International Journal of the Physical Sciences Vol. 5(11), pp. 1796-1806, 18 September, 2010
Available online at http://www.academicjournals.org/IJPS
ISSN 1992 - 1950 ©2010 Academic Journals

Full Length Research Paper

StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem

B. B. Zaidan[1], A. A. Zaidan[1], Alaa Taqa[2], Gazi Mahabubul Alam[3]*, M. L. Mat Kiah[2] and A. Hamid Jalab[2]

[1]Faculty of Engineering, Multimedia University Jalan Multimedia, 63100 Cyberjaya, Selangor, Malaysia.
[2]Faculty of Computer Science and Information Technology, University Malaysia, 50603, Kuala Lumpur, Malaysia.
[3]Department of Educational Management, Planning and Policy, Faculty of Education, University of Malaya, 50606 Kuala Lumpur, Malaysia.

Accepted 31 August, 2010

This paper discusses a secure novel approach of high rate data hidden using mosaic image and bitmap (bmp) cryptosystem. The mosaic image used in this approach together with the neural cryptosystem that have been implemented for the first time and has been successful, this new method of hiding data is based on LSB in mosaic images. A mosaic is an image that is comprised of hundreds or thousands of other images to create one common image. The proposed approach is named "StegoMos". Once the mosaic cover is chosen, then data is secured by the crypto-system which is used to encrypt the data before hiding. The crypto-system is based on BAM neural network. The importance of neural networks in this work is that they offer a very powerful and a very general framework for representing non-linear mapping from several input variables to several output variables. Merging high rate data hiding in mosaic images as well as making the data secure arises from the requirements of the problem of increasing the amount of data hidden and at the same time maintains the quality of image. The second requirement is the security of data. Experimental results show the effectiveness of using the mosaic image cover over the normal image.

Key words: Mosaic image, high rate data hiding, steganography and data hidden, data security using neural networks, BAM neural networks.

INTRODUCTION

Nowadays, the applications of security are wide; the term security presented in the scholar papers side by side with terms: Confidentiality, integrity, authenticity, non-repudiation, privacy and data protection. Sometime it has beyond that to present the privacy statements for surveys and interviews. It may not be exaggerating if we say e-life equal to security, researcher state many words on the role played by security in life. Haque et al. (2009) and Qabajeh et al. (2009) says "only protected transaction, have significant impact on consumers' perception about e-banking security, Hashim et al. (2010) said "Privacy and security are very important issues being discussed in the literature on the current use of ICT". According to Abomhara et al. (2010), Alanazi et al. (2010) and Hashim et al. (2010) privacy, copyright and security are very important issues. A mosaic image is an image which consists of hundreds or thousands of other images. A mosaic is created with a set number (specified by the user) of mosaic pieces wide and high with each piece being of the same size. The image that is part of a mosaic will be called a mosaic piece. Creating a mosaic image needs a database of hundreds of images; all of the images have the same size. When an image is created into a mosaic piece it is reduced in size appropriately to

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

fit with the size of that section. Each of the mosaic pieces resembles a section of the overall mosaic image. The size of mosaic is non-standard. according to one of the online Galleries, they publish mosaic image with size 324 MB, 12.000 * 9.000 pixels (Dali, 2009), other example has exceed the 9.4 Gigabytes with number of pixels: 3,366,400,000 (Gogh, 2010). This variation in size made the mosaic image as the best choice in term of, mosaic image has wide size range; this feature made the suspect of the availability of steganography in the mosaic image less comparing with the normal images. Hidden information in the cover data is known as the "embedded" data. The "stego" data is the data containing both the cover signal and the "embedded" information. The process of putting the hidden or embedded data into the cover data is sometimes known as embedding while splitting the embedded information from the cover is called "extracting". Though data can be hidden or embedded, an attacker could still steal these hidden statements or break it. Usually, people would hide their data in a multimedia files such as an image or video file. This can be done using many tools in the market. The concept of hiding data into multimedia files becomes very popular and it is no longer secret to the attacker. They can simply find out the file and extract the data out from it. Besides that, as for the user, there are some limitations in terms of the size of file that can be hidden.

Research aims and objectives

Data hidden is a general word for two techniques, Steganography and Digital Watermarking (Zaidan et al., 2010b). According to Hmood et al. (2010b, a), data hidden approaches are suffering from the limitation of the size. This research tries to achieve the following objectives:

1. To study the features of mosaic images that help to apply the data hiding
2. To investigate the capabilities of applying huge data within the mosaic image
3. To design and implement a cryptography algorithm based on BAM neural network.
4. To implement a gathering approach based on the analysis of mosaic image, and BAM neural cryptosystem

Research questions

Implementing a new approach of steganography or digital watermark needs to analyze the limitation of recent approaches. Thus, this research tries to spot the light and answer the following questions:

1. According to Abomhara et al. (2010) and Zaidan et al. (2010a), unlike Asymmetric cryptography, Symmetric cryptography, in the most cases is the only suitable cryptosystem. The question is: Is there any other cryptosystems that can be applied on multimedia files?
2. Increasing the amount of data hidden within the multimedia file might affect the texture of image, video frame, and the signal of audio, therefore, the cover of data hiding would be affected and the distortion would be visible (Al-Frajat et al., 2010). The question is: Is there any type of multimedia files, where increasing the amount of data hidden might not be visible?
3. Steganography can not stand alone (Zaidan et al., 2010c); the question is: Is having a hybrid approaches (that is consists of steganography and cryptography) worthy?
4. Do you trust the metrics used to evaluate the steganography object?

Problem and discussion

Hiding data in image is the most popular known application for the LSB algorithm. In our previous research paper, we have discussed in details how to implement LSB method in the image. In the same paper, we have shown an enhanced LSB encoding and it uses 4 LSB layers which mean we may embed 50% from the size of the cover file. Four layers according to the LSB method might affect the texture of the images. The data security problem is considered here as the problem of keeping the hidden data in both normal images and mosaic images private and secure. In this paper, an efficient technique for data security is presented by using Bidirectional Associative Memory (BAM) neural networks. The decryption scheme used in this work is based on a multi keys super-increasing Knapsack technique based on BAM neural network.

