International Journal of the Physical Sciences Vol. 5(11), pp. 1776-1786, 18 September, 2010
Available online at http://www.academicjournals.org/IJPS
ISSN 1992 - 1950 ©2010 Academic Journals

Full Length Research Paper

Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem

A. A. Zaidan[1], B. B. Zaidan[1], Y. Alaa Taqa[2], M. Kanar Sami[2], Gazi Mahabubul Alam[3]* and A. Hamid Jalab[2]

[1]Faculty of Engineering Multimedia University, 63100 Cyberjaya, Selangor Darul Ehsan, Malaysia.
[2]Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia.
[3]Faculty of Education, University of Malaya, Kuala Lumpur, Malaysia.

Accepted 12 August, 2010

Steganography is defined as the art of concealing a sensitive data through other carrier to insure the confidentiality of the data. Four novel concepts has been presented on this paper, beginning with steganography, the prevailing methods, well-known is the use of a single cover to hide the data, in this paper, we invent a new concepts on Steganography which is "multi-cover steganography" using remote sensing image; Remote sensing Image is an image taken from the satellite in a manner of three shots, engagimg these images generate one false color image, this type of image has been proposed in this research. The second concepts is general recursion neural cryptosystem, this approach has been designed and implemented to defeat the problem of exchange cryptography keys through the network, the new cryptosystem exchange the keys through trine the neural network data which later on used to decrypt the data, this powerful cryptosystem merged with the multi-cover steganography to produce the third novel concept. The fourth concept is designing irregular encoding method base on LSB algorithm. The new way of encoding has approved the security of data hidden. The experiment has approved that, our system has been extremely secure, confidential, and there is no way to extract the data from the cover

Key words: Remote sensing image, steganography, general regression neural cryptosystem (GRNN), cryptography, data hidden.

INTRODUCTION

As the amount of products and services offered via the Internet grows rapidly, consumers are more and more concerned about security and privacy issues (Jahangir and Begum, 2008). Information hiding techniques have recently become important in a number of application areas, digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly. According to Alanazi et al. (2010), Hashim et al. 2010, Zaidan et al. (2010) privacy, copyright and security are very important issues. As the amount of products and services offered via the Internet grows rapidly, consumers are seriously concerned about security and privacy issues and their concern is increasing (Jahangir and Begum, 2008). Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction (Everett, 2005; Stevens and Attorney, 2007; Stevens and Library of Congress Washington Dc Congressional Research, 2009; Abomhara et al., 2010; Al-Frajat et al., 2010).

In order to reduce perceived risk, the secure transaction mechanisms, such as information disclosure, transaction transmission, information privacy should be guarantee and the responsible should be known. (Mondéjar-Jiménez et al., 2009; Azmi and Kamarulzaman 2010; Lu Huang et al., 2010; Zaidan et al., 2010c).

*Corresponding author. E-mail: gazi.alam@um.edu.my, gazimalamb@yahoo.com. Tel: + 603-7967 5077. Fax: + 603-7967 5010.

Research objectives

Data hidden has two main approaches, steganography and digital watermarking, these two approaches have many techniques (Zaidan et al., 2010). The literature is rich with data hidden approaches; most of these approaches have limitations with the size and security (Hmood et al., 2010a; Hmood et al., 2010b). This research tries to achieve the following objectives:

1. To study the features of false color images that help to apply the data hiding. 2. To investigate the capabilities of applying irregular hiding techniques. 3. To design and implement a cryptography algorithm based on general recursion neural network. 4. To implement a gathering approach based on the analysis of false color image, irregular hiding techniques and general recursion neural cryptosystem.

Literature review

One of the latest techniques that have been used in this area by researchers, they managed to hide the secret texts in DNA by using a technique called Genomic steganography, by adapt and fit the data in the nuclei chromosomes then integrate it with millions sentences and sent to the other party. To extract the secret message is soaking get special distinction sentences used on the other and then placed under the microscope to extract the required text (Shimanovsky et al., 2003). The oldest steganography technique has been taken from the legendary stories Greeks Herodotus. Other means that the common use since the first century AD, invisible inks Invisible Inks, which was able to write a confidential letter with any other non-value-confidential and usually write between lines, for example those rabbis some fruit juices Fruit Juices, milk, urine, vinegar, and all these species become dark and visible when exposed to heat the written document (Petitcolas et al., 1999; Naji et al., 2009).

The chemical characteristics of the same old species with a more accurate and efficient have been used during the first and second world wars in the military secrecy of correspondence. The modern stegagraphy or digital watermark has invented and invite many techniques. In (Zaidan et al., 2009) they used a sample of more than 100 images, to approve that it might be easy to recognize the stego-image if the mount of data hidden pass the 50% of the original image size. The experiment showed it might be easy to classify the image into neutral image and stego image, the test has been applied also into the gray level image, the result also shows the capability of apply the algorithm was greater than the result in the color images. A new study deals with constructing and implementing new algorithm based on hiding a large amount of data (image, audio, text) file into color BMP image applied in (EL-Emamb, 2007). They have been used adaptive image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly rather than sequentially by using new concept defined by main cases with their sub cases for each byte in one pixel. This concept based on both visual and statistical. Other construction is used in (Dobsicek, 2004); this scheme used hash value obtained from a file name and password and a position of header of hidden file is located. Thapproach is used by the present work with new modifications. An application of steganography is developed in (Mittal and Phamdo, 2002), where the content is encrypted with one key and can be decrypted with several other keys, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information. Because of the continual changes at the cutting edge of steganography and the large amount of data involved, stego-analysis's have suggested using machine learning techniques to characterize images as suspicious or non-suspicious developed in (Pavan et al., 2005), used entropy based technique for detecting the suitable areas in the document image where data can be embedded with minimum distortion (Zaidan et al., 2010d).

MATERIALS AND MOTIVATIONS

Strangeness of the steganography module

The strength lies of steganography on the difficulty of estimate the technique of encode the hidden data, not like the encryption where the algorithms are fixed and keys might be changed which give the attackers more opportunity to assault the cipher. LSB or least significant bit is one of the most popular algorithms on steganography and digital watermark, our analysis to LSB showed there are thousands way of encoding the data. One of the remarkable observations that showed in Figure 1, where using one bit only to implement LSB algorithm might give at lest seven different encodes.

Furthermore, the way of encoding data using LSB can be represent in a relation between the encoded bit and 2n.

$$Ne > 2n \quad (1),$$

Where Ne is the number of encodes.

