Journal of Engineering and Development, Vol. 13, No. 3,September (2009) **ISSN 1813-7822**

On the security of Bitmap Images using Scrambling based Encryption Method

Asst. Lec. Fatimah Shamsulddin Abdulsattar
Computer & software Eng. Dept.
College of Eng./ Al-Mustansiriya University

Abstract

Image encryption is one of the most important applications in transferring images through the internet. In most of the natural images the values of the neighboring pixels are strongly correlated. This means that the value of any given pixel can be reasonably predicted from the values of its neighbors. This paper presents an approach for image encryption based on combination of image scrambling and well known encryption and decryption algorithms such as RC4 and AES. The original image can be viewed as an arrangement of pixels, which were rearranged into a scrambled image using pseudo random index generator, and then the generated image was encrypted using one of the encryption algorithm. The results showed that the correlation between image elements was significantly decreased by the proposed technique. Also, a number of performance measuring factors were considered to show the impact of the proposed technique.

الخلاصـــــة

تعتبرعملية تشفير الصورة واحدة من التطبيقات المهمة في عملية ارسال الصور عبر الانترنت . ان في اغلب الصور تكون قيم العناصر المتجاورة عادة مترابطة بصورة قوية ،اذ انه يمكن تخمين قيمة اي عنصر من عناصر الصورة من قيم العناصر المجاورة له . في هذا البحث تم تقديم طريقة لتشفير الصور تعتمد على بعثرة عناصر الصورة الواحدة لتقليل الترابط الموجودة بينها من خلال استخدام مبدأ توليد التسلسل العشوائي، ثم يليها تطبيق واحدة من خوارزميات التشفير المعروفة كا (*RC4* او *AES*) للحصول على الصورة المشفرة النهائية ، وقد بينت النتائج ان الطريقة المتبعة قد قللت من الترابط الموجود بين عناصر الصورة، اضافة الى ان العديد من مقاييس الكفاءة التي تم اعتمادها في هذا البحث قد بينت كفاءة الطريقة المقترحة .

1. Introduction

The amount of visual information available in digital format has grown exponentially in recent years. Retrieving particular images in a way that is both effective and efficient remains an open problem. With the further development of multimedia technologies and the rapid spread of computer networks, the rapid development of computer communication and the Internet makes it very easy to loose exchange data via networks [1].

Internet and wireless networks offer powerful channels to deliver and exchange images. The increased popularity of image exchange places a great demand on efficient image storage and transmission techniques. The major hurdle for allowing much broader access of digital images lies in how to make sure that an image is used for its intended purpose by its intended recipients. Sensitive and confidential information is vulnerable to various kinds of misuse when data in or transmitted to/from computer system [1,2], then the development of secure management usage of digital images becomes one of the important applications in image processing.

The wide use of digital images and videos in various applications brings serious attention to the security and privacy issues today. Many different encryption algorithms have been issues today, but some of them have known to be insecure [1,3].

In most of the natural images, the values of the neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors) [4]. In order to dissipate the high correlation among pixels and improve the security level of the encrypted images, the method of position scrambling can be used before encryption. This paper adopted the idea of combining the most popular encryption techniques (such as AES or RC4) with the pixel position scrambling, which can overcome the single encryption algorithm disadvantage effectively. By using the correlation coefficient as a measure of security, the scrambling process will be expected to result in a lower correlation value when compared to using the encryption algorithms alone. Two different variable-length secret keys are needed in the scrambling and encryption processes. The secret keys must be known to both sender and receiver.

2. Related Works

The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images.

Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. Zeghid M. et al [5] modified the AES algorithm by adding key stream generator using (A5/1 or W7) to AES to ensure improving the encryption performance. Hossam El-din H. et al [6] presented an efficient chaos based feedback stream cipher (ECBFSC) for image cryptosystems, which is based on the use of a chaotic logistic map and an external secret key of 256-bit.

Mohammed A.[4] introduced a block-based transformation algo``1rithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish.

