Abdelkader Moumen* and Hocine Sissaoui

Images Encryption Method using Steganographic LSB Method, AES and RSA algorithm

DOI 10.1515/nleng-2016-0010
Received February 23, 2016; accepted December 17, 2016.

Abstract: Vulnerability of communication of digital images is an extremely important issue nowadays, particularly when the images are communicated through insecure channels. To improve communication security, many cryptosystems have been presented in the image encryption literature. This paper proposes a novel image encryption technique based on an algorithm that is faster than current methods. The proposed algorithm eliminates the step in which the secrete key is shared during the encryption process. It is formulated based on the symmetric encryption, asymmetric encryption and steganography theories. The image is encrypted using a symmetric algorithm, then, the secret key is encrypted by means of an asymmetrical algorithm and it is hidden in the ciphered image using a least significant bits steganographic scheme. The analysis results show that while enjoying the faster computation, our method performs close to optimal in terms of accuracy.

Keywords: Image encryption, Decryption, Steganographic LSB Method, AES, RSA

1 Introduction

The images are considered as one of the most widely used form of information, the internet revolution and the massive use of information technology facilitate communication and thus make more fragile the information. The exchange of digital data posed a security problem, so encryption become more important.

Based on the keys we can classify cryptography in two branches known as symmetric and asymmetric. The best known symmetric algorithms are AES (Advanced Encryption Standard), DES (Data Encryption Standard) and 3-DES [9]. These techniques are economical and comparatively secure. The biggest problem with these techniques is the exchange and storage of the secret key.

The second branch is Asymmetric (public) key cryptosystem [1], it uses the same algorithm for encryption and decryption with a pair of keys, public and private, computationally is impossible to derive the private key from the public key. Asymmetric systems such as RSA (Rivest, Shamir and Adleman) [1] requires the use of large numbers (greater than 512 bits) which is inappropriate for encrypting images [2, 8]. This branch of cryptography has of major interest, it removes problem of transfer of the key. But it can not grab the place of symmetric encryption algorithm because its computation time is comparatively long. For a large amount of data such as image, it is not preferable to use asymmetric encryption, for example, the RSA is 1500 times slower than symmetric DES algorithm [10, 11].

The steganography can also be a solution to increase amount of security. Steganography is a technique that imperceptibly hides secret data into cover media, such that an Oscar will not be able to extract the secret data. In literature one can find many efficient methods of steganography. Among all renown methods, LSB (Least Significant Bit) substitution, which embeds secret data by replacing k LSBs of a pixel with k secret bits directly [12].

In this paper we propose a method based on AES, RSA and LSB method. We encrypt the image using AES, then, the secret key is encrypted using RSA and it is hidden in the ciphred image using LSB technique. The major advantages of our approach it is eliminates the problem of key transmission. Presented approach is more efficient in terms of computation cost compared with schemes that use asymmetric encryption. We believe that projected approach is more secure due the strength of RSA, AES and LSB methods.

In Section 2 we will present an introduction to the cryptography and AES algorithm. Then, in Section 3, we wil give a brief description of the RSA algorithm. Section 4 consist of LSB steganographic method. After that, we describe propose approach in Section 5 and provide some experimental analyzes in Section 6. Finally, we give our conclusion in Section 7.

***Corresponding Author: Abdelkader Moumen:** Department of Mathematics. LANOS Laboratory, Badji Mokhtar University, Annaba BP 12, 23000, Annaba, Algeria, E-mail: abdelkader.moumen@gmail.com
Hocine Sissaoui: Department of Mathematics. LANOS Laboratory, Badji Mokhtar University, Annaba BP 12, 23000, Annaba, Algeria, E-mail: hsissaoui@hotmail.com

Table 1: Number of rounds depend on the key length.

	Key Length (Nk words)	Block Size (Nb words)	Number of Rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

2 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) which is adopted by the U.S. government in 2001, is now used in the Wifi security, compression tools. This algorithm has been developed by two Belgian researchers, Joan Daemen and Vincent Rijmen to replace the DES and the 3DES algorithms [5]. The AES algorithm is easy to implement, it consumes less memory and it uses keys of 128, 192 or 256 bits. The required number of rounds (i.e., linear and non-linear transformations), depend on the key size [4], see Table 1.

AES has four steps such as Byte sub, shift row, mixed column and add round key (see Figure 1) [3, 4] . The only nonlinear step which is responsible to create confusion in the data is byte sub, the remaining steps are nonlinear. In other words we can say that in shift row, mixed column and add round key we are only applying permutation operation for the sake to diffusion.