Literature review

In the field of image-base steganography, several approaches have been implemented and the authors would like to enumerate the well known image-based approaches. In Por et al. (2008), they combine three steganography algorithms on GIF image through StegCure system. Furthermore, the unauthorized user is forbidden from intercepting the transmission of the covert data during a communication because of the PKI involved on this approach. In Zaidan et al. (2009b), the author tried to test the largest amount of data that might be hidden in the image using pure steganography. The result was good and the author succeeded in hiding data amounting to 50% of the size of the images with a condition that “no flat area from the same color” or what we so-called simple texture.

In Zaidan et al. (2009a, b), the relation between the quality of Image and quantity of data hidden in the Image

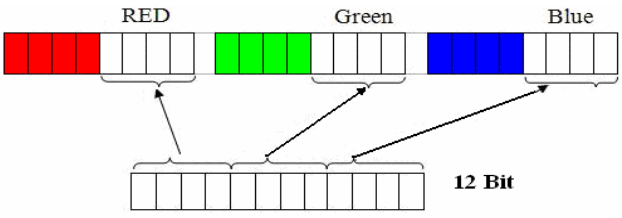


Figure 1. One pixel from 24-bit image.

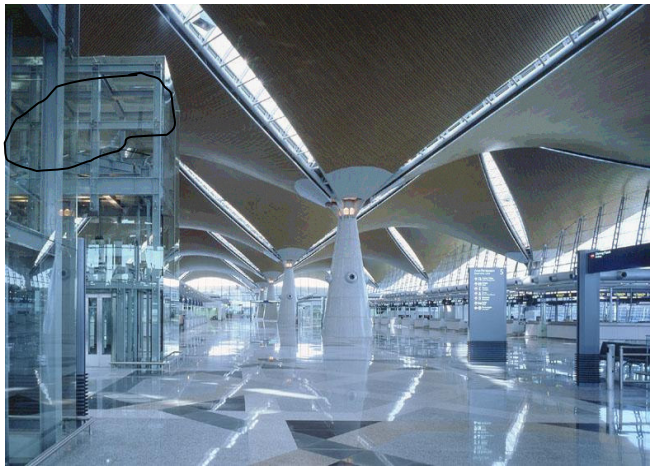


Figure 2. Image after hidden data shows the black curve surrounding the distorted region.

was described by using the human vision system and pure Steganography. The main purpose of this paper is to evaluate the effect of increasing the size of the data and the quality of image which focused on the property of human vision system that helps to increase the amount of data hidden in the bitmap (bmp) image.

MATERIALS AND METHODS

Four LSB layer

Increase in the amount of data hidden in the 24-bit is experimentally shown in the fourth LSB layer. As depicted in Figure 1, the image distortion clearly appeared and the reason behind this distortion was the simple texture in the images (Figure 2).

Let $I = \{Xi\ ,\ i \in \Omega\}$

Where Ω is an index set denote the mean subtracted cover image. The set Ω can be partitioned into three subsets A 1, A2, and A3, where, $\Omega = \cup_{i=1}^{3} Ai\ Ai \text{ and } Ai \cap Aj = \emptyset \text{ for } i \neq j$ Then, the pixel values in a LSB based stego-image $I\,s = \{Yi\ ,\ i \in \Omega\}$ can be represented as:

$$Yi = \begin{cases} Xi + S, S\epsilon\{1,2\ldots.,15\} & if\ i\epsilon A1 \\ Xi - S, S\epsilon\{1,2\ldots.,15\} & if\ i\epsilon A2 \\ Xi & if\ i\epsilon A3 \end{cases} \quad (1)$$

After applying four LSB Layer

According to Zaidan et al. (2009b), these areas containing large tracts of contiguous excerpts have the same value. This distortion fades slowly and heads towards smooth texture areas. This becomes very sensitive to the color change especially when the level of colors in flat spaces occurs with less sensitivity. As the process of concealment here applies to all parts of the picture equally, the success of this process requires that the image selected as cover verify the requirement above negative for the presence of any region with an area of flat color.

There are several ways to determine the smooth texture and the noisy texture and this is beyond the scope of this study. To calculate the smooth texture, the mathematics Equations 2 and 3 are used:

Let $P = \sum_{n=1}^{i} \sum_{k=1}^{j} Pi$ (2)

N = {1,2,…..,j} width, K = {1,2,…….,j} length

Let $W = \sum_{z=1}^{g} \sum_{x=1}^{g} Pi$ (3)

And let

$$P = \begin{bmatrix} x1,1 & x1,2 & \ldots\ldots & x1,j-1 & x1,j \\ x2,1 & x2,2 & & x2,j-1 & x2,j \\ \vdots & \vdots & \ddots & \vdots & \\ xi-1,1 & xi-1,2 & \ldots\ldots & xi-1,j-1 & xi-1,j \\ xi,1 & xi,2 & & xi,j-1 & xi,j \end{bmatrix}$$

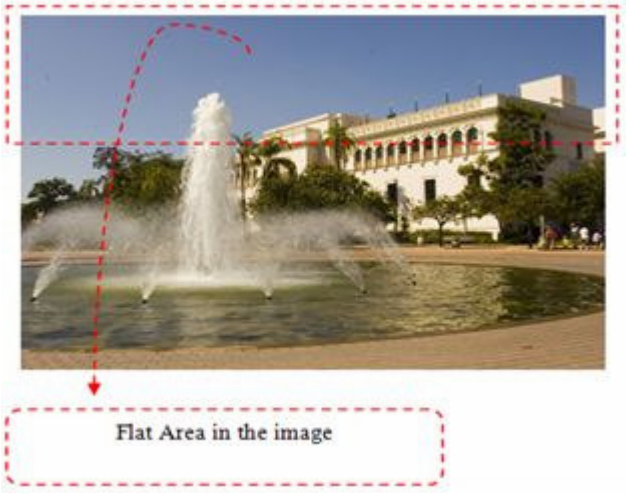


Figure 3A. Appoint the flat areas in the image.