3. Overview of the Encryption Algorithms

This section will give a brief overview on the construction of each encrypting algorithms. To show the effectiveness of the proposed technique, two different encryption algorithms would be considered here. The first one is the AES, which is an example of a symmetric block cipher, while the other is the RC4, which represents the most popular stream cipher.

3-1 AES (Rijndael) Algorithm

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr=10,12,14) [5,7,8]. These rounds are governed by the following transformations:

(i) *SubBytes transformation:* Is a non linear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation. Figure (1) shows the step of the SubBytes transformation.

(ii) *Shiftrows transformation:* Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.

(iii) *Mixcolumns transformation:* Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

(iv) *Addroundkey transformation:* Is a simple XOR between the working state and the roundkey. This transformation is its own inverse.

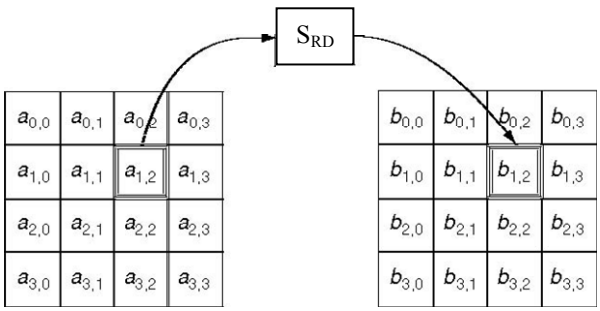


Figure (1): Subbytes acts on the individual bytes o the state

The encryption procedure consists of several steps as shown by the following pseudo code. After an initial addroundkey, a round function is applied to the data block (consisting of subbytes, shiftrows, mixcolumns and addroundkey transformation, respectively). It is performed iteratively (Nr times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-SubBytes, the Inv-Shiftrows, the Inv-Mixcolumns, and the Addroundkey allow the form of the key schedules to be identical for encryption and decryption.

Pseudo code of AES round transformation:

```
Round(State,ExpandedKey[i])
{
SubBytes(State);
ShiftRows(State);
MixColumns(State);
AddRoundKey(State,ExpandedKey[i]);
}
FinalRound(State,ExpandedKey[Nr])
{
SubBytes(State);
ShiftRows(State);
AddRoundKey(State,ExpandedKey[Nr]);
```

3-2 The RC4 Algorithm

RC4 was designed by Ron Rivest of RSA Security in 1987. It is the most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer and WEP. The algorithm uses a mechanism to generate 8 bits pseudorandom numbers to encrypt/decrypt plaintext byte-by-byte [figure (2)]. The internal state of RC4 consists of two counters *i* and *j* (each within 0–255) plus an array of 256 8-bit bytes, called the S-box [9,10]. The S-box is initialized using the key *K* as follows:

/* Initialization */
for i = 0 to 255 do
S(i) = i
/* Initial Permutation of S */
j = 0
for i = 0 to 255 do
j = (j + S(i) + K(i)) mod 256
swap S(i) and S(j)
/* Stream Byte Generation */
i = 0 ; j = 0;
While (true) do
i = (i + 1) mod 256

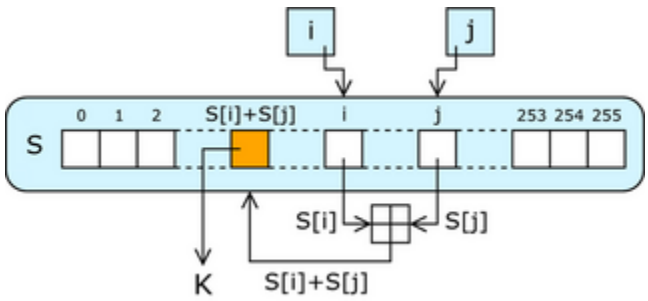


Figure (2): The structure of the RC4 algorithm

j = (j + S(i)) mod 256
swap S(i) and S(j)
k = S(S(i) + S(j)) mod 256

To encrypt, XOR the value k with the next byte of plaintext. To decrypt, XOR the value k with the next byte of ciphertext.

