International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-6, June 2016
ISSN: 2395-3470
www.ijseas.com

Digital Image Encryption Based on the RC5 Block Cipher Algorithm

R.Sateesh Kumar[1], I.Navakanth[2]

[1] *Computer Science and Engineering, Vasavi College of Engineering, sateeshramatenki@gmail.com*

[2] *Computer Science and Engineering, Vasavi College of Engineering, i.navakanth@gmail.com*

ABSTRACT- Recent developments in digital image processing and network communications during the past decade have created a great demand for real-time, secure image transmission over the Internet and through wireless networks. Reliable image encryption techniques are of utmost importance for the protection of data from counterfeiting, tampering, and unauthorized access. These image encryption techniques employ a kind of randomness which cannot be inferred by other unauthorized users.

Implementation of the RC5 block cipher algorithm for digital images in different modes of operation. The encryption efficiency analysis of the RC5 block cipher algorithm for digital images is investigated using several metrics including visual testing, maximum deviation, irregular deviation, information entropy, correlation coefficients, avalanche effect, histogram uniformity and key space analysis. The evaluation consists of theoretical derivations and practical experimentation. Experimental results have proved that the RC5 block cipher algorithm can be implemented efficiently for encryption of real-time digital images and demonstrated that the RC5 block cipher algorithm is highly secure from the strong cryptographic viewpoint.

Keywords: RC5, Encryption, Decryption, Correlation Coefficient

1. INTRODUCTION

Recent developments in digital image processing and network communications during the past decade have created a great demand for real-time secure image transmission over the Internet and through wireless networks. Thus, reliable image encryption techniques are of utmost importance for the protection of data from counterfeiting, tampering, and unauthorized access. These image encryption techniques employ a kind of randomness which cannot be inferred by other unauthorized users.

Many digital services require reliable security in storage and transmission of digital images. Due to the rapid growth of the internet in the digital world today, the security of digital images has become more important and attracted much attention. The prevalence of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of users privacy for all applications. Encryption techniques of digital images are very important and should be used to frustrate opponent attacks from unauthorized access.

Digital images are exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. Encryption is the preferred technique for protecting the transmitted data. There are various encryption systems to encrypt and decrypt image data, however, it can be argued that there is no single encryption algorithm which satisfies the different image types.

Most of the available encryption algorithms are used for text data. However due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data.

2. DIGITAL IMAGE ENCRYPTION

2.1 Existing Techniques Used For Digital Image Encryption

Several image encryption methods have been proposed to secure the contents of digital images, but some of them, including public key encryption methods such as RSA and El Gamal, do not provide encryption rates suitable for encryption of large data files and images. Moreover, the security of the majority of public key cryptographic schemes relies on the inability to perform factorization of large numbers or to solve the discrete logarithm

problem in a fast, efficient manner. Recent advances in algorithmic techniques, number theory, and distributed computing have seriously challenged the basis of these techniques. Also, traditional encryption algorithms such as DES, IDEA and Blowfish are not suitable for practical image encryption, especially under the scenario of on-line communications, due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels.

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. The key should be distributed before transmission between entities. Keys play an important role. If weak key is used in algorithm then everyone may decrypt the data. Strength of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key ,DES uses one 64-bits key, Triple DES uses three 64-bits keys while AES uses various (128,192,256) bits keys. Blowfish uses various (32-448) default 128bits while RC6 is used various (128,192,256) bits keys.

2.1.1 EI Gamal

The ElGamal system is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol. The system parameters consist of a prime p and an integer g, whose powers modulo p generate a large number of elements, as in Diffie-Hellman. Alice has a private key a and a public key y, where $y = g^a \pmod p$. Suppose Bob wishes to send a message m to Alice. Bob first generates a random number k less than p.

then computes $y_1 = g^k \pmod p$ and $y_2 = m \text{ xor } y^k$, where xor denotes the bit-wise exclusive-or. Bob sends (y_1, y_2) to Alice. Upon receiving the cipher text, Alice computes $m = (y_1^a \bmod p) \text{ xor } y_2$

The ElGamal signature algorithm is similar to the encryption algorithm in that the public key and private key have the same form, however encryption is not the same as signature verification, nor is decryption the same as signature creation as in RSA.