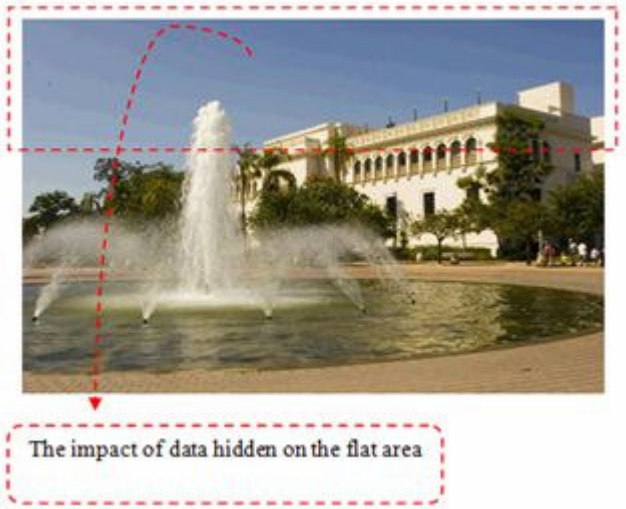


Figure 3B. Depicted the areas that had beeneffected by increasing amount of data hidden.

Let W = $\begin{bmatrix} y1,1 & y1,2 & \dots & y1,8 \\ y2,1 & y2,2 & \dots & y2,8 \\ \vdots & \vdots & \dots & \vdots \\ y8,1 & y8,2 & \dots & y8,8 \end{bmatrix}$

Here, we use the window sliding technique to understand in the matrix and how we can classify the image into smooth and complex texture. The final formula becomes:

$$ST = \sum_{e=1}^{j-7} \sum_{r=1}^{i-7} Ch \quad (4)$$

Ch = F (W) check function on the matrix W. After extracting the 8*8 pixel from the image, then the pixels on this matrix should be not be equal or at least not near to each amount of color. The image in Figure 3A involve a flat area bounded by red color; this areas if the high rate data hidden is applied, the result will not exceed the 33.3%, simple texture and complex texture explained in Figures 3A and B. Up to the 4-bit data hid the distortion in the flat areas being clear as shown in Figure 3B. Figure 4 show the Pseudo-code of the new approach.

Mosaic creation

The mosaic creation algorithm is a straight forward way of creating a mosaic. This algorithm is used with an image the mosaic is supposed to resemble (that is the original image), a large collection of images (mosaic pieces) and two integers that tell how many images wide and high the mosaic is to be. The first task the algorithm performs is to read in the original image and the mosaic pieces to memory. Each of these images read in are stored as a PicPixels object. The original image is then broken down into sections corresponding to the size of a mosaic piece as depicted in Figure 5. Then, each section is compared to all of the mosaic pieces to find the piece with the least difference. The example

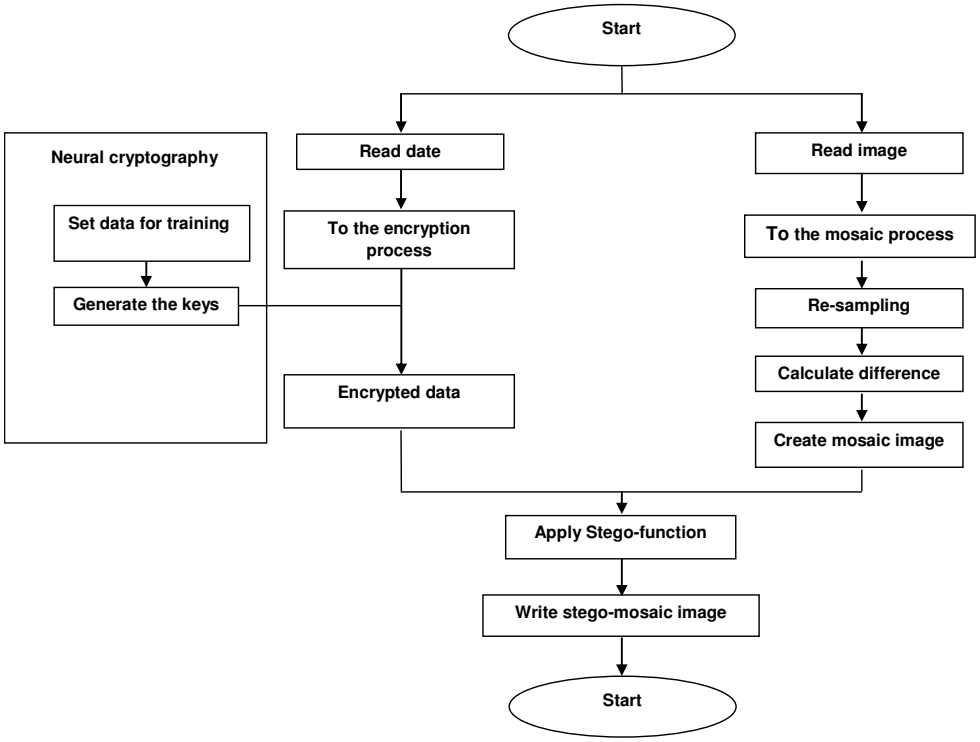


Figure 4. Pseudo-code of the four LSB layer approach.