4. Pseudo Random Index Generator and scrambling process

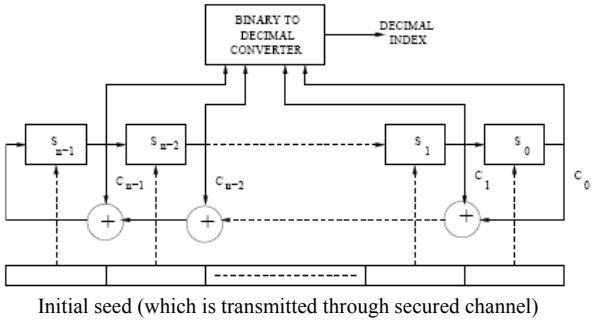
Pseudo random index generator (PRIG) for scrambling purpose can be usually constructed using the linear feedback shift registers (LFSR) [8,10,11]. A PRIG contains *n* shift registers and is initiated with a starting seed, which is usually transmitted through a secured channel for intended users only. The outputs of the shift registers are multiplied with the coefficients $(C_{n-1}, C_{n-2}, \ldots, C_1, C_0)$ of a primitive polynomial with respect to mod-2 operation. The resultant output obtained by the modulo operation is then fed back to the first shift register. The shift register output values are converted into decimal index using binary to decimal converter. The general structure of such a PRIG is shown in Figure (3). Note that the periodicity of such a random index generator is 2^n-1.

A scrambling process of degree z refers to the operation of replacing an arrangement $\{p_i|\ i=1,2,\ldots,z;\ p_i \in S\}$ by a second arrangement $\{q_i|\ i=1,2,\ldots,z;\ q_i \in S\}$ and is represented as

$$\Omega = \begin{pmatrix} p_1 p_2 \ldots p_z \\ q_1 q_2 \ldots q_z \end{pmatrix} \quad \ldots.(1)$$

Where S denotes any non-empty set. The reverse of this scrambling process is specified as

$$\Omega^{-1} = \begin{pmatrix} q_1 q_2 \ldots q_z \\ p_1 p_2 \ldots p_z \end{pmatrix} \quad \ldots.(2)$$



Figure(3): Structure of a general pseudo random index generator

5. The proposed Scheme

The proposed combination scheme consists of image scrambling followed by encryption (i.e. AES or RC4). The main idea behind the present work is that an image can be viewed as an arrangement of pixels, which can be rearranged as follows:

$p_1, p_2, p_3 \ldots p_{N\times N}$ where N×N is the dimension of an image

The intelligible information present in an image is due to the correlations among the pixels in a given arrangement. The perceivable information can be reduced by reducing the correlations among the pixels of an image by scrambling the position of the pixels across the entire image

using pseudo random index generator. Then, the scrambled image is fed into encryption algorithm to modify the pixel values ultimately using secret key. The block diagram of the adopted scheme is shown in figure (4). The proposed encryption algorithms will be called (Modified RC4 and Modified AES).

