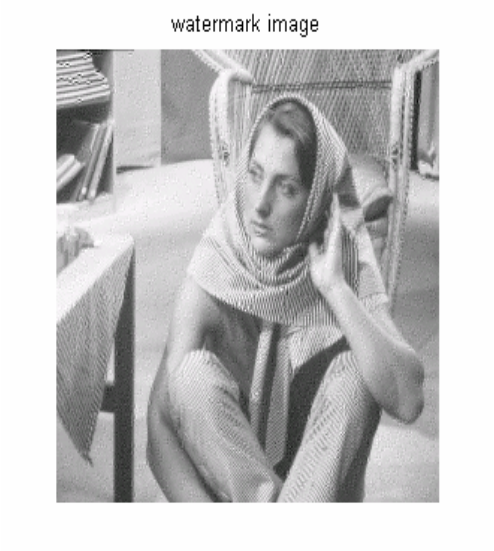

Figure 16 Invisible received image with watermarking Rijndael code

Table (3) shows the calculation for epoch and MSE.

Table (3) Calculation results for Epoch and MSE.

EPOCH	MSE
0/100	1.69344/0
25/100	1.06089/0
50/100	1.01018/0
75/100	0.959222/0
100/100	0.793693/0

The backpropagation neural network training at received point shown in Fig. (17) illustrates the MSE.

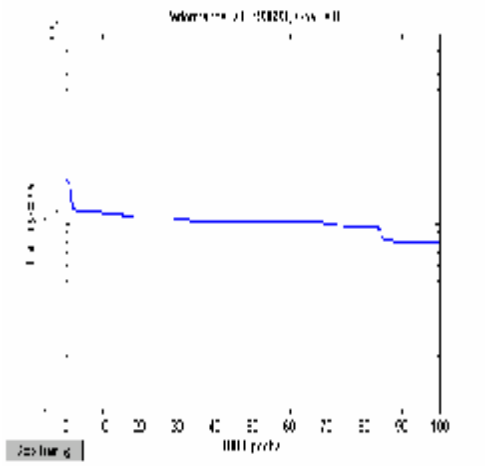

Figure 17 The relation to calculate MSE for BPNN training network

after detecting it by backpropagation neural network and deciphered by inverse Rijndael algorithm shown below:
Watermark String Answer: KHALID

B. Example2:
At sender: Enters Watermark String

Number of copy:	15
Watermark key:	55
Rijndael key password:	PALESTINE
Watermark string:	QUDS2004
Wavelet kind:	Coif1

The DWT for Wbarb image is shown in Fig.18.

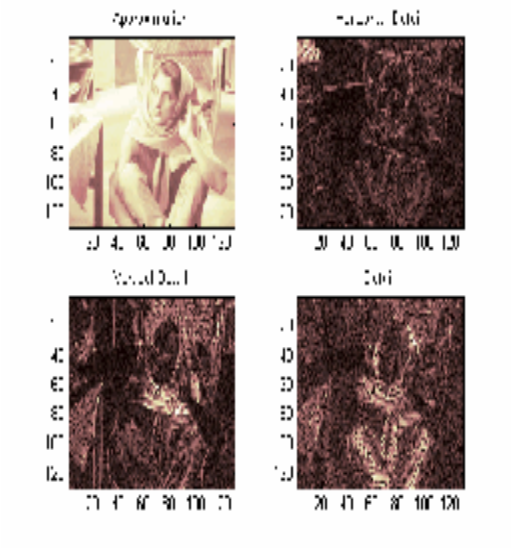

Figure 18 Applying DWT for 2-D image

The original image and invisible watermark images are shown in Figures (19) and (20) respectively.

Figure 19 Two dimensional original image

Figure 20 Invisible Watermarking image with Rijndael cipher code

ii) At Receiver: Enter Two Keys To obtain Watermark String By BPNN:

Watermark key	**55**
Rijndael key password	**PALESTINE**
Number of first hidden layer:	**17**
Number of second hidden layer:	**6**
Number of output:	**1**

The received invisible image with watermarking Rijndael cipher code technique is shown in Fig.21, while Table (4) shows the calculations of epoch and MSE.

