EUROPEAN ACADEMIC RESEARCH
Vol. II, Issue 4/ July 2014

Impact Factor: 3.1 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Image Encryption by Using RC4 Algorithm

Dr. ROOJWAAN S. ISMAEL
DR. RAMI S. YOUAIL
SHAHAB WAHHAB
Department of Information and Communication Engineering
Erbil Polytechnic University
Erbil, Iraq

Abstract:

Image encryption has a wide area of application by using different encryption algorithms. Unlike the text encryption, image encryption suffers from redundancy in the plaintext which represents a problem that should be faced. In this paper, a gray-level image encryption is implemented by using RC4 algorithm. RC4 is stream cipher algorithm and it's popular in WEP. After program execution and results assessments, we found that the encrypted image is resistant to several types of cryptanalysis, and it shows a high level of randomness in the ciphertext. Also, the encrypted image has passed the FIPS 140 randomness tests.

Key words: image encryption, RC4 Algorithm, cryptanalysis, randomness tests

1. Introduction

With the high development of communication and Internet technology; the need raised to have a secure communication to exchange confidential information, such information could be audio, video, or image files. One way to have such secure communication is to change the shape of the transmitted data; which is called encryption. In the encryption process, the data is encrypted by using an encryption method and secret key.

In this paper, the RC4 encryption algorithm is used to encrypt an image data file (gray level image); this method is widely used in WEP. After the implementation of this algorithm; the encrypted file is analyzed and subjected to many tests. The encrypted file showed good results during these tests.

Image encryption has been performed using differed methods; in [1] a new image encryption algorithm with a large pseudorandom permutation which is computed from chaotic maps is proposed. Manuscript [2] also used chaotic maps to generate long pseudorandom bits for encryptions. The improvement of the properties of confusion and diffusion in terms of discrete exponential chaotic maps, and design a key scheme for the resistance to statistic attack, differential attack and grey code attack has been performed in [3].

The rest of this paper is organized as follows: section 2 includes a description for the RC4 algorithm. In section 3, an evaluation and analyzation to the proposed method is performed together with results assessment. Finally, the paper ends with the conclusion and references.

2. Algorithm description

RC4 is a variable-key-size stream cipher developed in 1987 by Ron Rivest for RSA Data Security [4]. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key, where the key is independent of the plaintext [5].

RC4 has an 8×8 S-box: S_0, S_1,..., S_{255}. The entries are a permutation of the numbers 0 through 255, and the permutation is a function of the variable-length key. It has two counters, i and j, initialized to zero. To generate a random byte; follow the following pseudo code [4]:

$i = (i + 1) \bmod 256$
$j = (j + Si) \bmod 256$
swap Si and Sj
$t = (Si + Sj) \bmod 256$

K = St

In encryption process, the ciphertext is produced by XORing the byte *K* with the plaintext. While in decryption process, the plaintext is re-produced by XORing the ciphertext with the byte *K*. For more details about RC4 refer to [4,6,7].

3. Experimental results

A secure encryption method must be resistant to many cryptanalysis and attacks and passes several tests, such as histogram analysis and FIPS 140 testing. Our method has been applied to a gray level image JPEG ( ) file format of size 250×250 pixel, see figure 1 for the sample image.

Fig. 1: the sample image

3.1 Histogram test

The biggest problem that faces image encryption and does not exist in text encryption is the redundancy in plaintext. Therefore the used algorithm must give high distribution pixels for the ciphertext image so that the attacker cannot extract any useful information from it.

The following figure compares the histograms of plaintext image and ciphertext image.

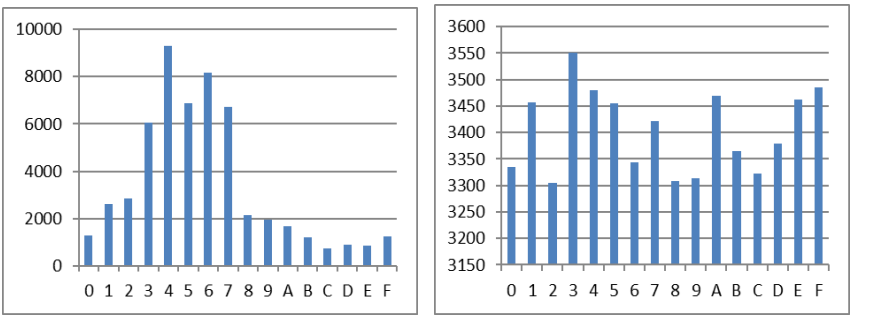

Fig.1: histogram before and after encryption

In the previous figure, the X-axis represents the pixel value, while the Y-axis represents the frequency of each pixel. From figure 1.a, we can see that the image before encryption has a certain distribution; were the pixels are intensive in the middle of the histogram. The maximum value is 9287 and minimum value is 741, the difference is 8546. While after the encryption process, figure 1.b, we notice that the pixels are normally distributed along the X-axis, the maximum value is 3550 and minimum value is 3305, the difference is 245.