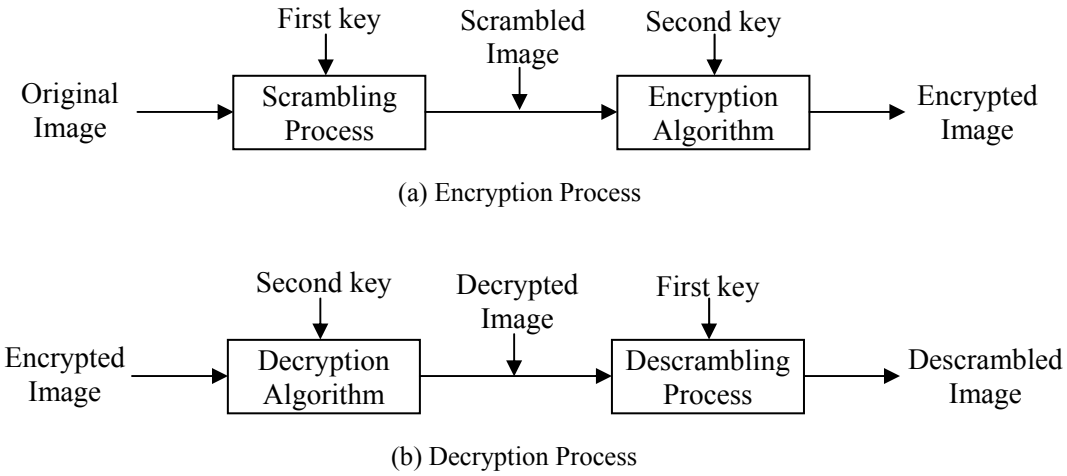


Figure (4): Block diagram of the adopted scheme

6. Quality of Encryption Measurements

One of the important factors in examining the encrypted image is the visual inspection where highly disappeared features of the image the better the encryption algorithm. But depending on the visual inspection only is not enough in judging the complete hiding of the content of data image. So, other measuring techniques are considered to evaluate the degree of encryption qualitatively.

With the implementation of an encryption algorithm to an image, a change takes place in pixel values as compared to the values before encryption. Such change may be irregular. Apparently this means that the higher the change in pixel values, the more effective will be the image encryption and hence the quality of encryption. So, the quality of encryption may be expressed in terms of the total deviation (changes) in pixel values between the original image and the encrypted one [12].

In addition to the visual inspection, three measuring quality factors will be considered to evaluate and compare between the encryption algorithms RC4 and AES alone and its modified versions.

6-1 The Correlation Coefficient Measuring Factor (C.C)

Correlation is a measure of the relationship between two variables. If the two variables are the image and its encryption, then they are in perfect correlation (i.e; the correlation

coefficient equals one) if they are highly dependent (identical). In this case the encrypted image is the same as the original image and the encryption process failed in hiding the details of the original image. If the correlation coefficient equals zero, then the original image and its encryption are totally different, i.e., the encrypted image has no features and highly independent on the original image. If the correlation coefficient equals -1, this means the encrypted image is the negative of the original image [12]. So, success of the encryption process means smaller values of the C.C. The C.C is measured by the following equation:

$$\text{The correlation coefficient} = \frac{\text{cov}(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \quad \textbf{.....(3)}$$

Where, $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, while, x and y are gray-scale pixel values of the original and encrypted images.

6-2 The Maximum Deviation Measuring Factor (Dev)

The maximum deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images [12]. The steps of this measure will be done as follows:

1) Count the number of pixels of each grayscale value in the range from 0 to 255 for both original (h_1) and encrypted images (h_2) (i.e; get their histogram distributions).

2) Compute the absolute difference or deviation between the two curves ($h=h_1-h_2$).

3) Count the area under the absolute difference curve, which is the sum of deviations (Dev) and this represents the encryption quality. (Dev) is given by the following equation:

$$\text{Dev} = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \qquad \text{.....(4)}$$

Where h_i is the amplitude of the absolute difference curve at value i. Of course, the higher the value of Dev, the more the encrypted image is deviated from the original image.

6-3 The Irregular Deviation Measuring Factor (ID)

This quality measuring factor is based on how much the deviation caused by encryption (on the encrypted image) is irregular. It gives an attention to each individual pixel value and the deviation caused at every location of the input image before getting the histogram as described in [12] which does not preserve any information about the location of the pixels. This method can be summarized in the following steps:

1) Calculate the 'D' matrix which represents the absolute values of the difference between each pixel values before and after encryption. So, D can be represented as:

2)

$$D = | I - J | \qquad \textbf{....(5)}$$

where I is the input image, and J is the encrypted image.

2) Construct the histogram distribution 'H' of the absolute deviation between the input image and the encrypted image. So, H = histogram (D).

3) Get the average value of how many pixels are deviated at every deviation value (i.e., the number of pixels at the histogram if the statistical distribution of the deviation matrix is a uniform distribution). This average (DC) value can be calculated as:

$$DC = \frac{1}{256}\sum_{i=0}^{255} h_i \qquad \text{....(6)}$$

where h_i is the amplitude of the absolute difference histogram at the value i.

4) Subtract this average from the deviation histogram, then take the absolute value of the result.

$$AC(i) = | H(i) - DC | \qquad \text{.... (7)}$$

5) Count the area under the absolute AC value curve (ID), which is the sum of variations of the deviation histogram from the uniformly distributed histogram.

$$ID = \sum_{i=0}^{255} AC(i) \qquad \text{.... (8)}$$

The lower the ID value, the better the encryption algorithm.