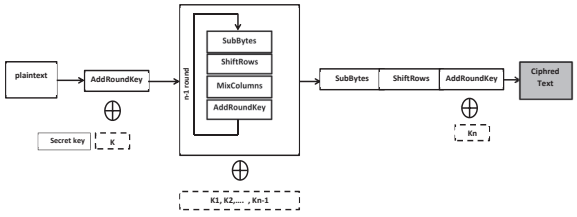


Fig. 1: Algorithm 1 : AES Encryption Algorithm

(i) SubBytes : A non linear transformation of the bytes. Each byte is replaced with a matrix called S-box using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation.

(ii) ShiftRows : It is a simple cyclic shift of each row of the matrix to the left.

(iii) MixColumns : Is a multiplication of matrix data by an other matrix to reorder the columns.

(iv) AddRoundKey : It is a simple XOR between the working state and the roundkey.

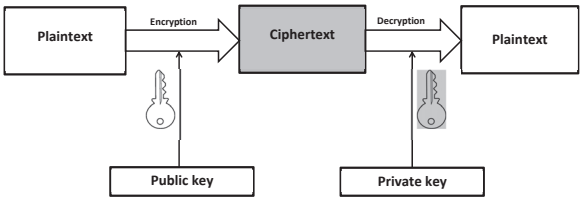


Fig. 2: Asymmetric encryption/decryption

The AES algorithm can support the following methods of encryption : ECB, CBC, OFB, CFB and CTR [4].

3 RSA Algorithm (Rivest, Shamir and Adleman):

The first solid system have been invented public key. It uses the same algorithm for encryption and decryption with a pair of keys, public and private (see Figure 2). Published in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology (MIT), the RSA is based on the difficulty of factoring large numbers.

In RSA we uses the same algorithm for encryption and decryption, we need pair of keys, public and private key (see Figure 2). We have three principal steps [18]:

1. Key generation :
   - Manufacturing large prime numbers p and q (+ – 100 digits).
   - Given an integer $n = pq$, it is very difficult to find the factors p and q from n.
   - Private key : (p, q), large prime numbers "p" and '"q".
   - Public key: (n, e), $n = pq$ and an integer "e" prime with $(p - 1)(q - 1)$.

   If "M" the plaintext and "C" the ciphertext.
2. Encryption :
$$C = M^e \bmod [n] \quad (1)$$
3. Decryption : Is based on the inverse function :
$$M = C^d \bmod [n] \quad (2)$$
where $e.d = 1 \bmod [(p - 1)(q - 1)]$

Algorithm 1: RSA

1. Begin.
2. m = the ASCII code of the plaintext.
3. c = the ASCII code of the ciphertext.
4. Choose two large prime numbers p and q (+100 digits).
5. Compute $\varphi(n) = (p-1)(q-1)$.
6. Compute $n = pq$
7. Choose any number $1 < e < \varphi(n)$ that is coprime to $\varphi(n)$.
8. Compute the value of d such that $(d * e) \bmod \varphi(n) = 1$.
9. Public key is (e, n).
10. Private key is (d, n).
11. The encryption of m is $c = m^e \bmod n$.
12. The decryption of c is $m = c^d \bmod n$.
13. End.

4 Hiding Methods in Image Steganography

Steganography is the science to hide secret information in other data, long before the invention of the computer. One can find in literature several different techniques of steganography [7, 12]. LSB is the best known method. LSB is to change the least significant bit of the cover media [6, 12, 13].

4.1 The LSB Method

For each pixel, color is coded with three bytes: red, green and blue respectively. Each byte indicates the intensity of the corresponding color, and the range is from 0 to 255. It takes a byte corresponding to one of the three colors of a pixel, for example 01010110. The idea is to replace these low order bits of information by those that one wishes to conceal. If the message is successfully hidden in well-chosen then image the naked eye cannot perceive the difference.

5 Our approach

Asymmetric encryption is inappropriate for images because the computation time is long, but it is more secure than symmetric encryption because it removes the exchange of the secret key, also it is mathematically infeasible to know the private key from the public key. The speed of symmetric encryption is better then asymmetric encryption but less secure since it requires secret key sharing.