Analysis based on the best available algorithms for both factoring and discrete logarithms shows that RSA and ElGamal have similar security for equivalent key lengths. The main disadvantage of ElGamal is the need for randomness, and its slower speed. Another potential disadvantage of the ElGamal system is that message expansion by a factor of two takes place during encryption. However, such message expansion is negligible if the cryptosystem is used only for exchange of secret keys.

2.1.2 RC2

RC2 (”Rivest Cipher”) is seen as a replacement for DES. It was created by Ron Rivest in 1987, and is a 64-bit block code and can have a key size from 40 bits to128-bits (in increments of 8 bits). The 40-bit key version is seen as weak, as the encryption key is so small, but is favoured by governments for export purposes, as it can be easily cracked. In this case the key is created from a Key and an IV (Initialisation Vector). The Key has 12 characters (96 bits), and the IV has 8 characters (64 bits), which go to make the overall key. RC2 is a block cipher with a 64-bits block cipher with a variable key size that range from 8 to128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts.

2.1.3 RC 4

RC4 is a stream cipher designed by RSA Data Security. The secure socket layer (SSL) protocol and wireless communications (IEEE 802.11a/b/g) use RC4. It uses a pseudo random number generator, where the output of the generator is XOR’ed with the plaintext. It is a fast algorithm and can use any key-length. Unfortunately the same key cannot be used twice. Recently a 40-bit key version was broken in eight days without special computer power.

Recent developments in digital image processing and network communications during the past decade have created a great demand for real-time, secure image transmission over the Internet and through wireless networks. Reliable image encryption techniques are of utmost. Importance for the protection of data from counterfeiting, tampering, and unauthorized access. These image encryption techniques employ a kind of randomness which cannot be inferred by other unauthorized users.

3.RC5

3.1 BMP File Format

BMP is a graphics format used commonly as a simple graphics file format on Microsoft Windows platform. Sometimes it is called DIB which stands for device-independent bitmap. The BMP file format, also known as bitmap image file or device independent bitmap (DIB) file format or simply

a bitmap, is a raster graphics image file format used to store bitmap digital images, independently of the display device (such as a graphics adapter), especially on Microsoft Windows and OS/2 operating systems.

A device-independent bitmap (DIB) is a format used to define device-independent bitmaps in various color resolutions. The main purpose of DIBs is to allow bitmaps to be moved from one device to another (hence, the device-independent part of the name). A DIB is an external format, in contrast to a device-dependent bitmap, which appears in the system as a bitmap object. A DIB is normally transported in metafiles, BMP files.

The bitmap image file consists of fixed-size structures (headers) as well as variable-size structures appearing in a predetermined sequence. Many different versions of some of these structures can appear in the file, due to the long evolution of this file format. A bitmap image file loaded into memory becomes a DIB data structure – an important component of the Windows GDI API. The in-memory DIB data structure is almost the same as the BMP file format, but it does not contain the 14-byte bitmap file header and begins with the DIB header. For DIBs loaded in memory, the color table can also consist of 16 bit entries that constitute indexes to the currently realized palette (an additional level of indirection), instead of explicit RGB color definitions. In all cases, the pixel array must begin at a memory address that is a multiple of 4 bytes. In non-packed DIBs loaded in memory, the optional color profile data should be located immediately after the color table and before the gap1 and pixel array.

3.2 RC5 block cipher algorithm

The RC5 block cipher algorithm is a parameterized symmetric encryption algorithm, and it can be represented with the notation of RC5-w/r/b, where w/r/b are reconfigurable parameters.

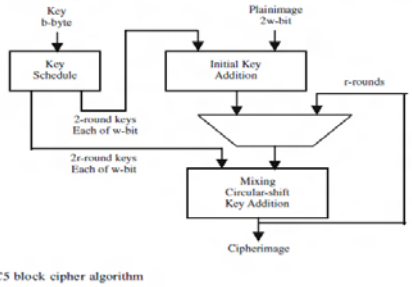


Figure 3.1 the RC5 Block Cipher Algorithm

1. w is the word size in bits and its standard value is 32 bits; allowable values are 16, 32, and 64 bits. The RC5 encryption algorithm encrypts two-word blocks so that the plain image and cipher image blocks are each 2w bits long.
2. r signifies the number of rounds. The number of rounds can range from 0 to 255.
3. b signifies the number of bytes in the secret key K. The secret key size can range from 0 bits to 2,040 bits in size.
4. The RC5 algorithm consists of three components: a key expansion algorithm, an encryption algorithm, and a decryption algorithm.
5. The RC5 algorithm uses three primitive operations and their inverses. Addition/subtraction of words modulo 2^w , where w is the word size.