7. Results and Discussion

All encryption algorithms were applied with a three different bmp images that have 256×256 pixels with 256 colors. These images are Lena, sailboat, and peppers. The three images are encrypted using RC4, AES, Modified RC4, and Modified AES. The number of rounds for the AES is (Nr=10). For all encryption algorithms, the key length is kept the same at 16 bytes.

The results of the three measuring factors are given in the following tables where DEV-1 indicates the correlation coefficient measure, DEV-2 indicates the maximum deviation measure, and DEV-3 indicates the irregular deviation measure. Tables (1-3) illustrate the results with the measure of DEV-1 the smaller is the better, with DEV-2 the greater is the better, while with DEV-3 the smaller is the better.

Table (1): The quality of encryption Lena image

	Quality measures		
Cipher	Dev-1	Dev-2	Dev-3
RC4	0.0028	4.6908×10^{4}	5.8207×10^{4}
Modified RC4	3.8764×10^{-4}	4.6944×10^{4}	5.8052×10^{4}
AES	0.0029	4.6507×10^{4}	5.8035×10^{4}
Modified AES	3.3632×10^{-4}	4.6518×10^{4}	5.7870×10^{4}

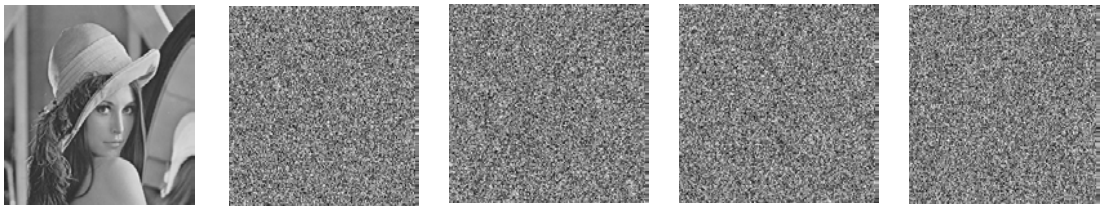
Table (2): The quality of encryption sailboat image

	Quality measures		
Cipher	Dev-1	Dev-2	Dev-3
RC4	8.8976×10^{-4}	4.3973×10^{4}	5.4086×10^{4}
Modified RC4	-0.0017	4.4466×10^{4}	5.3705×10^{4}
AES	9.9292×10^{-4}	4.3598×10^{4}	5.4060×10^{4}
Modified AES	-0.0034	4.4448×10^{4}	5.3725×10^{4}

Table (3): The quality of encryption peppers image

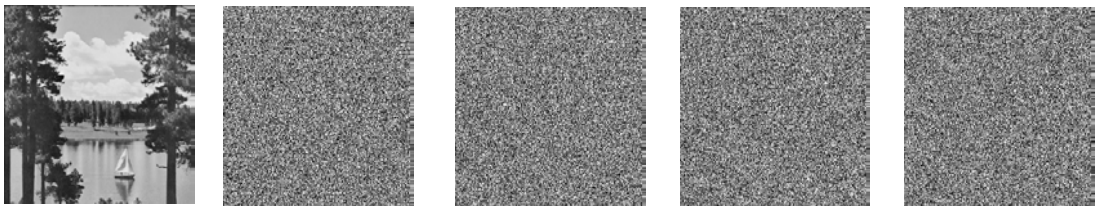
	Quality measures		
Cipher	Dev-1	Dev-2	Dev-3
RC4	0.0017	3.7114×10^{4}	5.7737×10^{4}
Modified RC4	8.3086×10^{-4}	3.7318×10^{4}	5.7465×10^{4}
AES	0.0019	3.7134×10^{4}	5.7789×10^{4}
Modified AES	8.3028×10^{-4}	3.7388×10^{4}	5.7284×10^{4}

From the tables (1-3), it can be shown that the modified encryption algorithms resulted in a better performance (i.e. lower DEV-1, greater DEV-2, lower DEV-3) than compared to using the encryption algorithms alone in all test cases. The scrambling process applied before the encryption algorithms resulted in a lower correlation coefficients. Figures (5 through 7) investigate the visual inspection of the encrypted images. All the encryption algorithms best hide the features of the images.



