Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Image Steganography Based on Hybrid Cryptographic Algorithm Designed by making use of Blowfish, AES and RSA Algorithm

Deepankar Verma
Computer Science
R.B.I.E.B.T,
India

Jasleen Kour
Computer Science
B.I.E.B.T,
India

Abstract---Stenography and cryptography are two processes that are more widely used for sending information in secret way. Goal of both processes are to provide protection for information but in different way. In this paper our motive is to represent a new method for protection that is generated by combination of both process stenography and cryptography. There are many algorithms that exist for both processes. For cryptography there are algorithms like RSA, IDEA, AES, and DES but here we are using hybrid cryptography technique by making use of a RSA, AES, Blowfish. The secret data is encrypted by using this hybrid cryptography technique and resulting data is then embedded behind the prepared cover image by making use of MLSB embedding technique. Before embedding, the cover image is prepared by using hop field neural model. All implementation performed on the basis of PSNR, MSE parameters. So the image generated as result is encrypted that is very robust to attack.

Keywords--- Stenography, Cryptography, RSA, AES, Neural Network, key.

I. INTRODUCTION

There are two techniques exist that are used for sending information in secret way. These techniques are known as cryptography and stenography. Both techniques widely used for protection of information or data. Steganography is the art in which information hides on the way of communication between two nodes. Cryptography encode the message in cipher text form so that it is not possible for unauthorized party to understand it. So the information hidden by stenography technique cannot seen by any other person who is not authorized for it. In this paper we are going to develop a new system by using both processes i.e. stenography and cryptography. New system developed for better protection and confidentiality. Now a days, in market we have several hybrid cryptography technique - RSA very secure technique. After that we use custom neural network technique for applying second encryption technique to make more secure. Even we can apply these both techniques alone but any attacker can get original message by decrypt separately. So we apply both the techniques at same time so that any intruder cannot decrypt it or not as easy as single encryption technique can. This paper will highlight a new method that is developed for more security where image can be encrypted by using hybrid cryptography and stenography. We know how these processes can process as like:

- It is more secure to send a encrypted data in hidden form as compared to send original data in encrypted form .
- Main benefit of hidden data is that attention of intruder cannot be notice.
- By chance if data is extracted then it will be in encrypted form.
- So there can be a way to crack the encrypted image but the algorithm proposed by us has some good features with different ways to be implemented as following:
- At place of hiding complete text in image we firstly make segments according to 32*32 segmentation plan.
- To merge ascii encoded bits into the base image using public or private keys.
- Original message is accessible to those who know about this with the help of keys that are used for encryption.

Reverse process is applied to get original message.

Finally our objective is to develop a method which is more secure and if anyone is trying to access it from stego image then it becomes waste for that intruder.

II. BASIC CONCEPT AND RELATED WORK

There are many techniques available for secure transmission through communication channel, one of these is cryptography. But it should be in mind that when only cryptography is applied for protection that is not sufficient to provide good security. There are some basic requirements for cryptography as like integrity, authentication and redundancy etc. There are three basic algorithms described for encryption as following: -

a). Symmetric cryptography: In this algorithm only a single key is used for encryption and decryption. The key used for cryptography is known as private key. Key and encrypted data both are transmitted on different timing.

b). Asymmetric Cryptography: In this algorithm two keys are used for encryption and decryption. For encryption on sender side public key of receiver is used. On the receiving side means for decryption process private key of receiver is used.

c). Hash function: In this cryptography scheme mathematical concept is used for more protection.

As like cryptography, stenography is other technique that is used for secure communication. There are many ways to hide information like in audio, video text, and any other digital representative. There are many techniques for data hiding like Substitution system, Transform domain techniques, Spread spectrum techniques, Statistical method, Distortion techniques and Cover generation methods.