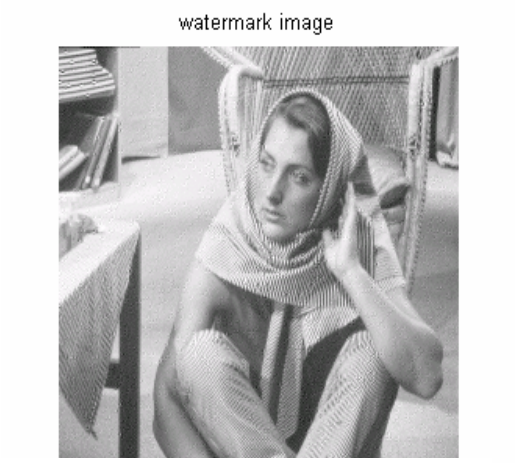

Figure 21 Invisible Watermarking received image with Rijndael cipher code

Table(4): Calculation results for epoch and MSE

STEPS NUMBER	EPOCH	MSE
0	0/100	1.89334/0
1	24/100	1.32721e-016/0

The backpropagation neural network training for received image shown in Figure (22) illustrates MSE.

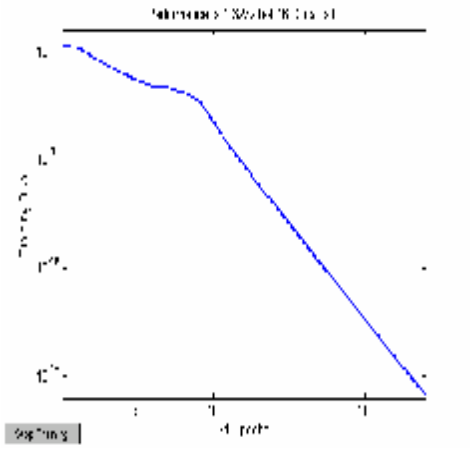

Figure 22 The relation to calculate MSE for training network

Watermark String Answer: QUDS2004

8. Conclusions

In this paper, we have introduced the invisible watermark using secret method called Rijndael algorithm. Matlab simulation is built and used to examine the performance for using invisible watermarking Rijndael code
by new technique called meaning by factoring methods. Many mathematical operations: ***(Byte Substitution, ShiftingRow, Mixing Column and AddRoundKey state) used for Rijndael algorithm.*** apply ***Discrete Wavelet Transform (DWT)*** for original image to give four bands **(low-low), (low-high), (high-low)** and **(high-high)** which process watermark Rijndael code in three bands using meaning by factoring method and reconstruct four bands using inverse wavelet transform to original watermark Rijndael code image. The designer must secure two parts Rijndael secret key and watermark key without any one identifing this information. Using Back Propagation Neural Network (BPNN) to detect watermark Rijndael code gives low mean square error.

References

[1] Huda K.Al-jobori, "Watermarking System for 3D Models" Ph.D. Thesis, University of Technology, Computer Science Department, July 2003.
[2] Kenny, k., "A Simulator for Wireless Local Area Networks", M.Sc.

Thesis, Waterloo. Ontario, Canada, 1998.
[3] Wi,Fi., ”D-Link Air Plus DWL-520+:Enhancment 2.4GHz Wireless PCI Adapter” , Manual Rev051002, Taiwan,1999.
[4] Joen Daemen and Vincent Rijmen ”AES Proposal: Rijndael” Document Version2,Internet Paper.1999,Site: http://csrc.nist.gov/encryption/aes/rijndael/Rijndael
[5] Stefan, Lucks., ”Attacking Seven Rounds of Rijndael Under 192-bit and 256-bit Keys”, Report University of Maunheim, Germany, 2000.
[6] Fedral, et al., ”Announcing the Advanced Encryption Standard (AES)”, Internet Paper from Information Processing Standards Publication, 2001.
Website: http://www.cs.technion.ac.il/~cs236506/online/fips197
[7] Deepa, Kunder. ”Digital Watermarking Using Multiresolution Wavelet Decomposition”, Paper presented at University of Toronto, Electrical and Computer Engineering, Canada 1999.
[8] Hisashi, and Akio., ” An Image Watermarking Methods Based on the Wavelet Transform ”, Report, Kyushu University, Fukuoka, 812-8581, Japan, 2000.
[9] Laurent, B., and Aleksadro, M., ” Wavelet Domain Features for Texture Description, Classification and Replicability Analysis”, Bell Laboratories, Luncent Technology, Murray Hill, NJ, 1999.
[10] Chen, D. S., ” A Robust Back Propagation Learning Algorithm for Function Approximation ”, IEEE Trans .Neural Network,Vol.5,May 1994.
[11] Lippman, R., ”An Introduction to Computing with Neural Networks”, IEEE Assp Magazine, pp4-22, April 1987
[12] Narendra, K. S.,” Identification and Control of Dynamical Systems Using Neural Networks”, v1, n1, pp4-27, March 1990.