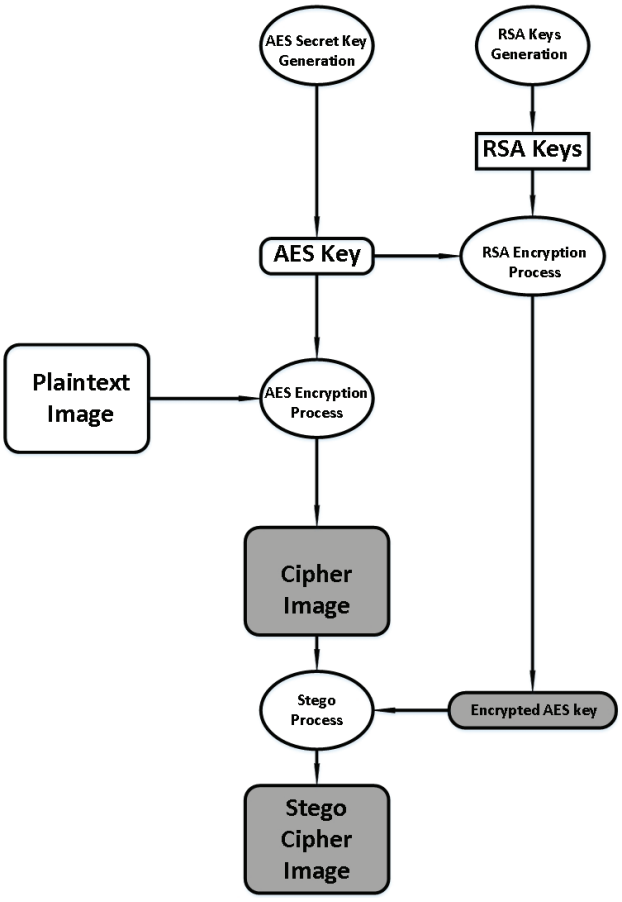


Fig. 3: Our approach

To take advantage of the speed of symmetric encryption and security of asymmetric encryption and steganographic methods. We propose an algorithm which combines AES, RSA and LSB method. First of all we encrypt the plaintext image using AES and a secret key k generated randomly (see Figure 3). Then this secret key k is encrypted using RSA , finally the ciphered key k' is hidden in the ciphertext image using LSB method. As showed in Figure 3, the proposed approach eliminates sharing key during the encryption process.

Initially, we have encrypted the original image using a symmetric algorithm. In our case we have used advance encryption standard (AES).

Then, the AES secret key is encrypted by using an asymmetrical RSA algorithm.

At the end, we will hide the encrypted secret key in the cipher image using least significance bits (LSB) technique.

In propose scheme we have encrypted the plain image using AES and the secret key is enciphered by RSA asymmetric algorithm. The strength of our technique is based on the plus points of RSA and AES. Because for huge data it is not economical to use RSA as DES is 1500 time faster than RSA [10, 11].

Algorithm 2: Proposed encryption scheme

1. Needed : AES cryptographic algorithm. RSA cryptographic algorithm, LSB steganographic algorithm.
2. Input: Original image I.
3. Output: Stego-ciphered image I_2.
4. Generate randomly secret key "k".
5. Encrypt the image I using AES algorithm and the secret key "k".
6. Encrypt secret key "k" using RSA algorithm (algorithm 1).
7. Hide the ciphered key "k'" using LSB algorithm in the ciphered image I_1.
8. Return the stego-ciphered image I_2.

Algorithm 3: Proposed decryption scheme

1. Needed : AES cryptographic algorithm. RSA cryptographic algorithm, LSB steganographic algorithm.
2. Input: Stego-ciphered image I_2.
3. Output: Decrypted image I.
4. Extract using LSB method the ciphered secret key "k'" frome the cover image I_2.
5. Decrypt using RSA algorithm the secret key "k'".
6. Decrypt the image I_1 using AES algorithm and the secret key "k".
7. Return the decrypted image I.

6 Experimental Results

We analyze propose algorithm on several gray-scale images of different sizes in order to evaluate its strength. We have chosen three images which are presented in Figures 4, 5 and 6 with dimensions of 256× 256 and 512 × 512 respectively. For encryption we applied stream ciphers using AES algorithm in OFB mode (Output Feedback Block) with a 128 bits key length. The key k has been encrypted with the RSA algorithm. Then using the LSB method, the key k' is hidden into the ciphered image (Figure 4.b.). After extracting the secret key and decrypting (Figure 4.c.) we get the decrypted image (Figure 4.d.).