A. (DCT)-Frequency Domain Algorithm for Steganography

DCT method is used in this paper to get host image. Total numbers of 56 bits are hidden in form of 1 and 0. Blocks of 8 x 8 are created for the transform of image. 56 larger positive coefficients are selected with low mid-range frequency domain. High frequency coefficients are beneficial for image detail and also beneficial for some manipulation operation like filtering, and compression etc. Main issue is robustness so our concept is to apply it on whole image. So for robustness we choose low and mid frequency coefficient that are most suitable. We select coefficient *ci* in ordered magnitude and then it will modified by the corresponding bit in the message stream. If bit *s (i)* to be merged with *ith* message is "1", then we have a coefficient of quantity D. Persistence factor is now represented by quantity D. If same quantity is subtracted from coefficient then the message bit should be "0". Thus the replaced DCT coefficients are

DCT (new) = DCT+1*D for s(i)=1;

Else

DCT (new) =DCT-1*D for s(i)=0.

So image can be divided in frequency with value high, medium, and low.

B. (RSA)-Algorithm for Cryptography

RSA based on a public key system that is generated in 1978 by Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman. Three basic steps are required to complete the process of RSA operations that are; key generation, encryption and decryption. Firstly the messages or data are converted to numbers or integers, and then the numbers are manipulated according to the prescribed encryption scheme. Here is the description of the RSA cryptosystem. For the implementation of RSA we have to follow following steps :

Step 1 Firstly Choose two prime number p and q.

Step 2 Then compute value of n= p x q.

Step 3 Chooses e with (e, $(p-1)(q-1)$) = 1 and computes d with $de \equiv 1 (\mathrm{mod}(p-1)(q-1))$.

Step 4 Makes n and e public and keeps p, q, and d secret.

Step 5 Sender encrypts m as $c \equiv m^e \pmod{n}$ and sends c to Receiver

Step 6 Bob decrypts by computing $m \equiv c^d \pmod{n}$.

C. (AES)-Cryptography Algorithm

***A**dvanced **E**ncryption **S**tandard*, a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Diemen and Vincent Ragmen. The U.S government adopted the algorithm as its encryption technique. In October 2000, DES encryption technique is replaced by it . AES operates at multiple network layers at the same time. While the terms AES and Irondale are widely used methods bu there are some differences between these two methods. AES has a fixed block of size 128-bits and a key size of 128, 192, or 256-bits, whereas Irondale can be specified with any key and block sizes that is a multiple of 32-bits, having 128-bits minimum and 256-bits maximum.

AES Algorithm have following steps.

Step 1 *Key Expansion* : In this step , round keys are derived from the cipher key using Rijndael's key schedule.

Step 2 *Initial Round:* a) Add Round Key - In this step each byte of the state is combined using bitwise XOR with the round key.

Step 3*Rounds* : a) Sub Bytes –It is a non-linear substitution step in which each byte is replaced with another according to the enteries in a lookup table.

b) Shift Rows- It is a transposition step in which each row of the state is shifted cyclically at a certain number of steps.

c) Mix Columns-In this step a mixing operation is operated on the columns of the state, combining the four bytes in each column.

d) Add Round Key

Step 4 *Final Round* : a) Sub Bytes b) Shift Rows c) Add Round Key

D. Blowfish Cryptography Algorithm

Blowfish is an amended algorithm of AES. It is based on Feistel network with a block cipher of size 64 bit and a variable key of size up to 448 bits long. Blowfish algorithm operates on two stages: key-expansion and data encryption. During key expansion, the inputted key is converted into several subkey arrays total 4168 bytes. Here P- array consists of 18 32-bit boxes, and the S-boxes consists of four 32-bit arrays with 256 entires each. These boxes are first initialized with a fixed string that is the hexadecimal digits of pi (less the number 3).

After initialization step , the first 32 bits of the key are XORed with P1 (the first 32-bit box in the P-array). Similarity the second 32 bits of the key are XORed with P2, and so on, until all 448 key bits have been XORed.

Encryption: Blowfish encryption algorithm consist of 16 rounds. The input is a 64-bit data element X. X is divided into two 32- bit halves that is XL, XR. Then, the following computations are performed form r=1 to 16.