In additional, this assumption has invented for a very special issue, where the data encoded over the entire image is same, means that if we encode LSB on the red color, the same encode will be applied on the entire image. In our previous study we have shown that there were a possibility of embedding 50% using pure steganography and 4-LSB with out affecting the quality of the image. Depending on Equation 1, thousands ways to encode the data if we consider there were four bits used to hide the data (refer to Figure 2).

Generate other ways of encoding the hidden data

Equation 1 represent the minimum number of the encoding ways using LSB algorithm, the question is: can we generate more ways? The way followed to calculate the encode method adopted the

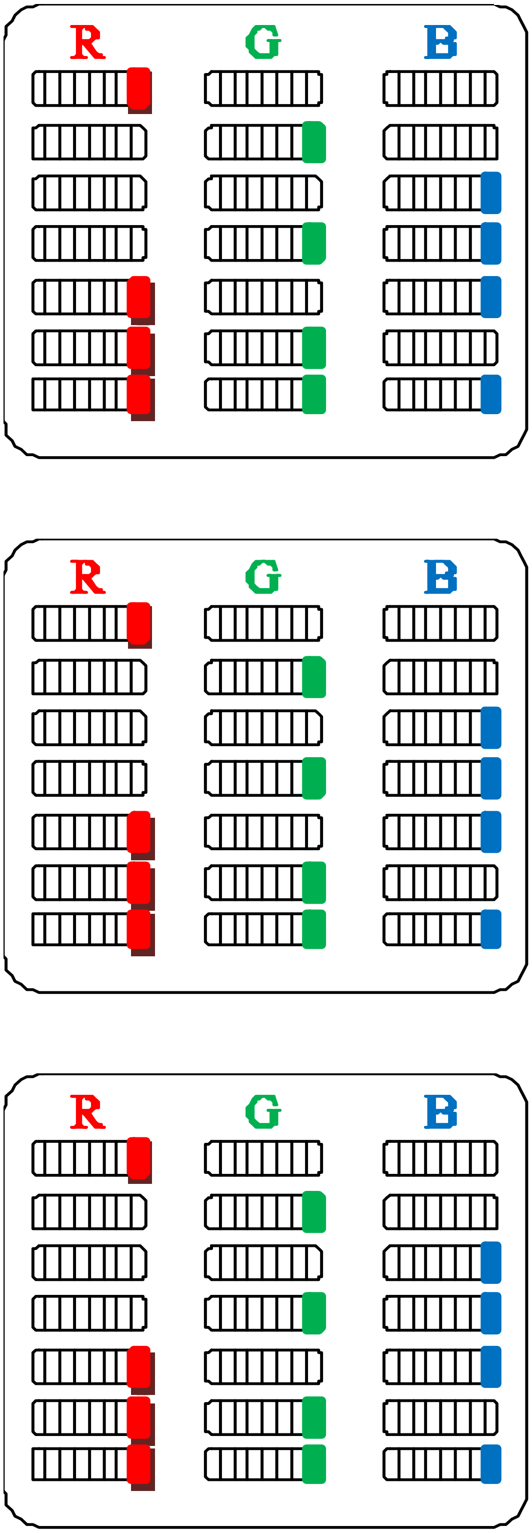

Figure 1. the possible way of encode the data using LSB algorithm.

principle of the logic design and repeats the process over the image. Irregular techniques might generate unlimited methods of steganography (Figure 3).

Therefore, we can always trust steganography more than other systems and that because of two reasons, first there are millions or maybe billions of the multimedia and non-multimedia resources available on the internet which can be use as a cover for data hidden, secondly it is not possible to recover the data from the stego-object unless we have the method of the encoding.

False positive images

Human eyes can distinguish teens gray scales for grey image. However for color image, the capability of human eyes is stronger than that of grey one. People can distinguish more than 13000 different colors by machine (Unser and Eden, 1989; Thai and Healey, 1999; Varma, 2004). Thus, the method of false color image composite is most commonly used for visual interpretation. Three grey images can combined into one color image which can show us more different objects features. The main weakness of ratio image is lost the reflection intensity information of ground objects. In order to remedy the deficiency, one origin band and two ratio images can be combined into one color image (Juna et al., 2008) (Figure 4).

Neural cryptography

ANN has many applications including function fitting, pattern recognition, and identification, classification, speech, vision and control systems as well as solving problems that are difficult for conventional computers or human being (Ardil and Sandhu, 2010; Celik, 2010; Xu et al., 2010), also, artificial neural network can simulate the function of human brain through learning mechanism (Gullu and Yilmaz, 2010; Tayi, 2010), in this paper the author has implement secure encryption method using ANN, the fallowing sections explains how this algorithm works.

Design of the proposed system

The encryption function includes three sub-functions: 1. Creating the keys. 2. Breaking the input message into blocks equal to the number of keys, the input message is processed one block at a time as input to the neural network. 3. The neural network (GRNN) is used to encrypt each block of data to produce the encrypted message.

In the following sub section, we will describe these three sub-functions.

Creating the keys: First we have to choose a super-increasing Knapsack with which to encrypt the data, the number of keys chosen is equal to N, so that:

1. The sum of these numbers (keys) must be less than 2x where x = 2N;
2. These numbers need not to be equal (K1 ≠ K2 ≠ …≠ Kn ≠ 0).

To keep it simple, in our simulation, we have objects of the following numbers (27, 14, 68) such that K1 = 68, K2 = 14, and K3 = 27, these will be the keys.

Breaking input data: Suppose M is some N-bit initial unipolar data [4], that is Mi = {-1, 1}, 0 ≤ i ≤ N – 1.

In this model a 3-bit plaintext is entered (N = 3) and an 8-bit cipher text is output 2N.