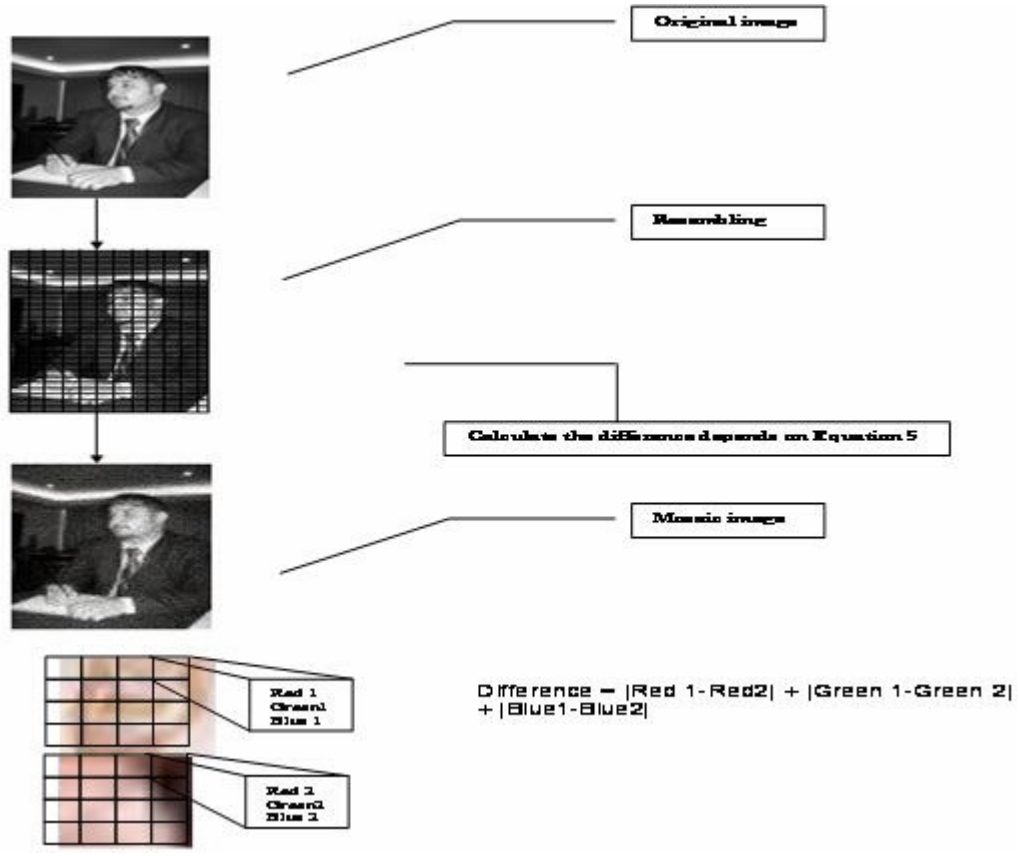


Figure 5. Convert the normal image into mosaic image.

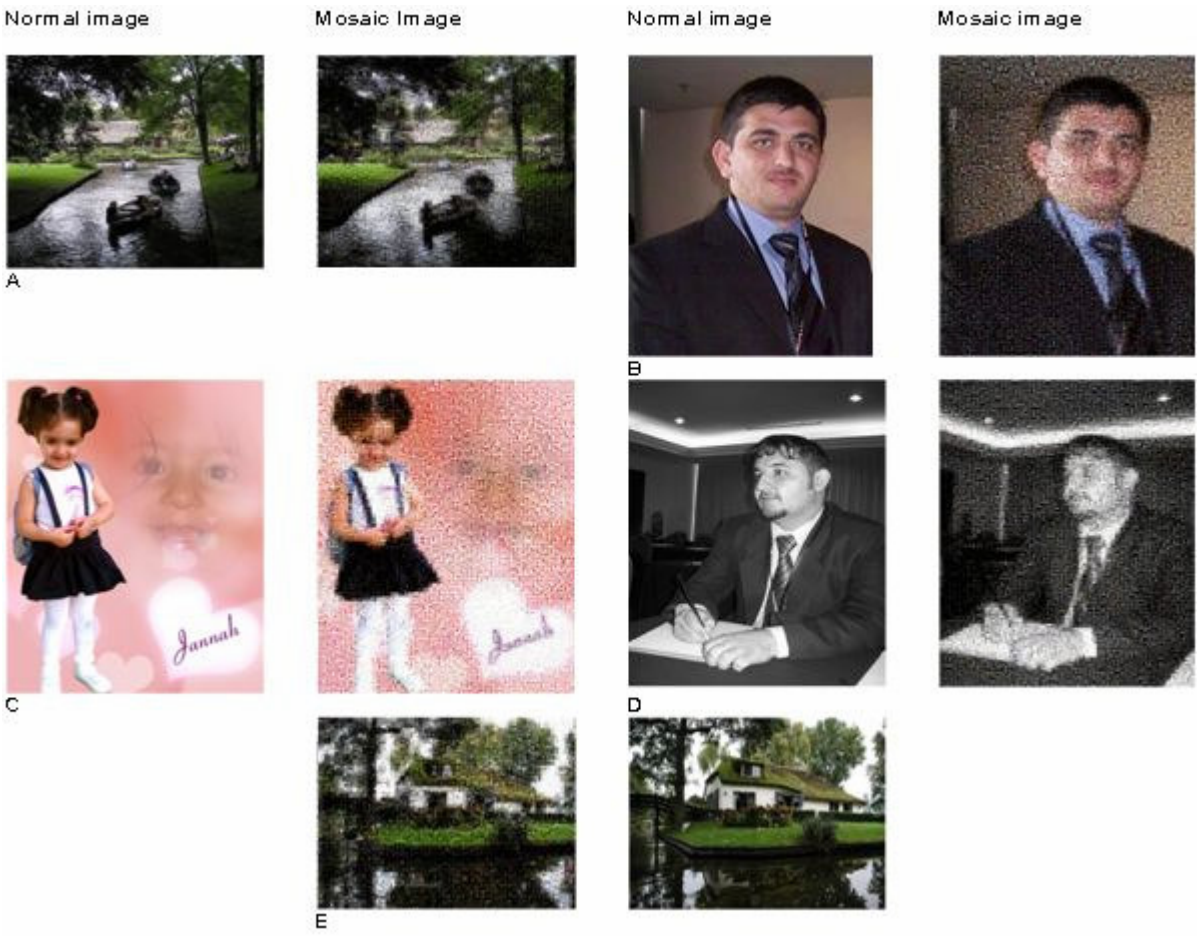


Figure 6. The selected (that is, normal and mosaic) images for tests.

showing one section of the original image compared to a collection of mosaic pieces is given as:

Difference = |Red 1-Red2| + |Green 1-Green 2| + |Blue1-Blue2|

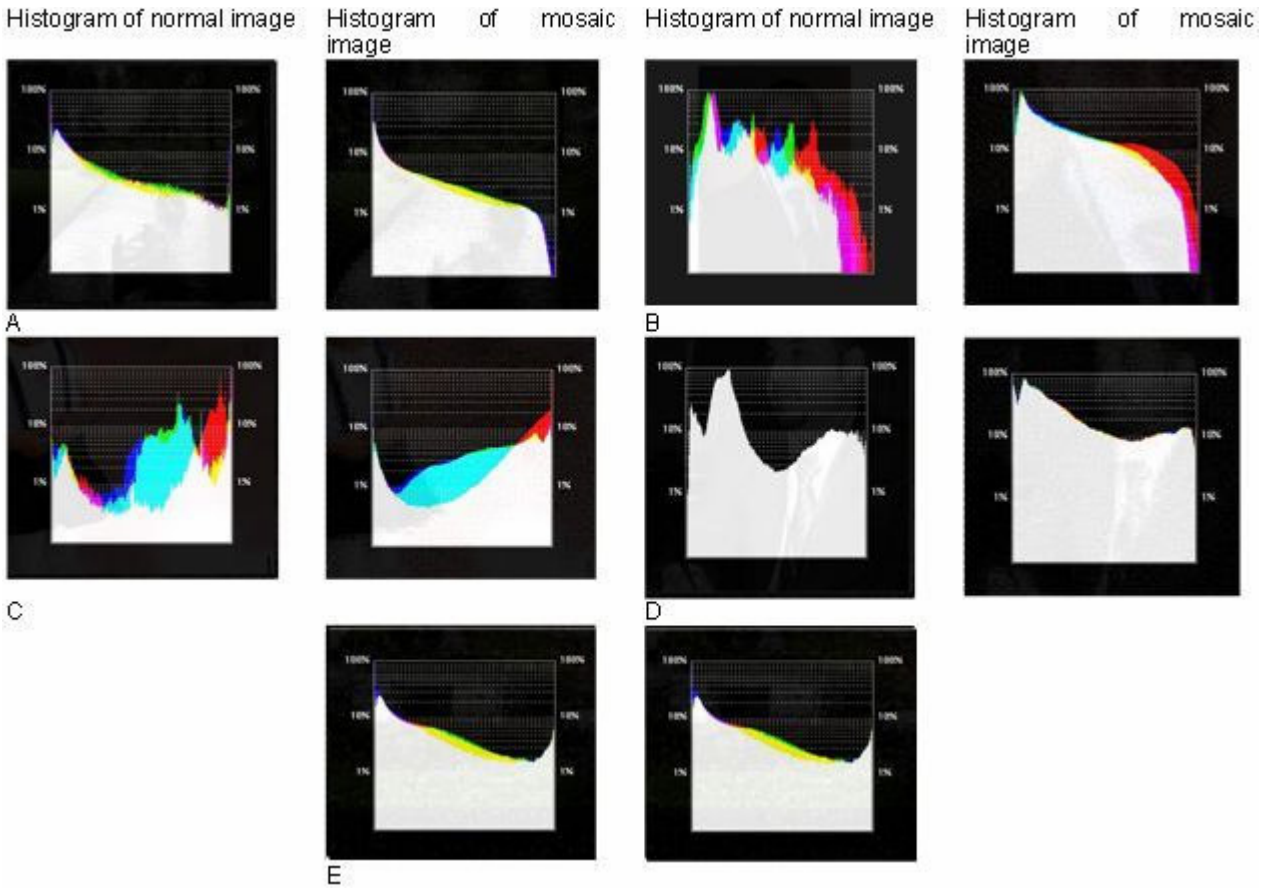
Choosing the best mosaic piece for each section of the original image has two options. The first option is to allow an image to be used more than once. In this method when a mosaic piece is found to be the best match for that section, then it is selected and assigned to that section. It is then placed back into the pile of mosaic pieces so that it can be chosen again. The other option is to disallow duplicate images in the mosaic. With this option, when a mosaic piece is selected, it is not placed back into the pile and therefore it will not be selected again. This option is only possible if the user provides as many images as there are sections in the mosaic being created.

Figure 6 is a sample of five selected images; each image has been taken for particular test. Figure 6 A and E are two images for landscape. Figure 6B and D are two images taken from different camera belonging to different persons; Figure 6C is a high resolution color image, the distinguish property of this image is that, it is a multi-layer image created using Photoshop, in the test of high rate data hidden, these images present a weak cover for data hidden and that because, the images include a wide simple texture area in the image. Unlike the landscape images which contain complex texture on the image, the test depicted the success of the high rate data hidden test.

In this stage, the author has converted the images from normal images into mosaic. Both images “the natural images and the convert images” will be involved in the test to generate the data for comparative study between the new types of covers that is “mosaic cover” and the old type “normal images”. This is done for the purpose of evaluating the new approach. Figures 6 to 9 shows the image histogram before and after converting to mosaic images.

In the second stage we will hide the data in both “normal images and mosaic images” and compare the new approach with the old approach, regarding to measurements metrics, the author will use the histogram to depicts the differences between the images before and after hiding the data. Most of the Steganography approach has been tested using PSNR, SNR, MSE and RMSE, Regardless to (Kanvel and Monie, 2009) where the author mentioned that the peak signal-to-noise ratio (PSNR) and root mean square error (RMSE) offer a more objective way to compare various algorithms’ performance. However, the metrics have been widely criticised as well for not correlating well with perceived quality measurement. According to Hmood et al. (2010c) the well-known objective metrics (that is PSNR, SNR, MSE and RMSE) is not functional

Figure 8 tests the images under the four layers LSB. Two tests have been applied in this experiment. The first test was done on the image before it had been converted to mosaic image and the second test has done on the mosaic images after it was converted from the original image. The reason of the first test is to have an extensive data towards a comparison study. Figures 8A and E depicted the successful work of the algorithm in both (that is, the



Figures 7A - E. The histogram of the normal images and the images after converting to mosaic images.

original image and the mosaic image) because both images have not included simple areas. While in Figures 8 B and D shows no success for normal image because both included simple texture. Figure 8 C has been affected in the normal test, although the mosaic test for the same image showed that the new cover is successful in hiding data for the same reason as in Figures 8 A and E. All images in the selected samples showed a good result for the mosaic images, while the normal images in three samples failed to be a good cover for data hidden.

Figure 9 compares the histogram of a normal image after the high rate data hidden and the same test on the mosaic image for the same images. Each of the images in Figure 9A to G represents the histogram of the images sorted as in Figure 8A to G.

The image depicted in Figure 10 shows a part of the distortion that would not appear on the mosaic images. It should be noted that the distortion had only affected the normal images while the mosaic images have not been affected even in one sample. It gives strong evidence that mosaic cover is undetectable and it is more secure than the normal images (Figure 10).