XL = XL $\oplus$ Pi

XR = F (XL) ⊕ XR
Swap XL and XR
After 16 rounds Swap XL and XR. Then XR and XL are XORed with P17 and P18.
XR = XR ⊕ P17
XL = XL ⊕ P18
Lastly XL and XR are recombined . Decryption procedure is same as encryption, except that P1, P2,.P18 arrays are used in the reverse order.

E. Hop-Field Neural Network

Neural networks are used in our proposed algorithm with hybrid cryptography technique to get well encrypted image. In neural networks a node can be connected more than 40000 nodes for exchange information. The nodes in networks are called neurons. When a neuron is strongly connected to other neuron then both can exchange information. We are going to applying neural networks over the hybrid cryptography technique . The way of computing in neural networks is shown in the fig 1.

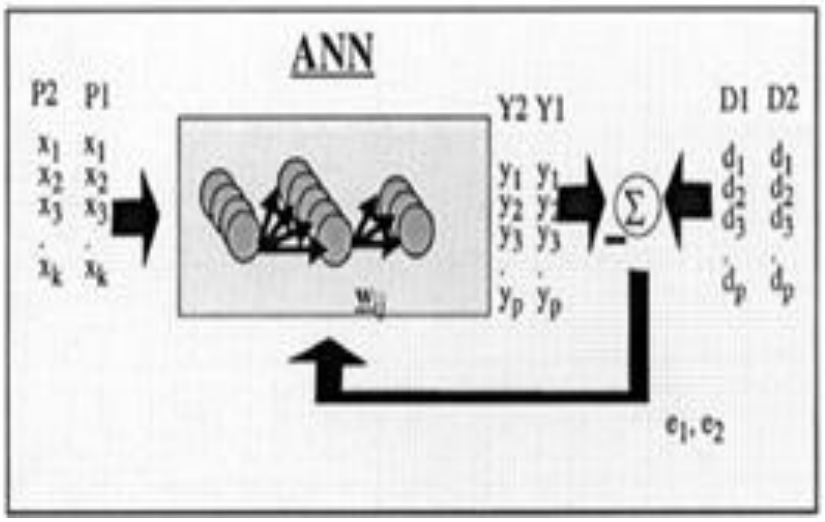


Fig1. Style of computing.

With the help of this algorithm decision taken on number of layers and number of nodes in hidden layers. When the connection is started then weights are assigned in a randomly way.
There are two layer exist one is input and other is output. In input layer vectors that are pre-processed are presented and at output layer calculation of error performed. If error is finding at output layer then it comes on input layer by backward process. This process is continuing till the last pattern. This form one-iteration process. At end of every-iteration test patterns are presented to neural network, and the prediction performance of network is evaluated.

III. PROPOSED ALGORITHM

We have proposed a new algorithm that provides more protection as compared to existence algorithms. For combination of two algorithms we have to follow basic idea behind it. First of all we have to distort the message and then this distorted message hide in existence and then get back original message. Both algorithm combined when required environment should be provided shown in table I.

Table I: Simulation environment

Size of the image	512 *512
Number of bits in each pixel of the cover image considered	8 bits(background)
Number of bits preferred in each message image	8 bits (foreground)
Method of embedding	Replacing two or three least significant bits of the cover image with equal number of bits of message image.(Multiple Least significant bit embedding)

The new algorithm can be proposed by following these steps:

- At place of hiding complete text in image we firstly segments according to 32*32 segmentation plan. For the segmentation we require an algorithm that DCT which we used in this implementation. The image is then quantized by using Hop-field neural network.
- To merge ascidia encoded bits into the base image using public or private keys. Here we implement hybrid cryptography algorithm by making use of RSA, AES, Blowfish cryptography algorithm to encode the secret data.

- The secret data(encrypted form) is then embedded by using MLSB technique behind the prepared cover image and stego image is formed.
- Original message is accessible to that who knows about this with the help of keys that are used for encryption. During decryption the reverse process is applied to get original message.

Fig 2 is showing a flowchart that is basic idea for development of new algorithm.