Now we need something to encrypt, for example 011010110. First we break it down into blocks (N = 3) which are the length of our Knapsack, so: 011 010 110. If we look at the first (011), there are 1's in the second and third positions. This means that we take

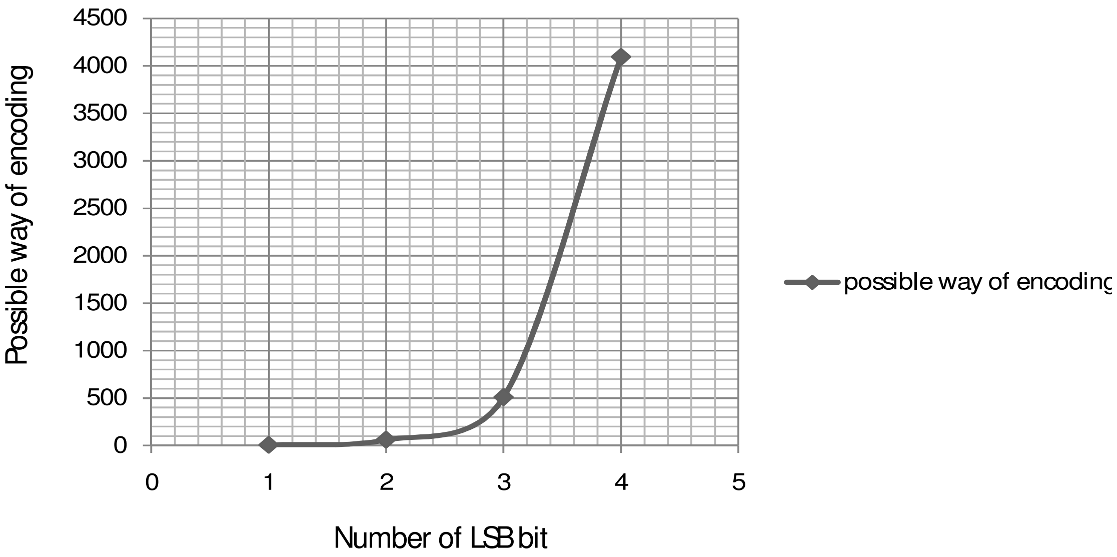

Figure 2. The relationship between the number of LSB bits and the number of the possible way to hide the data.

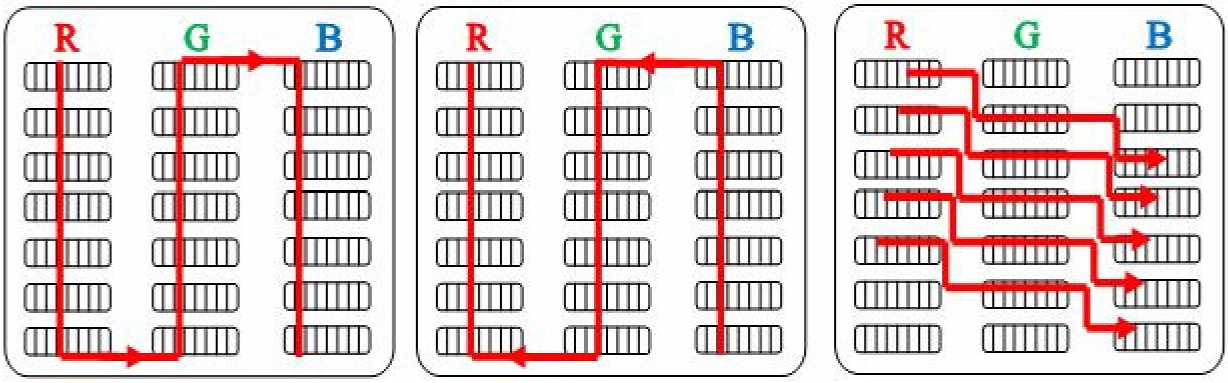

Figure 3. Irregular encodeingmethods using LSB algorithm.

the second and third keys and add them together: 0 + 14 + 68 = 82. Repeating this for all blocks of the input data. This gives us the encrypted version 01001000 as 82, as shown in Table 1. This encrypted data would then be transmitted to the recipient.

Proposed neural network-based crypto-system: A neural network is a structure (network) composed of a number of interconnect units (artificial neurons). Each unit has an input/output (I/0) characteristics and implements a local computation or function. The output of any unit is determined by its I/O characteristic, its interconnection to other units, and (possibly) external inputs [5].

In this paper, a simple one-parameter neural network model, general regression neural network (GRNN), proposed for encryption and decryption. The general regression neural network (GRNN) developed by Specht, is a simple yet very effective local approximation based on neural network in the sense of estimating a probability distribution function. The main advantages of GRNN are:

1. Fast learning; 2. Convergence to optimal regression surface as number of samples gets large; 3. Can be effectively used with sparse data; 4. Can handle non-stationary data.

GRNN uses a standard statistical formula for calculating the conditional mean Y of scalar random variable y given a measurement X of a vector random variable x. The vector random variable x corresponds to the input of the network and the random variable y corresponds to the output of the network. As well as being used as a static regression technique, GRNN can be used in situations where the statistics of the data changes over time. This is derived recently by specifying a time constant and a threshold. To build a GRNN:

1. Set the number of input, pattern, and output layer (PEs) (processing elements), 2. Choose the pattern unit, 3. Choose time constant and reset factor, 4. Set the radius of influence.

This is a simple clustering mechanism which assigns an input vector to a cluster if the cluster center is the nearest cluster center to the input vector AND is closer than the radius of influence. Otherwise, the input vector is assigned as the center of a new cluster (if possible).