The proposed neural network-based crypto-system

According to Fındık et al. (2010) and Tay (2010), ANN has been developed as a generalization of mathematical models of human cognition and neural biology. The available data set is partitioned into two parts, one corresponding to training, and the other corresponding to test of the model. The purpose of training is to determine the set of connection weights and nodal thresholds that cause the ANN to estimate outputs that are sufficiently close to target values. This fraction of the complete data to be employed for training should contain sufficient patterns so that the network can mimic the underlying relationship between input and output variables adequately.

Artificial neural network applications are used in many fields such as engineering, industry, medicine, agriculture, finance, communication, meteorology, space and aeronautics. By the help of sophisticated computing technologies, the learning algorithms used in artificial neural networks allowed solving many problems that remained as undecided and defied any mathematical expression (Gullu and Yilmaz, 2010; Tay, 2010). In this paper we present a crypto-system which is based on Bidirectional Associative Memory (BAM) neural networks. The neural network is used to construct an efficient encryption system that uses multi keys (private and secret key). Therefore, to encrypt the secret data, the sender encrypts the data using the chosen keys (private key). On the receiver side, the receiver decrypts the ciphered data by the help of the generated secret key. The process to determine the values of these parameters on the basis of the data set is called learning or training algorithm, and for this reason the data set is generally referred to as a training set. The crypto-system includes the following three 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:

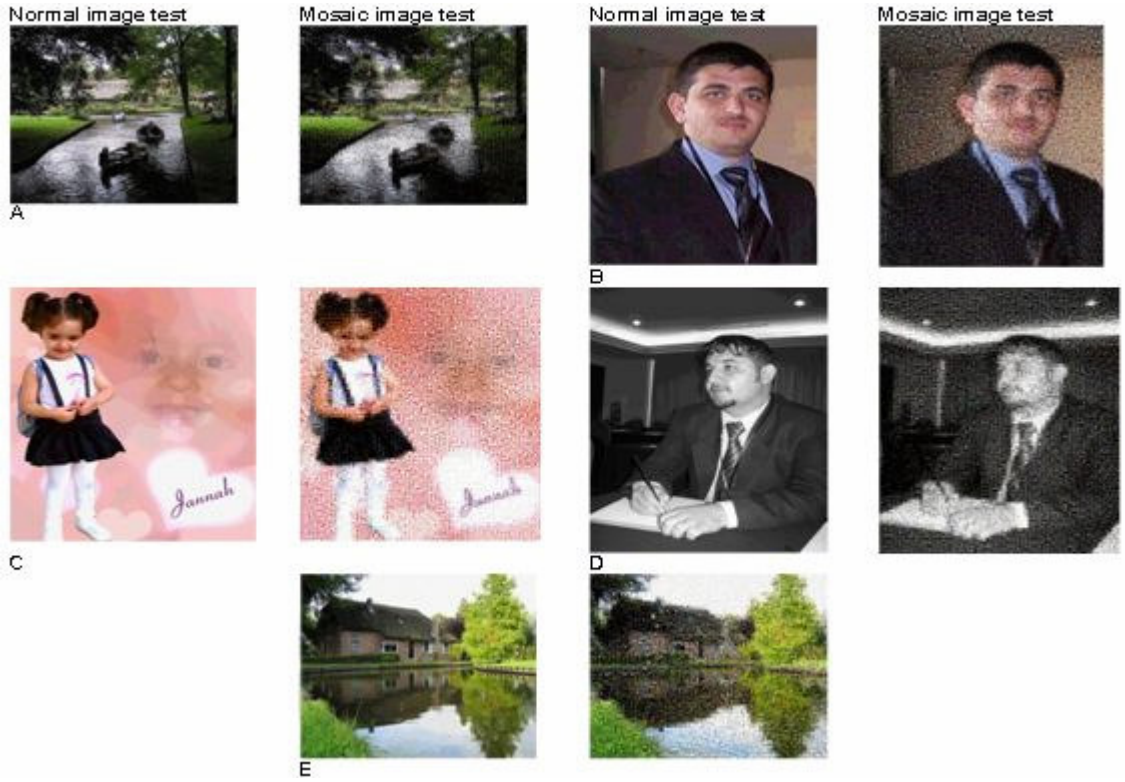
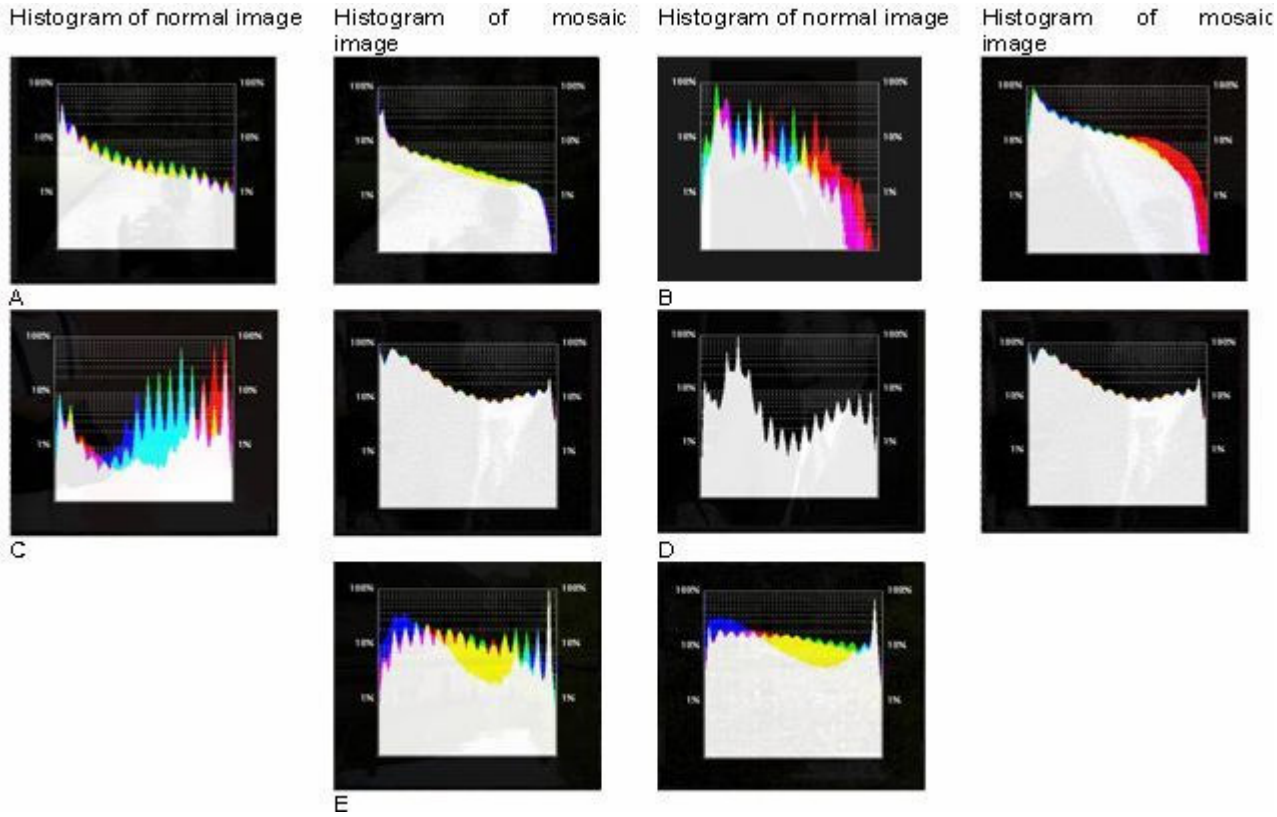