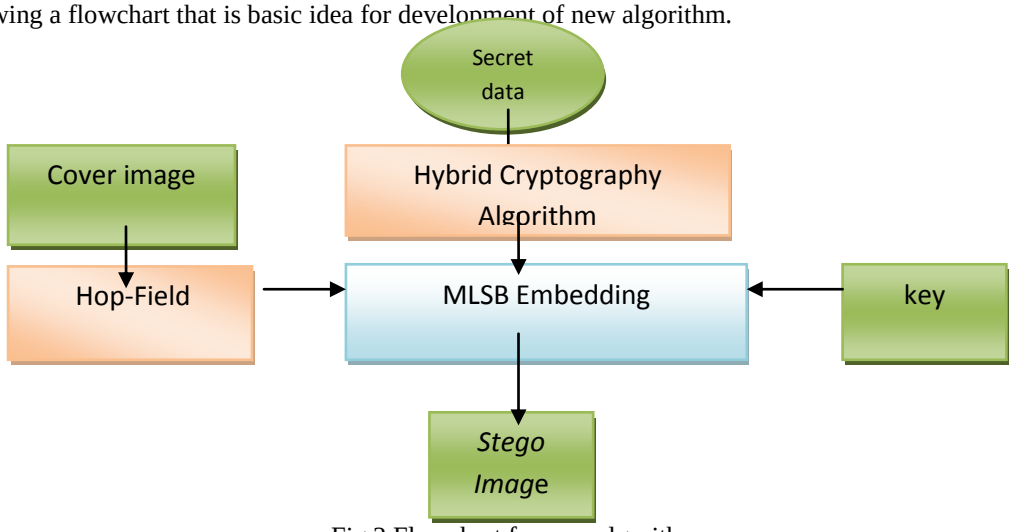


Fig 2 Flowchart for new algorithm

The steps shown in flowchart which we need to follow to get results as we expected from new developed algorithms.

IV. PERFORMANCE ANALYSIS AND RESULT

The result obtained using hybrid cryptography scheme and MLSB embedding is shown for different file format.

a).Fig. 1 shows the Lena cover image with its stego image (jpg format). The PSNR and MSE values have been shown between original Lena cover image and stego Lena image.

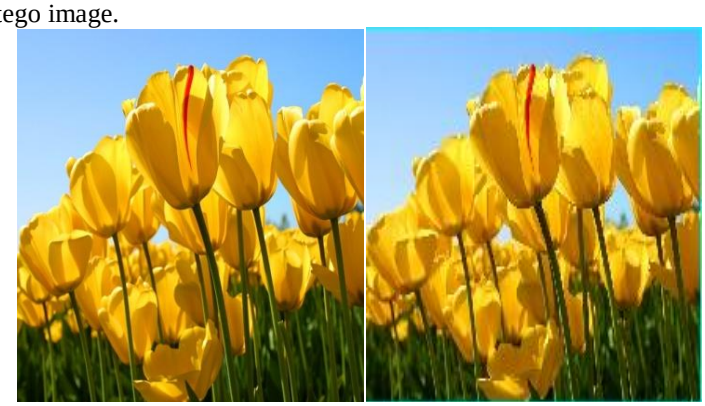
Cover Image(1) Stego Image(2)

PSNR between Image (1) and Image (2) = 118.383

MSE between Image (1) and Image (2) = 0.078

Fig. 1- PSNR and MSE values between original cover image Lena and its stego image

b)Fig. 2 shows the tulip cover image with its stego image The PSNR and MSE values have been shown between original tulip cover image and its stego image.



Cover Image(1) Stego Image(2)

PSNR between Image (1) and Image (2) = 107.315

MSE between Image (1) and Image (2) = 0.2800

Fig. 2- PSNR and MSE values between original cover image tulip and its stego image

c)Fig. 3 shows the cover image of cameraman with its stego image.The PSNR and MSE values have been shown between original cameraman cover image and stego image.