3.3 Key Expansion (Schedule) Algorithm

The key-expansion routine expands the user's secret key K to fill the expanded key array S, so that S resembles an array of t = 2r +2 random binary words determined by K.

The key expansion algorithm uses two magic constants, and consists of three simple algorithmic parts. These parts are the conversion, the initialization, and the mixing, respectively.

3.4 Encryption Efficiency Evaluation of RC5 Algorithm to Digital Images

3.4.1 Visual Testing of the RC5 Block Cipher Algorithm to Digital Images

We have conducted some experiments to test the encryption efficiency of the RC5 block cipher algorithm for application to digital images. As stated previously, we must firstly extract the image header for the image to be encrypted/decrypted before applying the RC5 algorithm. Then, we can apply the RC5 algorithm to the image. There is no visual information observed in the encrypted image, and the encrypted images are visually indistinguishable even with a big difference with respect to the original images.

3.4.2 The Correlation Coefficient

Correlation is a measure of the relationship between two variables. If the two variables are the plain image and cipher image, then they are in perfect correlation if they are highly dependent. In this case, the cipher image is the same as the plain image and the encryption process failed in hiding the details of the original image. If the correlation coefficient equals zero, then the plain image and its cipher image are totally different. If the correlation coefficient equals -1, this means the cipher image is the negative

of the plain image. Therefore, success of the encryption process corresponds to smaller absolute values of the correlation coefficient. The correlation coefficient is measured by the following equation.

$$\frac{cov(x,y)}{\delta_x \delta_y} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \quad (15)$$

Where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$

x and y are gray scale values of the plain image and cipher image. The procedure to test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in plain image/ cipher image.

3.4.3 Maximum Deviation

The maximum deviation measures the encryption efficiency in terms of how it maximizes the deviation between the original and the encrypted images.

The steps of this procedure were as follows:

1. Count the number of pixels of each grayscale value in the range from 0 to 255 and present the results graphically (in the form of curves) for both original and encrypted images (i.e.; get their histogram distributions).
2. Compute the absolute difference or deviation between the two curves and present it graphically.
3. Count the area under the absolute difference curve, which is the sum of deviations (D) and this represents the encryption quality.

$$D = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i$$

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

3.4.4 The Avalanche Effect Measuring Factor

Diffusion is an important parameter that must be measured to judge the encryption algorithm randomization. A desirable property for the RC5 block cipher algorithm is that it is highly sensitive to small changes in the plain image (single bit change in plain image).

In general, the opponent may make a slight change such as modifying only one pixel of the original image, and then observes the change of the result. In this way, he may find out a meaningful relationship between the plain image and the cipher image.

As one minor change in the plain image can cause a significant change in the cipher image, this differential attack would become very inefficient and practically useless. If an algorithm has a good diffusion characteristic, the relation between the encrypted image and the original image is too complex and cannot be predicted, easily. To measure the diffusion of any algorithm, a bit is changed in the Plain image, and the difference between the encrypted image obtained from the original plain image and the encrypted image obtained from the modified one is obtained.

To test the influence of one-pixel change on the whole image encrypted by the RC5 algorithm. Let two ciphered images, whose corresponding plain images have only one pixel difference, be denoted by C_1 and C_2. Label the grey-scale values of the pixels at grid (i,j) in C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$, respectively. Define a bipolar array, D, with the same size as images C_1 and C_2. Then, D(i, j) is determined by $C_1(i, j)$ and $C_2(i, j)$, namely, if $C_1(i, j) = C_2(i, j)$, then D(i, j) = 1; otherwise, D(i, j) = 0.

The NPCR is defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

Where W and H are respectively the width and height of C_1 or C_2. NPCR measures the percentage of different pixel numbers between these two images.