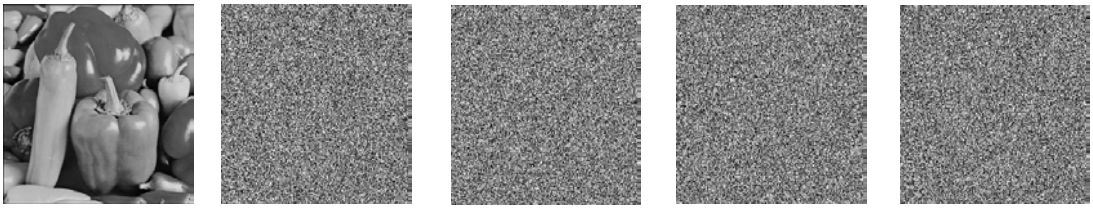
(a) (b) (c) (d) (e)

Figure (5): Encryption of lena image. a) Original image, b) RC4, c) AES, d) Modified RC4, e) Modified AES.



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

Figure (6): Encryption of sailboat image. a) Original image, b) RC4, c) AES, d) Modified RC4, e) Modified AES.



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

Figure (7): Encryption of peppers image. a) Original image, b) RC4, c) AES, d) Modified RC4, e) Modified AES

8. Conclusion

Image data has strong correlation among adjacent pixels. However, it is very important to disturb the high correlation among image pixels to increase the security level of the encrypted images. In this paper, a simple and strong method had been proposed for image security using a combination of image scrambling and encryption techniques. Different test cases showed that the correlation was decreased when the proposed scheme was applied to them before encryption algorithms. Different evaluation measuring factors were considered. With all measuring factors, the proposed scheme had the superior performance in all cases.

9. References

1. Al-Sultanny Y., "***Image Encryption by Cipher Feedback Mode",*** ICIC International, Vol.3, No.3, pp. 589-596, June 2007.
2. Al-Sultanny Y., ***"Test Image Encryption by Output Feedback",*** Journal of Computer Science, Vol.4, No.2, pp.125-128, 2008.
3. Shujun L. and Xuan Z., "***On the security of an Image Encryption Method***", Institute of Image Processing, School of Electronics and Information Engineering, China, Polytechnic University, 2003.
4. Mohammad A., Bani Y., and Aman J., "***Image Encryption Using Block-Based Transformation Algorithm***", IAENG International Journal of Computer Science, Vol.35, No.1, 19 February 2008.
5. Zeghid M., Machhout M., Khriji L., Baganne A., and Tourki R., "***A Modified AES Based Algorithm for Image Encryption***", International Journal of Computer Science and Engineering Vol. 1, No. 1, pp.70-77, March 2007.
6. Hossam H., Hamdy M., and Osama S., "***An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption***", Menoufia University, Faculty of Electronic Engineering, Department of Computer Science & Engineering, 32952, Egypt, Informatica, Vol.31, pp.121–129, 2007.
7. Man Y. R., "***Internet Security: Cryptographic Principles, Algorithms and Protocols***", John Wiley & Sons Ltd, England, Copyright © 2003.
8. Henk C.A. and Van T., "***Encyclopedia of Cryptography and Security***", Springer Science Business Media, Inc, 2005.
9. http://***en.wikipedia.org/wiki/RC4***
10. Bruce S., "***Applied Cryptography: protocol, algorithms, and source code in C***", 2nd edition, John Wiley and Sons, 1996.
11. L. T.Wang and E. J. McCluskey, "***Linear Feedback Shift Register Design Using Cyclic Codes***," *IEEE Transaction Computers*, Vol. 37, No. 10, pp.1302-1306, Oct. 1988.
12. I. Ziedan, M. Fouad, and D. H. Salem, "***Application of Data Encryption Standard to bitmap and JPEG Images***," in Proceedings Twentieth National Radio Science Conference (NRSC 2003), pp.C16, Egypt, March 2003.