Figure 8. The tested images (that is, normal and mosaic).



Figures 9. A, B, C, D, E, F and G are the histogram of the tested images.

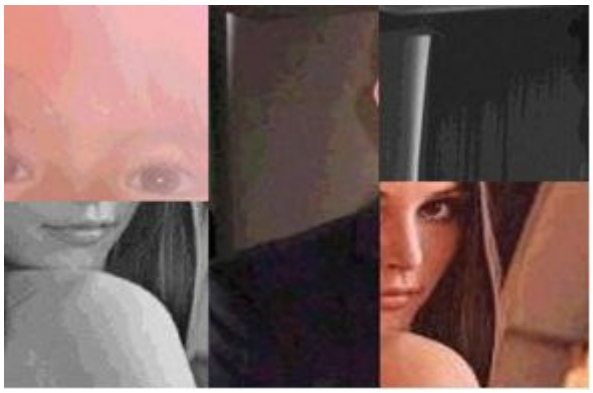


Figure 10. Part of distortion in the tested images.

Table 1. The training data for encryption process.

Input				Output				
16	**8**	**5**	**2**	**16**	**8**	**4**	**2**	**1**
K4	**K3**	**K2**	**K1**	**C4**	**C3**	**C2**	**C1**	**C0**
0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1	0
0	0	1	0	0	0	1	0	1
0	0	1	1	0	0	1	1	1
0	1	0	0	0	1	0	0	0
0	1	0	1	0	1	0	1	0
0	1	1	0	0	1	1	0	1
0	1	1	1	0	1	1	1	1
1	0	0	0	1	0	0	0	1
1	0	0	1	1	0	0	1	0
1	0	1	0	1	0	1	0	1
1	0	1	1	1	0	1	1	1
1	1	0	0	1	1	0	0	0
1	1	0	1	1	1	0	1	0
1	1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1	1

1. The sum of these numbers (keys) must be less than 2^x where x = 2^N;
2. Each number is greater than the sum of the previous numbers.
These keys are considered as sender's private key. To keep it simple, we have objects of the following key numbers (2, 5, 8, 17) such that K_1=2, K_2=5, K_3=8 & K_4=16. Notice that the key number 8 is greater than (2 + 5) and 16 is greater than (5+8). These will be the keys.
3. The sum of the keys =31 which is less than 2^x where x = 2^N (2^{16}).

Breaking the input data

Suppose M is some N-bit initial bipolar data, (that is M_i = {-1, 1}, -1≤ i ≤ N-1). In this model a 4-bit plaintext is the input (N = 4) and 5-bit cipher text is the output. Now we need something to encrypt, for example 01101011. First we break it down into blocks (N = 4), so: 01101011. If we look at the first part (1011), there are 1's in the first, second and fourth positions. This means that we take the first, second and fourth keys and add them together: 16 + 0 + 5 + 2 = 23. Repeat this for all blocks of the input data. This gives us the encrypted version 10111 as 23, as shown in Table 1.

BAM neural networks

BAM is a two-layer feedback network of interconnected neurons. Each neuron x_i in layer X is totally connected by "synapses" to every neuron y_i in layer Y and vice versa. No neurons are connected within the same layer**.** BAM encoding (learning) is performed by modifying the synapses (weights) between its neurons (Jalab, 2006). The basic BAM architecture is a two layers network, as shown in Figure 11.

There are two sets of outputs in the network that is one for each layer. The BAM units typically have [-1 1] outputs. All connections between units are bi-directional. Information passes back and forth from one layer to other, through these connections. For bipolar input vectors, the weight matrix can be given by:

$$W_{ij} = \sum_{p} X_i(p) Y(p)_j \quad (5)$$

The weight matrix from Y layer to X layer, can be given by the transpose of the weight matrix W^t.

Once the weight matrix is constructed, the network can be used to recall the stored information, by performing the following steps:

1. Apply an initial vector pair (X, Y) to the processed elements of the BAM.
2. Propagate the information from the X layer to the Y layer and update the values on the Y-layer units.
3. Propagate the updated Y information back to the X layer and update the units there.
4. Repeat steps 2 and 3 until there is no further change in the units on each layer.