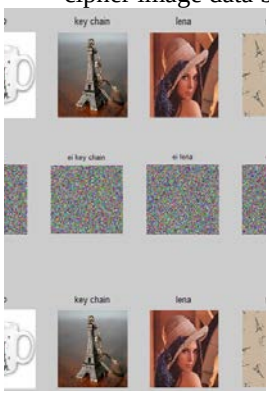
3.5.5 Key Space Analysis

A good image encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute-force attacks infeasible. For the RC5 block cipher, the key space analysis and testing have been carefully performed and completely carried out.

4.RESULTS

The encryption process takes a plain image input and produces a cipher image as the output. In the encryption process of the RC5 image encryption, the image header is extracted from the image to be encrypted and the image data stream is divided into 2wbit blocks. The first 2w-bit block of image is entered as the plain image to the encryption process of the RC5 algorithm. Then, the next 2w-bit plain image block follows it, and so on with the scan path until the end of the plain image data bit stream. The key-expansion process must have already been performed before this process. In the decryption process, the cipher image is also divided into 2w-bit blocks. The 2w-bit cipher image is entered to the RC5 decryption algorithm and the

Same expanded secret key is used to decrypt the cipher image but the expanded secret key is applied in a reverse manner. Then the next 2w-bit cipher image block follows it, and so on until the end of the cipher image data bit stream.



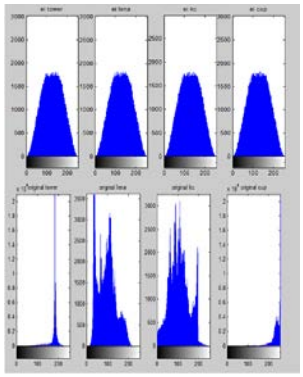


Figure 4.1 Original, encrypted and decrypted images

Figure 4.3 Encrypted and Original Images Histograms

Key Space Analysis

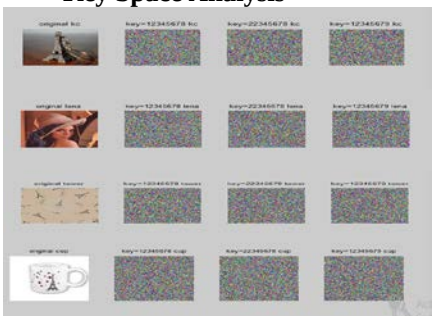


Figure 4.2 Original Images and Encrypted Images Using Key=12345678, Key=22345678 and Key=12345679

Correlation coefficient

Image Name	ECB
Lena	0.002
Cup	0.004
Tower	0.068

Table 4.1 Correlation coefficient of Original Images and Different Modes Images

Maximum Deviation

Image Name	ECB	Mc / CE
Lena	153260	15
Tower	414262	39
Cup	475876	46
Key Chain	114734	11

Table 4.2 Maximum Deviation of Original Images and Different Modes Images

V. CONCLUSION

The RC5 block cipher algorithm has been shown to be an excellent alternative for the encryption of digital images due to characteristics such as variable word size, variable number of rounds, variable-length secret key and the heavy use of data dependent rotations.

VI. REFERENCES

[1] William Stallings, *Cryptography and network security*, 5th Edition.
[2] Dr Dobbs Journal, Rivest, R. L , *RC5 encryption algorithm*. (1995).
[3] Rivest, R. L ,The RC5 encryption algorithm. MIT Laboratory for Computer Science, (1997).
[4] Furht, B., & Socek, D, *A survey of multimedia security technical report*, (2003).
[5] Ahmed, H. E. H., Kalash, H. M, & Allah, O. S. F, *An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption*, International Journal of Computer information, (2007).
[6] Ahmed, H. E. H., Kalash, H. M., & Allah, O. S. F, *An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption*, An International Journal of Computing and Informatics, (2007).
[7] Shannon C.E, Communication theory of secrecy system, Bell System Technical Journal, (1949).
[8] http://theory. lcs. mit. cdu/-rivest/Rivest-rc5rev. pdf
[9] ftp://ds.internic.net/rfc/rfc2040.txt.
[10] http://theory.lcs.mit.edu/*rivest/Rivest-rc5rev.pdf.
[11] Ronald L.Rivest,"RC5 Encryption Algorithm", Dr Dobbs Journal, Vol. 226, PP. 146-148, Jan 1995.
[12] Ronald L. Rivest, the RC5 Encryption Algorithm, MIT Laboratory for Computer Science 545 Technology Square, Cambridge, Mass. 02139 (Revised March 20, 1997).