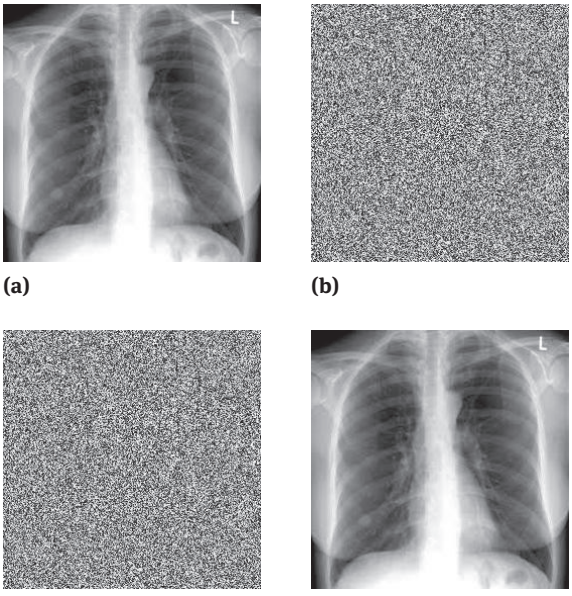


Fig. 4: Lung cancer: (a) Original image, (b) Ciphered image, (c) Stego-image, (d) Decrypted image.

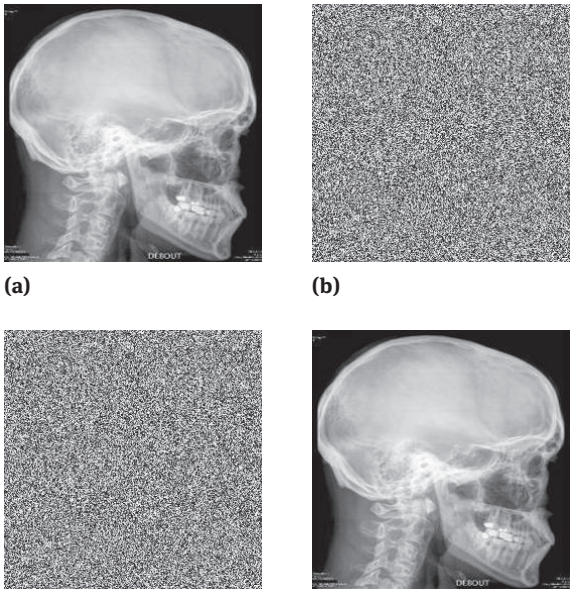
Table 2: Resistance for noises.

images	image size	PSNR of decrypted image (dB)
Lung cancer	256 × 256	52.42
Skull	256 × 256	52.87
Hand	512 × 512	53.81

6.1 Effect of Noise

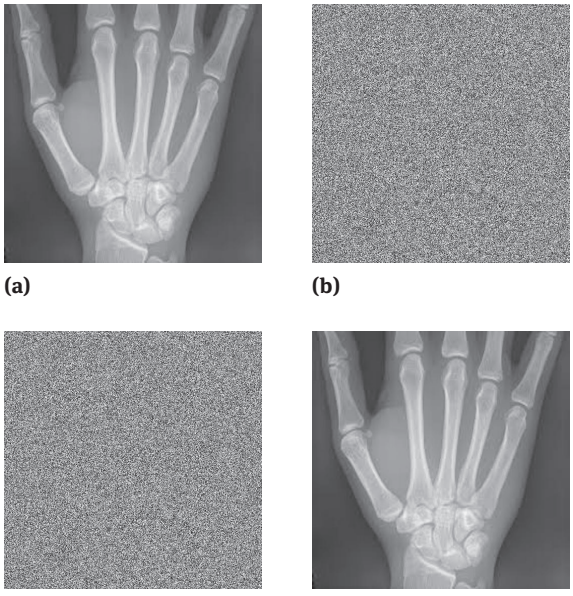
All types of digital data including images contains noise. If the decrypted image is similar to the original image, then the encryption system has resistant against noise. After decrypting the encrypted stego-image we observed the quality of the final image is good (PSNR > 50 dB) witch guaranties that propose algorithm is resistance for noise, the experimental results are shown in Table 2.

Peak Signal to the Noise Ratio (PSNR) which is used to evaluate the quality of the encrypted image is given as



(a) (b) (c) (d)

Fig. 5: Skull: (a) Original image, (b) Ciphered image, (c) Stego-image, (d) Decrypted image.



(a) (b) (c) (d)

Fig. 6: Hand: (a) Original image, (b) Ciphered image, (c) Stego-image, (d) Decrypted image.

Table 3: Lung cancer: Correlation analysis of two adjacent pixels.