Cover Image(1) Stego Image(2)
PSNR between Image (1) and Image (2) = 118.38
MSE between Image (1) and Image (2) = 0.078
Fig. 3- PSNR and MSE values between original cover image cameraman and its stego image.

d)Fig. 4 shows the Babara cover image with its stego image The PSNR and MSE values have been shown between original Babra cover image and its stego image.

Cover Image (1) Stego Image(2)
PSNR between Image (1) and Image (2) = 110.296
MSE between Image (1) and Image (2) = 0.198
Fig. 4- PSNR and MSE values between original Babra cover image and its stego image.

The tabular form represents the experimentally evaluated parameters for different image file formats:

Table I: Parameters Evaluation

Image name	**PSNR**	**MSE**	**Capacity**	**NC**
Lena	118.383	0.078	278528	0.992186
Tulips	107.315	0.280	835584	0.992173
Cameraman	118.38	0.078	354355	0.992327
Babra	110.296	0.198	299869	0.992299

COMPARISION: The PSNR of the proposed scheme is compared with the two previos scheme:
The first comparison is made with Image steganography technique based on RSA and HASH-LSB and it is experimentally observed that our research work gives the better PSNR parameters and differences between the two schemes are represented in tabular as well as graphical form as shown below:

Table II: PSNR value of previous technique and proposed technique

Image Name	**Previous techniques using RSA and HASH-LSB**	**Proposed scheme**
Parameters	**PSNR**	**PSNR**
lena	74.0189	118.383
tulips	73.8220	107.315

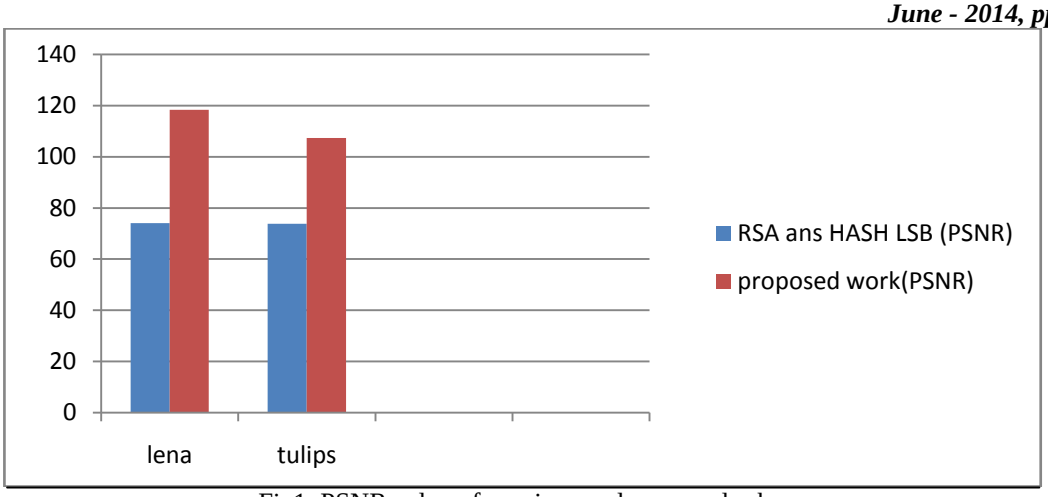


Fig1. PSNR value of previous and proposed scheme

2.The second comparison is made with" High Capacity Data Embedding using joint Intermediate Significant Bit (ISB) and Least Significant Bit (LSB) presented by Parah et. Al. It is experimentally observed that our research work gives the better PSNR parameters and differences between the two schemes are represented in tabular as well as graphical form as shown below:

Table III: PSNR value of previous technique and proposed technique

Image Name	**Previous techniques using ISB AND LSB**	**Proposed scheme**
P**arameters**	**PSNR**	**PSNR**
Cameraman	35.98	118.38
Babara	36.00	110.296