The implementation of GRNN allows an exponentially decaying

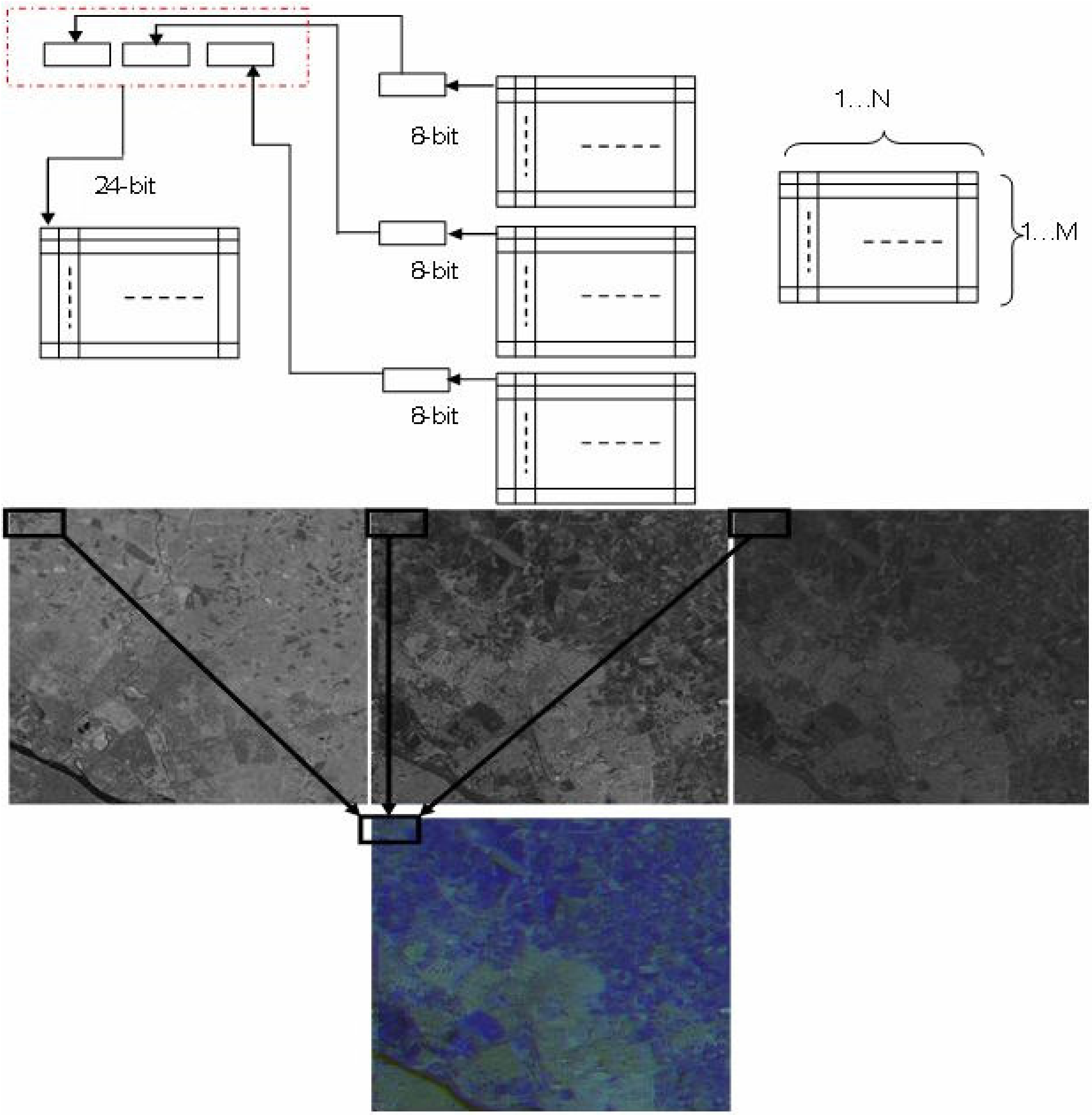

Figure 4. Three bunds of gray shots for the same area.

Table 1. The full pattern of training data sets.

Input			Output							
P_3	P_2	P_1	C_1	C_3	C_2	C_4	C_5	C_6	C_7	C_8
0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	1	0	0	0	1	0	0
0	1	0	0	0	0	0	1	1	1	0
0	1	1	0	1	0	1	0	0	1	0
1	0	0	0	0	0	1	1	0	1	1
1	0	1	0	1	0	1	1	1	1	1
1	1	0	0	0	1	0	1	0	0	1
1	1	1	0	1	1	0	1	1	0	1

Table 2. The half of full pattern of training data sets.

Input			Output							
P_3	P_2	P_1	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	1	1	1	0
1	0	0	0	0	0	1	1	0	1	1
1	1	0	0	0	1	0	1	0	0	1

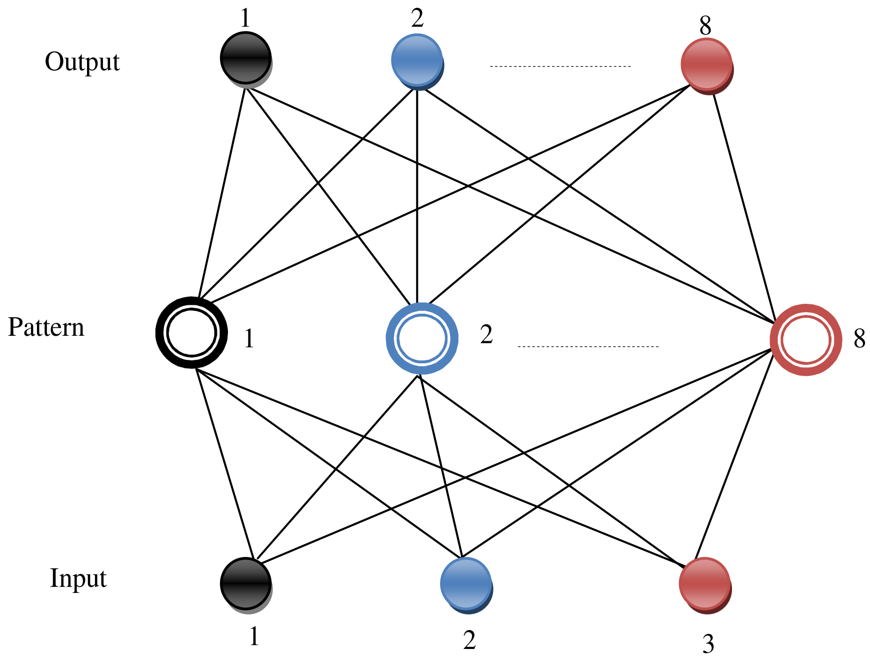

Figure 5. Three layered GRNN architecture.

sigma of the form:

Sigma = S/ (N^ (E/M),

Where N is the number of pattern units, M is the number of input PEs, and E must lie between 0 and 1. The problem we face is a computation problem, so we will use a multi-layer GRNN.

GRNN which is used for encryption consists of three layers. Each layer consists of a number of neurons which depends on the cases to be solved .In the encryption process, the input message is divided into 3 bit data sets, and 8 bit are produced after encryption process. The basic GRNN architecture is shown in Figure 1. Each layer consists of:

1. Input layer consisting of three nodes, which represents the N–bit blocks. 2. Pattern layer of eight nodes. 3. Output layer of eight nodes, used to define the decrypted output message.

The other parameters used with GRNN are:

1. Time constant = 1000.0; 2. Reset Factor = 0.000; 3. Radius of influence = 0.050; 4. Sigma scale = 1.000; 5. Sigma Exponent = 0.500. 6. A value of 0.5 for E is suitable under most circumstances. 7. A value of 0.0 for E allows using a constant value for sigma (equal to 5)

In order to study the behavior of the NNs, two set of training are used:

1. Full pattern of inputs which consists all possible inputs.
2. Half of the pattern mentioned above.

At the beginning of the learning the encryption key, GRNN fed with the valid states ,as shown in Table 1 for full pattern, and in Table 2 for half of the input pattern. The training set is repeatedly presented to the network and the weight values are adjusted until the overall error is below a predetermined tolerance. After the weight matrix is constructed, the network, is tested for encrypting (Figure 5).

RESULTS AND DISCUSSION

In order to evaluate the discussed mechanism, the encryption steps of a typical digital data are shown below.

Table 3. The encryption network results for full pattern of inputs.