The units compute sums of products of the inputs and weights to determine a net-input value:

1. Net-input on the Y layer:

$$net = Y_j = \sum_{j=1}^{n} W_{ij} X_i \quad (6)$$

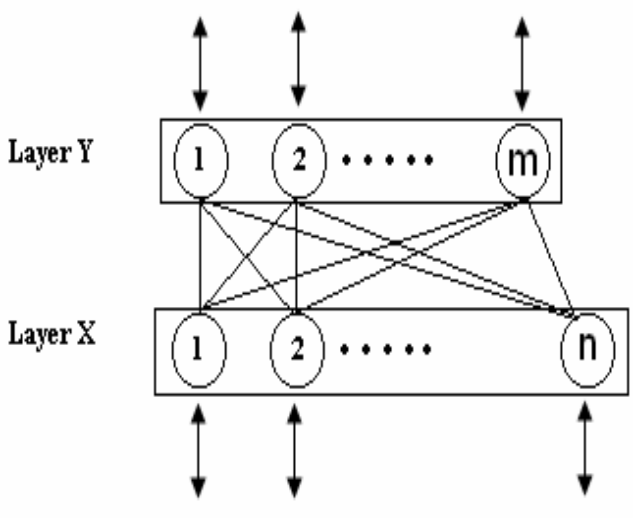


Figure 11. The basic BAM architecture.

2. Net-input on the X layer:

$$net = X_j = \sum_{j=1}^{n} W_{ij} Y_i \quad (7)$$

3. The output value for each processed element depends on the net-input value (threshold function) and on the current output value on the layer.

The new value of X is:

$$X_i = \begin{cases} 1 & if \quad X - net_i > 0 \\ unchanged & if \quad X - net_i = 0 \\ -1 & if \quad X - net_i < 0 \end{cases}$$

Similarly, the new value of Y is:

$$Y_i = \begin{cases} 1 & if \quad Y - net_i > 0 \\ unchanged & if \quad Y - net_i = 0 \\ -1 & if \quad Y - net_i < 0 \end{cases}$$

Implementation

The aforementioned crypto-system is applied on a sample of 4 bits data input for training and testing. In this model the input is denoted by X, while the output is denoted by Y, as shown in Table 1. To implement our neural network, we used the MATLAB 2009b. At the beginning of the training process, BAM is fed by the valid states and the weight values are adjusted. The weight set W for this operation shown in Table 2. After the weight set is constructed, the network is tested to encrypt and decrypt the new input data. For encryption the data is fed from X to Y while for decryption the data is fed from Y to X. In second case, we must take the transpose of the weight set (WT), which shown in Table 3.

Table 2. The weight set.

W =	5	3	1	1	1
	3	5	-1	-1	-1
	1	-1	5	1	5
	1	-1	1	5	1

Table 3. The weight transposes set.

		5	3	1	1
		3	5	-1	-1
W^T	=	1	-1	5	1
		1	-1	1	5
		1	-1	5	1

DISCUSSION AND FUTURE WORK

The motivation of this research is to support the problem that reported in several literature; they said, increase the amount of data hidden coupled with the image texture roughness. The finding and the summery of the result depicted the standpoint of the author, and meet with the expected result. Finally, there are three future suggestions for this research paper which are follows:

Firstly, increase the amount on the fifth LSB layer and sixth LSB to evaluate the habits of the mosaic image with amount exceeding 62 and 75% hidden data. Next improve the systems by encrypting the data using AES encryption algorithm before hiding the data. Thirdly, enhance the security by using PKI.

Conclusion

The mosaic is an image that is comprised of hundreds or thousands of other images to create one total image. The complexity of the mosaic image texture spots the light on the best cover for data hidden. The aforementioned experiment showed the capability of the mosaic image to hide a high rate of data hidden without any distortion. A sample from twenty images that were tested showed the success of the test was 50% in the normal image (ten images have not been affected and ten have been affected) while in the mosaic images there were no distortions at all. This means the test has 100% success rate over the entire sample. This work presents an asymmetric encryption mechanism based on BAM neural

networks. First, we presented the overall methods of encryption, and then we explored the necessary conditions of asymmetric methods. The secret key creation is based on BAM weights while the encryption technique and the private key creation processes are based on a super-increasing knapsack technique. The simulation results of this paper show positive results for different tests with relatively better performance than the traditional methods for encryption.

ACKNOWLEDGEMENT

This research has been funded in part from University of Malaya and Multimedia University. The author would like to acknowledge all workers involved in this project and had given their support in more ways than one.

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.

Alanazi HO, Jalab HA, Zaidan BB, Zaidan AA, Alam GM (2010). "Securing Electronic Medical Records Transmissions over Unsecured Communications: An Overview for Better Medical Governance." J. Medicinal Plants Res. In press.

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.

Dali S (2009). Landscape with Butterflies Mosaic Creator Gallery, http://www.aolej.com/mosaic/gallery.htm.

Fındık T, Tasdemir S, Sahin S (2010). "The use of artificial neural network for prediction of grain size of 17-4 pH stainless steel powders." Scientific Res. Essays, 5(11): 1274-1283.

Gogh V (2010). Starry Night. Mosaic Creator Gallery, http://www.aolej.com/mosaic/3giga.htm.

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

Haque A, Tarofder AK, Rahman S, Raquib MA (2009). "Electronic transaction of internet banking and its perception of Malaysian online customers." Afri. J. Bus. Manage., 3(6): 248-259.

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, Kasirun ZM, Jalab H, 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., 5(7): 1054-1062.

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

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.

Jalab HA (2006). "Fault Diagnosis Using Neural Network." Sana'a University J. Sci. Technol. (SUJST), 3(1): 57-63.

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

Por LY, Lai WK, Alireza Z, Ang TF, Su MT, Delina B (2008). "StegCure: a comprehensive steganographic tool using enhanced LSB scheme." W. Trans. on Comp., 7(8): 1309-1318.

Qabajeh LK, Kiah ML, Qabajeh MM (2009). "A Scalable and Secure Position- Based Routing Protocol for Ad-Hoc Networks." Malaysian J. Computer Sci., 22(2): 99-120.

Tay IN (2010). "Application of Neural Network models on analysis of prismatic structures." Scientific Res. Essays, 5(9): 978-989.

Zaidan AA, Zaidan BB, Alanazi O, Hamdan G, Abdullah ZO, Alam GM (2010a). "Novel Approach for High (Secure and Rate) Data Hidden within Triplex Space for Executable File." Scientific Res. Essays, in press.

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

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

Zaidan BB, Zaidan AA, Othman F, Raji RZ, Mohammed SM, Abdulrazzaq MM (2009a). Quality of Image vs. Quantity of Data Hidden in the Image. International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV'09), Las Vigas, Nevada, USA.

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