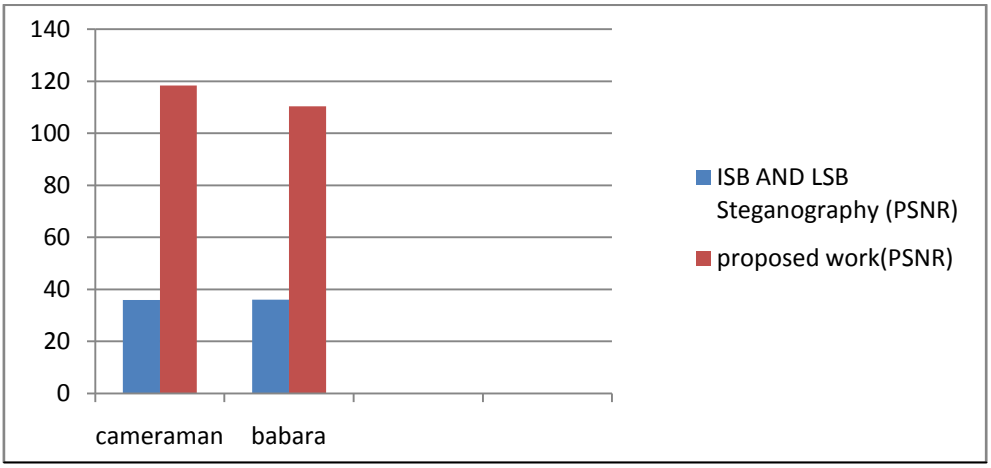


Fig2. PSNR values of previous and proposed scheme

V. CONCLUSION

This research paper presented the work that has been implemented to enhance the steganography technique so that the quality of the image remains the same.We have experimentally found out that the PSNR value of stego- image shows the better results in comparison with other existing steganography techniques. We overall concluded that managing the pixels to a deeper level increases the capacity of the image to hide certain messages. Hop- Field Neural Network has been found effective enough to find pixels to merge the data bits without much affecting the original pattern of the image. It has been also concluded that if we can encrypt the data up to some level before merging it to the image, it may enhance the chances of security into the image embedding

REFERENCES:

1] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[2] Swati malik, Ajit "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[3] Ishwarjot Singh ,J.P Raina," Advance Scheme for Secret Data Hiding System using Hop field & LSB" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[4] G. Manikandan, N. Sairam and M. Kamarasan "A Hybrid Approach for Security Enhancement by Compressed

Crypto-Stegno Scheme “, Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012

[5] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, “Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique”, International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.

[6] Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, “Extracting spread-spectrum hidden data from digital media “, IEEE transactions on information forensics and security, vol. 8, no. 7, july 2013.

[7] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., “ A new Steganographic method for color and gray scale image hiding”, Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194,2007.

[8] Bailey, K., and Curran, K., “An Evaluation of Image Based Steganography Methods”, Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, 2006.

[9] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh, “Triple-A: Secure RGB Image Steganography Based on Randomization”, International Conference on Computer Systems and Applications (AICCSA-2009), pp: 400-403, 10-13 May 2009.

[10] R.Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq and John Bosco Balaguru Rayappan , “Colour Guided Colour Image Steganography” Universal Journal of Computer Science and Engineering Technology , 16-23, Oct. 2010, pp. 2219-2158.

[11] Anil Kumar , Rohini Sharma,”A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique “,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[12] Gutub, A., Al-Qahtani, A., and Tabakh, A., “Triple-A: Secure RGB image steganography based on randomization”, Computer Systems and Applications, AICCSA 2009, IEEE/ACS, pp. 400 – 403, 2009..

[13] Dr. Fadhil Salman Abed “A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganography “, IJAIEM, Volume 2, Issue 4, April 2013

[**14]** K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, “Authentication of secret information in image steganography”, IEEE Region 10 Conference, TENCON- 2008, (2008) November, pp. 1-6.

[15] M. Chaumont and W. Puech, “DCT-Based Data Hiding Method To Embed the Color Information in a JPEG Grey Level Image”, 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, (2006) September 4-8.

[16] A. M. Hamid and M. L. M. Kiah, “Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis”, International Journal of Engineering and Technology (IJET): 0975-4042, (2009).