Test data			Outputs							
P1	P2	P3	C1	C2	C3	C4	C5	C6	C7	C8
0	0	0	0.000000	0.018004	0.000325	0.017732	0.035753	0.035063	0.035109	0.018057
1	0	0	0.000000	0.982032	0.000325	0.017732	0.035753	0.964971	0.018050	0.018057
0	1	0	0.000000	0.018004	0.017733	0.000324	0.982373	0.947597	0.947279	0.018057
1	1	0	0.000000	0.982031	0.017733	0.982031	0.017733	0.052370	0.982031	0.018057
0	0	1	0.000000	0.018004	0.017699	0.964386	0.982407	0.018315	0.964703	0.982084
1	0	1	0.000000	0.982032	0.017699	0.964386	0.982407	0.981720	0.964391	0.982084
0	1	1	0.000000	0.018004	0.964455	0.017629	0.999678	0.034964	0.034907	0.982084
1	1	1	0.000000	0.982031	0.964455	0.017629	0.999678	0.965070	0.017945	0.982084

Ta**ble 4.** The encryption network results for half of full pattern of inputs.

Inputs								Outputs		
C1	C2	C3	C4	C5	C6	C7	C8	P3	P2	P1
0	0	0	0	0	0	0	0	0.098354	0.515655	1.000000
0	0	0	0	1	1	1	0	0.432734	0.432450	1.000000
0	0	0	1	1	0	1	1	0.766760	0.279187	1.000000
0	0	1	0	1	0	0	1	0.632379	0.842112	1.000000

We tested the behavior of the neural network described above, and we found that:

1. The neural network works probably in the case of using full pattern and absolutely no errors found in the outputs, this is shown in Table 3.
2. The neural network feel weak in the case of using half or part of the full patterns of the inputs, many errors found in the outputs which make the neural network fail to encrypt the input data; this is shown in Table 4.

Another test is done for the effect of the number of hidden units on the convergence of the model. The results of this test is shown in (Figure 2); Figure 2, demonstrates the variation of errors as a function of the number of neuron numbers in the hidden layer for encryption. The figure shows that the errors decrease widely but converge rapidly to zero in the case of having only 8 hidden neurons, which is indicate that the number of neurons in hidden layer must be equal to the number of neurons in the output layers (Figure 6).

In our testing data the 3 bit plaintext data is encrypted according to the keys, to 8 bit cipher data. Table 3 shows the encryption network results for full pattern of the inputs. This result shows that, the neural network works probably and absolutely no errors found in the outputs. For the half of full pattern of training data sets, many errors found in the outputs of the neural network which make it fail to encrypt the input data; this is shown in Table 4.

At the receiving terminal, the decryption process is the reverse of the encryption process. In order to decrypt the cipher data correctly:

1. The receiver must be uses the same numbers of the key to decrypt the data.
2. The data must have reached its intended receiver because only the receiver has the correct numbers of the key which are needed to remove the encryption.

The message must have been authentic, because only the sender has the numbers of the keys needed to encrypt the message so that receiver numbers of the key will correctly decrypt it.

Steganography

Different encoding has been applied in our experiment, as in the normal images, remote sensing has three gray level captions, we will consider the first gray level caption is “i”, the second gray level caption is “j” and the third gray level caption is “z” the multi-cover arranged as ijz, izj, jiz, jzi, zij and zji, the data has been encoded within the single cover irregularly as it has been explained previously. The author has benefited from the low sensitivity for the human eyes to the changes on the false color images to implement high rate and high secure data hidden using multi-cover remote sensing images and general recursion neural cryptosystem. This method can be applied with any false color image. In this experiment,

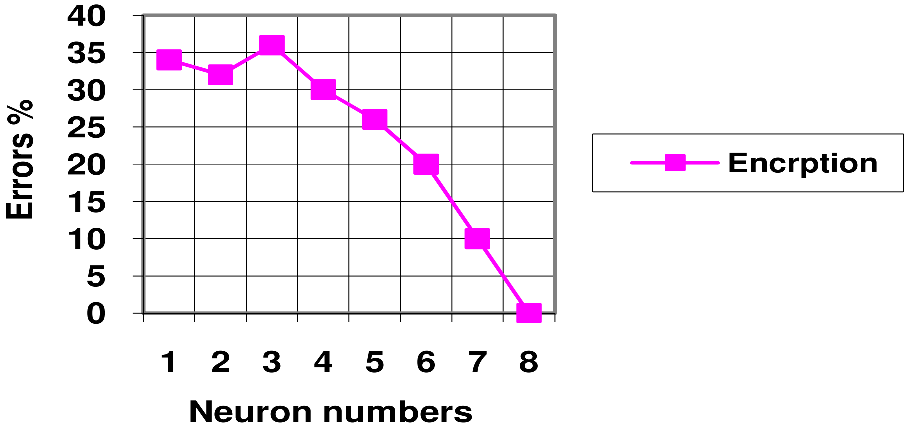

Figure 6. Error variations during training for encryption processes.

Table 5. Hardware performance.

Hardware	Performance
Land sat	5
Launch date	March 1, 1948
Carrier rocket	Delta 3920
Launch site	Vandenberg AFB SLC2W
Reference system	WRS-2
Type	Sun-synchronous, near polar
Altitude	705 km (438 mi)
Inclination	98.2º
Repeat cycle	16 days
Swath width	185km (115 mi)
Equatorial crossing time	9:45 AM +/- 15 min
Number of cycles to cover the earth	233
Type of sensors and number of bands	MSS/1,2,3,4 TM/1,2,3,4,5,6,7
Earth Recognition (meter)	79 m/ MSS 30/120 m /TM

we used remote sensing images taken from a satellite with the performance below.

Dataset

Dataset has been collected from remote sensing center at mosul. The data reception was 16 stations on the earth registered on the board satellite; the data has been recorded on high-density tape (CCT). The data is encoded in (8 bit numbers) (Lillesand et al., 1994), the scenes were taken in the region of Nineveh imagery Baltss TM (Thematic Map TM) stationed on the satellite Industrial 5 Landsat discriminatory capacity of 30 m and included the fallowing regions: Sheikh Ibrahim Mountain at Ba'shiqa center city of Mosul. The final scene of the valley of the red sea picked baltss TM stationed on Indian satellite IRS discriminatory capacity of 42 m (Al-Nuaimy, 2002) (Table 5).

During the research, only one limitation faced, this limitation is the dataset. Only three images provided from the source. Thus the authors forced to validate the new approach with testing the three images only (Figures 7 and 8).