3.2 The FIPS 140 tests

After the encryption process, we applied the FIPS-140 four tests to the ciphertext images [8]. Our method had passed these tests with good results.

There are four tests: Monobit, Poker, Runs tests and Long run tests. Each of the tests was designed to test the randomness of a sample sequence length of 20,000 bits as follows [1]:

1. The Monobit test: in this test we need to calculate X which represents the number of 1's in a 20,000 bits stream, the test is passed if $9{,}725 < X < 10{,}275$.
2. The Poker test: Divide the 20,000 bit stream into 5000 contiguous 4 bit segments. Count and store the number of occurrences of each of the 16 possible 4 bit values.

Denote g(i) as the number of each 4 bit value i where i=0,..,15. The calculate Y which is given by:

$$Y = \frac{16}{5000}\sum_{i=0}^{15} g(i)^2 - 5000$$

The test is passed if 2.16 < Y < 46.17.

3. The run test: the run represents the maximum sequence of continues zeros or ones. All runs of all lengths in the sample stream should be counted and stored. The test is passed if the runs of all length are within the given intervals below.

Table 1.

Run length	1	2	3	4	5	≥ 6
Pass value	2315-2685	1114-1386	527-723	240-384	103-209	103-209

4. The Long run test: in this test, the longest run of both zero and one within 20,000 bits must be calculated. The test is passed if the longest run is less than 26.

We applied the previous tests on 50 different samples of random locations from the ciphertext image. The following table represents the results of monobit test and poker test; only ten random runs are picked up.

Table 2. The results of Monobit and Poker tests

The test	Monobit Test	Poker Test
Run 1	10,021	16.3556
Run 2	10,074	29.0848
Run 3	9,957	10.0512
Run 4	10,058	11.472
Run 5	9,974	14.2048
Run 6	10,140	15.0432
Run 7	10,040	16.0256
Run 8	10,087	15.4626
Run 9	9,958	13.4016
Run 10	10,019	9.0048

Table 3 contains the results of run test, the number at the top of each column represents the length of the run.

Table 3. Run test Result

Run length	1	2	3	4	5	≥ 6
Run 1	2523	1236	633	302	156	86
Run 2	2416	1229	635	322	171	79
Run 3	2523	1231	646	324	171	73
Run 4	2528	1224	654	308	155	72
Run 5	2551	1228	608	310	158	83
Run 6	2535	1183	642	330	146	74
Run 7	2543	1250	617	312	146	77
Run 8	2544	1217	626	311	174	84
Run 9	2522	1257	614	307	154	76
Run 10	2544	1219	610	309	154	85

Conclusion

After implementing the proposed encryption scheme; we found that that encrypted image has a very high distribution calculated from histogram, all the pixels are randomly distributed and the different between the higher and lowest value is very small comparing with the difference before encryption. Also the system passed the FIPS test and the results are within the accepted ranges.

REFERENCES:

Chandra, Praphul, Alan Bensky, Tony Bradley, Chris Hurley, Steve Rackley, John Rittinghouse, James F. Ransome, Timothy Stapko, George L. Stefanek, Frank Thornton, and Jon Wilson. 2009. "Wireless Security." Elsevier. [6]

National Institute of Standards and Technology (NIST). 2001. *FIPS pub 140-2: Security requirements for cryptographic modules*. [8]

Oswal, Sumit, Sandeep Rai, and Nikesh Tiwari. 2013. "Secured Image with Pseudorandom Permutation Using longer bit with Chaotic Maps." *International Journal of Digital Signal and Image Processing* (IJDSIP) 1(1). [2]

Schneier, Bruce. 1996. *Applied Cryptography*. Second edition. John Wiley & Sons. [4]

Stallings, William. 2003. *Cryptography and network security: Principles and practice*. Upper Saddle River, New Jersey: Prentice Hall. [5]

Vacca, John R. 2009. *Computer and Information Security. Handbook*. Elsevier. [7]

Yoon, Ji Won and Hyoungshick Kim. 2010. "An image encryption scheme with a pseudorandom permutation based on chaotic maps." Elsevier, 2010. [1]

Zhang, Linhua, Xiaofeng Liao, and Xuebing Wang. 2004. "An image encryption approach based on chaotic maps." Elsevier. [3]