	Plain image	Ciphered image	Stego-ciphered image
Horizontal	0.9603	0.0915	0.0045
Vertical	0.9251	0.0152	0.0204
Diagonal	0.9143	0.0012	0.0425

Table 4: Skull: Correlation analysis of two adjacent pixels.

	Plain image	Ciphered image	Stego-ciphered image
Horizontal	0.9412	0.0065	0.0256
Vertical	0.9545	0.0376	0.0087
Diagonal	0.9205	0.0189	0.0141

Table 5: Hand: Correlation analysis of two adjacent pixels.

	Plain image	Ciphered image	Stego-ciphered image
Horizontal	0.9625	0.0075	0.0258
Vertical	0.9348	0.0526	0.0084
Diagonal	0.9066	0.0185	0.0213

Table 6: Entropy value of: Plain image, Ciphered image and Stego-ciphered image

Image	Plain image	Ciphered image	Stego-ciphered image
Lung cancer	7.5605	7.7625	7.7812
Skull	7.2856	7.6115	7.6822
Hand	6.8644	7.7365	7.8275

follow [19].

$$PSNR = 10 \times log_{10} \frac{255 \times 255 \times M \times N}{\sum_{i=1}^{M} \sum_{j=1}^{N} (P_{ij} - Q_{ij})^2} (dB), \quad (3)$$

where P_{ij} and Q_{ij} denote the pixel values in row i and column j of the original image and the encrypted image, respectively, M and N are the image sizes.

6.2 Key Space Analysis

For a secure cryptosystem, the key space must be large enough to make sure that brute force attack is infeasible. In our case, since we are using RSA encryption scheme to enrypt AES secret key, the key space is 2^{80} due to RSA, it is not possible with living technology.

6.3 The Correlation Analysis

We tested the correlation between the adjacent pixels in the plaintext image and cipher image, we got a negligible correlation, so it's difficult to break the algorithm using correlation attacks. The results are given in Tables 3, 4 and 5.

Table 7: Statistical Analysis of the Proposed Technique compared to AES [20].

Statistical Analysis	Proposed Technique (hand.jpg)		AES algorithm [20]	
Images	Plain Image	Stego Cipher	Plain Image	Cipher Image
Horizontal Cor	0.9625	0.0258	0.9282	–0.0067
Vertical Cor	0.9348	0.0084	0.9644	0.0504
Diagonal Cor	0.9066	0.0213	0.9116	–0.0156
Entropy Value		7.8275		7.9975

The correlation coefficient is calculated using the formula [14, 15]:

$$CC = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{n=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right)}{\sqrt{\sum_{n=1}^{N} \left(x_i - E(x)\right)^2}\sqrt{\sum_{n=1}^{N} \left(y_i - E(y)\right)^2}} \tag{4}$$

Where $E(x) = \frac{1}{N}\sum_{n=1}^{N} x_i$, x and y are the pixel values of the same indices of the original image and the ciphered image respectively.

If the correlation coefficient is near 1, this means that the original image and the encrypted image are very dependent on each other, i.e. the original image can be reproduced easily from the encrypted image [14, 15].

6.4 Entropy analysis

Information entropy is an important tool to analyze the strength of encryption scheme. The formula of $H(s)$ of a source s is as follow [17]:

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) log_2 \frac{1}{P(s_i)} \text{ bits}, \tag{5}$$

where $P(s_i)$ represents the probability of symbol s_i,

$$P(s_i) = \frac{\text{number of } s_i \text{ in the ciphred image}}{2^N}. \tag{6}$$

By entropy we can determine the degree of uncertainties of the the system [16]. If every symbol has an equal probability, i.e. $P(s_i) = \frac{1}{2^N}$ $(i = 0, 1, \cdots, 2^N - 1)$,

$$\begin{aligned} H(s) &= \sum_{i=0}^{2^N-1} P(s_i) log_2 \frac{1}{P(s_i)} \text{ bits} \\ &= \sum_{i=0}^{2^N-1} \frac{1}{2^N} log_2 2^N \text{ bits} \\ &= 2^N \frac{1}{2^N} log_2 2^N \text{ bits} \\ &= N \text{ bits} \end{aligned} \tag{7}$$

for gray-scale image $N = 8$ ($2^8 - 1 = 255$ gray scale), then the optimal value of entropy is $H(m) = 8$, which corresponds to a random source. In the practice information entropy is less than the ideal value 8. For a cryptosystem to be invulnerable, the entropy should be close to optimal value. The proposed algorithm meet this analysis with good reading as show in Table 6.