Testing and result discussion

Regardless to (Kanvel and Monie, 2009; Ahmed et al., 2010) where the author mentioned that the peak signal-to-noise ratio (PSNR) and root mean square error (RMSE), signal-to-noise ratio (SNR) offer a more objective way to compare various algorithms' performance. However, these metrics have been widely criticised as well for not correlating well with perceived quality measurement (Girod, 1993; Teo and Heeger,

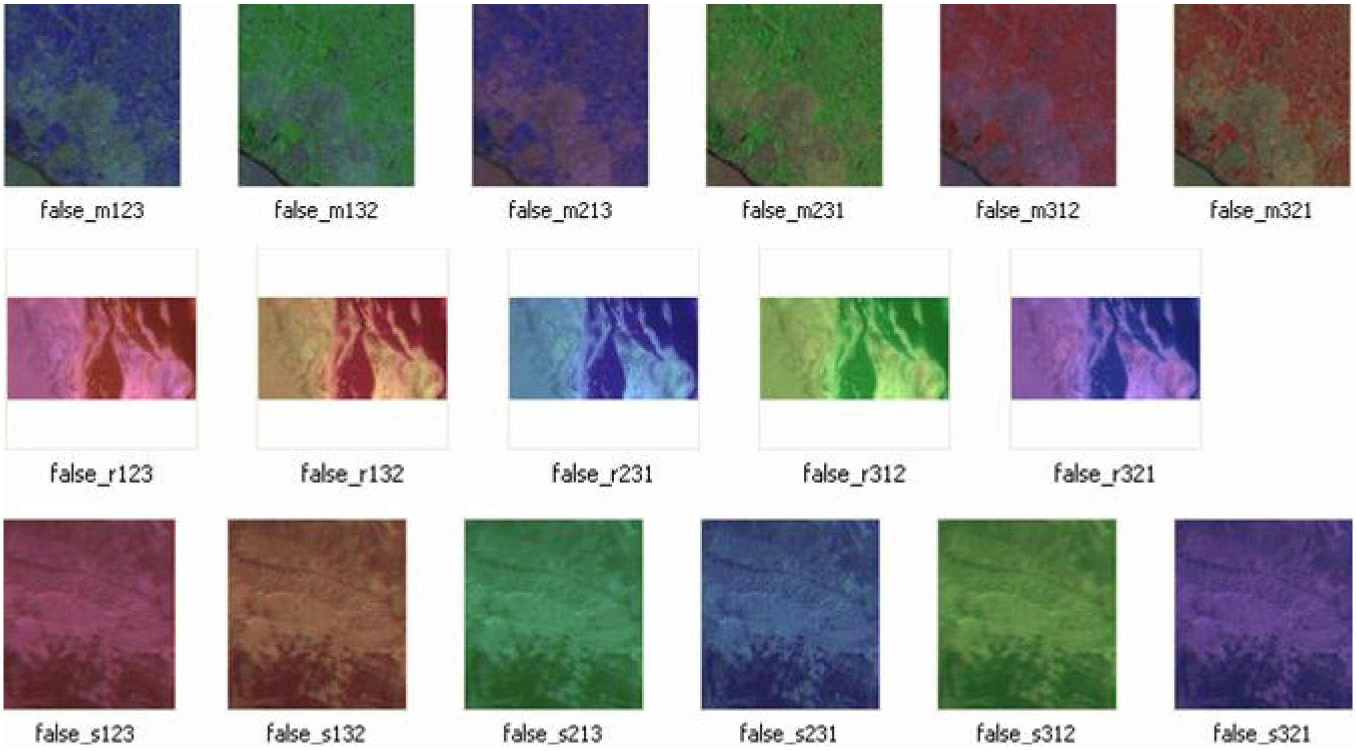

Figure 7. The false color image before hiding the data.

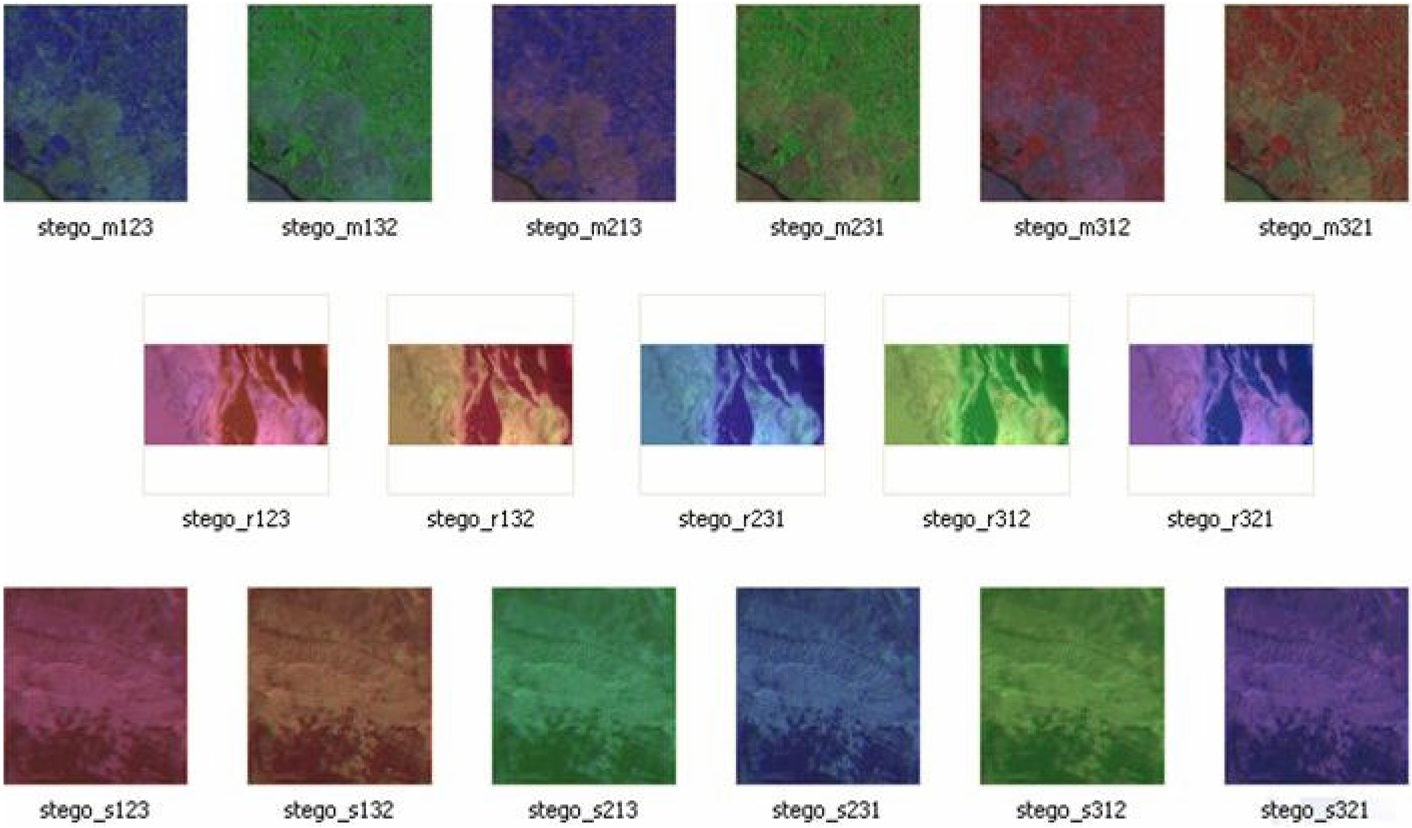

Figure 8. The false color image after hiding the data.

Table 6. Ten respondent's opinion on the output result.

Original image	Stego-image	U1	U2	U3	U4	U5	U6	U7	U8	U9	U10
false_m123.PNG	stego_m123.PNG	No	No	No	No	No	No	No	No	No	No
false_m132.PNG	stego_m132.PNG	No	No	No	No	No	No	No	No	No	No
false_m213.PNG	stego_m213.PNG	No	No	No	No	No	No	No	No	No	No
false_m231.PNG	stego_m231.PNG	No	No	No	No	No	No	No	No	No	No
false_m312.PNG	stego_m312.PNG	No	No	No	No	No	No	No	No	No	No
false_m321.PNG	stego_m321.PNG	No	No	No	No	No	No	No	No	No	No
false_r123.PNG	stego_r123.PNG	No	No	No	No	No	No	No	No	No	No
false_r132.PNG	stego_r132.PNG	No	No	No	No	No	No	No	No	No	No
false_r231.PNG	stego_r231.PNG	No	No	No	No	No	No	No	No	No	No
false_r312.PNG	stego_r312.PNG	No	No	No	No	No	No	No	No	No	No
false_r321.PNG	stego_r321.PNG	No	No	No	No	No	No	No	No	No	No
false_s123.PNG	stego_s123.PNG	No	No	No	No	No	No	No	No	No	No
false_s132.PNG	stego_s132.PNG	No	No	No	No	No	No	No	No	No	No
false_s213.PNG	stego_s213.PNG	No	No	No	No	No	No	No	No	No	No
false_s231.PNG	stego_s231.PNG	No	No	No	No	No	No	No	No	No	No
false_s312.PNG	stego_s312.PNG	No	No	No	No	No	No	No	No	No	No
false_s321.PNG	stego_s321.PNG	No	No	No	No	No	No	No	No	No	No

1994; Eskicioglu and Fisher, 1995; Wang, 2001; Wang and Bovik, 2002; Wang et al., 2002a; 2003, 2004; Lee et al., 2006). According to Hmood et al. (2010c) the well-known objective metrics (that is, PSNR, SNR, MSE and RMSE) is not functional. Hmood et al. (2010b) has explain how bad are these metrics, especially for steganography and digital watermarking; they provide evidences from more than 50 scholar papers to support this finding. Thus the author has choice the subjective test to evaluate the method output. Ten users has been asked if they found any manipulation on the images after the data has been hided, the answer was no for the entire sample, this means that, remote sensing image is perfect to be undetectable cover for steganography. The table depicted ten respondent's opinion (Table 6).

Considering the success factor of having a secure steganography approach is that, the added noise (that is, data hidden) is not visible. In this case we can say that, the new approach succeed on having undetectable data hidden, in addition to that, the data itself has been secured before hiding it using GRNN cryptosystem, while another level of security has been applied by distributing the data hidden irregularly over the cover file. In nutshell, we recommend using, neural network cryptosystems to generate non-standard encryption method for the purpose of securing the data over the unsecure transmission, moreover, implementing any steganography approaches within the false color images (that is remote sensing images) shall be successes due to the feature of the false image which have been explained above. Finally, irregular encoding within the cover file can prevent several kinds of attackers such as known-cover attackers.

Conclusion

Steganography is defined as the art of concealing a sensitive data through other carrier to insure the confidentiality of the data carrier to insure the confidentiality of the data. Multi-cover steganography has designed and implemented successfully, this new concept might open a wide areas on steganography, the new approach are robust, and undetectable to the human eyes, and overcome the problem of the distortion that happening on simple texture when we try to increase the amount of data hidden. In this research GRNN cryptosystem has been designed and implemented to defeat the problem of exchange cryptography keys through the network, the new cryptosystem exchange the keys through trine the neural network data which later on used to decrypt the data, this powerful cryptosystem has been merged with the multi-cover to produce confidentiality and integrity for data hidden.

ACKNOWLEDGEMENTS

This research has been funded partly by the University of Malaya under No. UM.C/625/1. The authors would also like to acknowledge Multimedia University as the co-founder for this project.

REFERENCES

Abomhara M, Khalifa OO, Zakaria O, Zaidan AA, Zaidan BB, Alanazi HO (2010). "Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview." J. Appl. Sci., 10(15): 1656-1661.

Ahmed MA, Kiah MLM, Zaidan BB, Zaidan AA (2010). "A Novel Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm." J. Appl. Sci., 10(1): 59-64.

Alanazi HO, Jalab HA, Zaidan BB, Zaidan AA, Alam, Gazi M (2010). "Securing Electronic Medical Records Transmissions over Unsecured Communications: An Overview for Better Medical Governance." J. Medicinal Plants Res., 4(19): 2059-2074.

Al-Frajat AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010). "Hiding Data in Video File: An Overview." J. Appl. Sci., 10(15): 1644-1649.

Al-Nuaimy KS (2002). Construction of a proposed system of Multiple Classification of Remotely Sensed Data. Remote Sensing Center. Mosul, Iraq, University of Mosul. M.Sc.

Ardil E, Sandhu PS (2010). "A soft computing approach for modeling of severity of faults in software systems." Int. J. Phys. Sci., 5(2): 074-085.

Azmi AAC, Kamarulzaman Y (2010). "Adoption of tax e-filing: A conceptual paper." Afr. J. Bus. Manage., 4(5): 599-603.

Celik CT (2010). "Performance of ANN in determination of unstable points in leveling networks." Int. J. Phys. Sci., 5(5): 401-407.

Dobsicek M (2004). Extended steganographic system. 8th International Student Conference on Electrical Engineering.