We compare the correlation coefficient and the entropy value of our scheme with the AES algorithm studied in [20] (see Table 7). From Table 7 one can see that proposed scheme is comparable with the analyses of AES presented in [20].

7 Conclusion

In this paper, we introduced a new method of image encryption. Our approach is based on symmetric, asymmetric encryption and steganography. In the beginning, we use symmetric encryption for the encryption of image, then we make use of asymmetric algorithm for the security of the key. Furthermore we hide our encrypted key in the cipher image using LSB steganographic method.

The outcomes of the security analyzes can be seen in Tables 2, 3, 4, 5, 6 and 7 and one can examine that propose algorithm is invulnerable against renown attacks. So we can make use of it for secure and economical image encryption.

References

[1] D. Bleichenbacher, B. Kaliski, and J. Staddou. "Recent Results on PKCS : RSA Encryption Standard"., *RSA Laboratories Bulletin, 24 June 1998.*

[2] C.C. Chang, M.S. Hwang, and T-S Chen. "A new encryption algorithm for image cryptosystems". *The Journal of Systems and Software.,* 58 :83–91, 2001.

[3] H. Cheng and X. LI, "Partial Encryption of Compressed Images and Videos". *IEEE Transactions on Signal Processing,*. 48(8): 2439–2451, 2000.

[4] J. Daemen and V. Rijmen. "AES Proposal the Rijndael Block Cipher". *Technical report,. Proton World Int.1, Katholieke Universiteit Leuven,* ESAT-COSIC, Belgium, 2002.

[5] J. Daemen and V. Rijmen. "The Design of Rijndael"., *SpringerVerlag New York,* Inc. Secaucus, NJ, USA, 2002.
[6] J. Fridrich and P. Lisonek , "Grid coloring in steganography", *IEEE Transactions on Information Theory,* 53 (4): 1547–1549, (2007).
[7] S. M. Douiri, M.B. O. Medeni, S. Elbernoussi1, E. Souidi. "A New Steganographic Method For Grayscale Image Using Graph Coloring Problem". *Applied Mathematical Sciences*. 7, No. 2, 521–527 (2013).
[8] R. Norcen,M. Podesser, A. Pommer, H.P. Schmidt, and A. Uhl. "Confidential storage and transmission of medical image data". *Computers in Biology and Medicine,*. 33 :277–292, 2003.
[9] National Bureau of Standards, "Data Encryption Standard," *FIPS Publication 46, (1977)*.
[10] Douglas R. Stinson. *Cryptography : Theory and Practice, (Discrete Mathematics and Its Applications)*. Chapman & Hall/CRC Press, New York, November (2005).
[11] Bruce Schneier, *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth),* John Wiley & Sons, Inc, (01/01/96).
[12] D.W. Bender, N.M. Gruhl and A. Lu, *Techniques for data hiding, IBM Syst.* J. 35, 313–316, (1996).
[13] C.M. Wang, N.I. Wu, C.S. Tsai and M.S. Hwang, "A high quality steganography method with pixel-value differencing and modulus function", *J. Syst. Softw.* 81, 150–158, (2008).
[14] N. El-Fishawy and O. Zaid, "Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms," International Journal of Network Security, vol. 5, no. 3, pp. 241–251, 2007.
[15] H. Elkamchouchi and M. Makar, "Measuring encryption quality for bitmap images encrypted with rijndael and kamkar block ciphers," in Radio Science Conference, 2005. NRSC 2005. Proceedings of the Twenty-Second National. IEEE, 2005, pp. 277–284.
[16] X. Shu-Jiang, W. Ying-Long, W. Ji-Zhi, and T. Min, "A novel image encryption scheme based on chaotic maps," in Signal Processing, 2008. ICSP 2008. 9th International Conference on. IEEE, 2008, pp. 1014–1018.
[17] Z. Han, W. Feng, L. Hui, L. Da Hai, and L. Chou, "A new image encryption algorithm based on chaos system," in Robotics, Intelligent Systems and Signal Processing, 2003. Proceedings. 2003 IEEE International Conference on, vol. 2. IEEE, 2003, pp. 778–782.
[18] US Federal Rules of Evidence 1001, 1002, and 1003. Federal Rules of Evidence (LII 2006 ed.)
[19] M. El-lskandarani, S. Darwish, and S. Abuguba, "A robust and secure scheme for image transmission over wireless channels," in Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on. IEEE, 2008, pp. 51–55.
[20] Jawad Ahmad and Fawad Ahmed. "Efficiency Analysis and Security Evaluation of Image Encryption Schemes" International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:12 No:04