EL-Emam NN (2007). "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" J. Comput. Sci., 4(3): 223-232.

Eskicioglu AM, Fisher PS (1995). "Image quality measures and their performance." IEEE Transactions on Communications, 43(12): 2959-2965.

Everett CE (2005). Bridging the gap between computer security and legal requirements. Workshop on the Economics of Information Security, pp. 1-21.

Girod B (1993). What's wrong with mean-squared error? Digital images and human vision, MIT Press, pp. 207-220.

Gullu M, Yilmaz I (2010). "Outlier detection for geodetic nets using ADALINE learning algorithm." Sci. Res. Essays, 5(5): 440-447.

Hashim F, Alam GM, Siraj S (2010). "Information and communication technology for participatory based decision-making-E-management for administrative efficiency in Higher Education." Int. J. Phys. Sci., 5(4): 383-392.

Hmood AK, Jalab HA. Kasirun ZM, Zaidan BB, Zaidan AA (2010b). "On the capacity and security of steganography approaches: An overview." J. Appl. Sci., 10(16): 1825-1833.

Hmood AK, Kasirun ZM, Jalab HA, Zaidan AA, Zaidan BB, Alam GM (2010c). "On the Accuracy of Hiding Information Metrics: Counterfeit protection for education and important certificates." Int. J. Phys. Sci.,

Hmood AK, Zaidan BB, Zaidan AA, Jalab HA (2010a). "An overview on hiding information technique in images." J. Appl. Sci., 10(18): 2094-2100.

Jahangir N, Begum N (2008). "The role of perceived usefulness, perceived ease of use, security and privacy, and customer attitude to engender customer adaptation in the context of electronic banking." Afri. J. Bus. Manage., 2(1): 032-040.

Juna L, Songweic C, Duanyoua L, Bina W, Shuod L, Liminga Z. (2008). "Research on false color image composite and enhancement methods based on ratio images." The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. XXXVII(Part B7).

Kanvel N, Monie EC (2009). "Adaptive lifting based image compression scheme for narrow band transmission system." Int. J. Phys. Sci., 4(4): 194-164.

Lee C, Cho S, Choe J, Jeong T, Ahn W, Lee E (2006). "Objective video quality assessment." Optical engineering, 45: 017004.

Lillesand TM, Kiefer RW, Chipman JW (1994). Remote sensing and image interpretation, John Wiley and Sons New York.

Lu CT, Huang SY, Lo PY (2010). "An empirical study of on-line tax filing acceptance model: Integrating TAM and TPB." Afr. J. Bus. Manage., 4(5): 800-810.

Mittal U, Phamdo N (2002). "Hybrid digital–analog (HDA) joint source–channel codes for broadcasting and robust communications." IEEE Transactions on Information Theory, 48(5).

Mondéjar J, Juan A, Mondéjar JJ, Ángeles M, Zurilla C (2009). "E-commerce and legal protection for consumers: Spanish analysis." Afr. J. Bus. Manage., 3(9): 426-432.

Naji AW, Zaidan AA, Zaidan BB (2009). "Challenges of Hidden Data in the Unused Area Two within Executable Files." J. Comput. Sci., 5(11): 890-897.

Pavan S, Gangadharpalli S, Sridhar V (2005). Multivariate entropy detector based hybrid image registration algorithm. IEEE International Conference on Acoustics, speech and Signal Processing

Petitcolas FAP, Anderson RJ, Kuhn MG (1999). "Information hiding-a survey." Proceedings of the IEEE, 87(7): 1062-1078.

Shimanovsky B, Feng J, Potkonjak M Eds. (2003). Hiding data in DNA. Information Hiding. Heidelberg, Springer.

Stevens G (2009). Federal Information Security and Data Breach Notification Laws, Library of Congress Washington Dc Congressional Research, Service.

Stevens GM, Attorney L (2007). Information Security and Data Breach Notification Safeguards, Library of Congress Washington DC Congressional Research Service.

Tayi N (2010). "Application of Neural Network models on analysis of prismatic structures." Sci. Res. Essays, 5(9): 978-989.

Teo PC, Heeger DJ (1994). Perceptual image distortion. Proceedings of the SPIE, Citeseer.

Thai B, Healey G (1999). "Spatial filter selection for illumination-invariant color texture discrimination." Computer Vision and Pattern Recognition, 2(6): 23-06.

Unser M, Eden M (1989). "Multiresolution feature extraction and selection for texture segmentation." IEEE Transactions on Pattern Analysis and Machine Intelligence, 2(7).

Varma M (2004). "Unifying statistical texture classification frameworks." Image and Vision Computing, 22: 1175-1183.

Wang Z (2001). Rate scalable foveated image and video communications, PhD thesis, Dept. of ECE, The University of Texas at Austin.

Wang Z, Bovik AC (2002). "A universal image quality index." IEEE Signal Processing Letters 9(3): 81-84.

Wang Z, Bovik AC, Lu L (2002a). Why is image quality assessment so difficult?, IEEE; 1999.

Wang Z, Lu L, Bovik AC (2004). "Video quality assessment based on structural distortion measurement." Signal processing: Image communication 19(2): 121-132.

Wang Z, Sheikh HR, Bovik AC (2003). "Objective video quality assessment." The Handbook of Video Databases: Design and Applications, pp. 1041–1078.

Xu H, Hu Y, Chen Y (2010). "A novel 3D spatial neighbor points coupling surface modeling method for scattered points." Int. J. Phys. Sci., 5(4): 313-320.

Zaidan AA, Zaidan BB, Alanazi OH, Gani A, Zakaria O, Alam GM (2010a). "Novel Approach for High (Secure and Rate) Data Hidden within Triplex Space for Executable File." Sci. Res. Essays.

Zaidan AA, Zaidan BB, Al-Fraja AK, Jalab HA (2010b). "Investigate the Capability of Applying Hidden Data in Text File: An Overview." J. Appl. Sci., 10(17): 1916-1922.

Zaidan AA, Zaidan BB, Al-Frajat AK, Jalab HA (2010c). "An Overview: Theoretical and Mathematical Perspectives for Advance Encryption Standard/Rijndael." J. Appl. Sci., 10(18): 2161-2167.

Zaidan BB, Zaidan AA, Al-Frajat AK, Jalab HA (2010d). "On the Differences between Hiding Information and Cryptography Techniques: An Overview." J. Appl. Sci., 10(15): 1650-1655.

Zaidan BB, Zaidan AA, Taqa A, Othman F (2009). "Stego-Image Vs Stego-Analysis System." Int. J. Eng. Technol. (IJET), 1(5): 596-602.