MODIFICATION OF RC6 BLOCK CIPHER ALGORITHM ON DIGITAL IMAGE

Mardiana¹, Fajrillah², Yuyun Dwi Lestari³, Ummul Khair⁴

¹Department of Informatics, Sekolah Tinggi Teknik Harapan, Medan, Indonesia
²Department of Management, STIE IBBI, Medan, Indonesia

Abstract. In the digital image of each pixel consists of three components, namely R, G, and B. If the three components are combined in a block then the block will have data with 24 bit or three characters. By default shortage of bits in each block will be filled by the next bit of the pixel so that each block will have the appropriate size is 32bit. The problem that happens is if the number of pixels is not in accordance with the division so it is necessary to block or adding padding bit 0 in register block, if padding occurs then the encrypted data size will change that affects the size of the image will change and will be hard pressed in preparing the return data encryption results in the form of images.

Keywords: RC6 Modification, Block Cipher, Digital Image, Encryption

1. Introduction

The importance of the security of digital images is increasing nowadays since the raise of communications using digital products over the network. Some experiments have been investigated over the encryption methods as the most important key to secure digital data [1-7]. DES (Data Encryption Data), RAS, and IDEA (International Data Encryption Algorithm) [8-10] have been studied to have a long computational time to process an image and need more power to compute the data. Besides, they also have some problems to secure the digital images [11]. Li et al that studied about a new chaotic key-based algorithm (CKBA) also found that CKBA method is not very secure, especially if it is seen from cryptographic viewpoint [12].

RC6 (Ron's Code 6) is an evolutionary method of RC5 block cipher. It is an encryption method which is easy to be applied for data security [14]. It has received much attention due to its simpler design. The difference between RC6 and RC5 is in the number of working registers used in the system. The addition of these working registers enhances the quality of security, decreases the rounds, and raises the throughput. Ahmed et al found that this method can be considered to be one of a real-time secure symmetric encryption for digital data such as digital images [11].

However, RC6 is found to have a problem with the RGB digital images which have an odd pixel size. The problem is happened if the number of pixels does not match the division of the block so that the padding is required. If padding occurs then the data size of the encryption will change. This condition will affect the image size, so it will be very to compile the data to returned it into the form of image.
Therefore, in this study, we proposed the modification of RC6 by changing the number of bits in every A, B, C, and D register and altering the constants P and Q. We studied the implementation of those two parameters in the digital images application. The comparation between the RC6 and the modified of RC6 is also given to evaluate the effectiveness of modified RC6.

2. Methodology

The encoding is done on each image pixel according to the width and height of the image. This is possible considering an image is a row of pixels that have components R (Red), G (Green), and B (Blue). These components are integers so they can be operated by converting them to ASCII form first.

RC6 is a chipper block method that uses four blocks of registers with each size of 32-bits. In other words each block will store four characters. In a digital image each pixel consists of three components: R, G, and B. If the three components are combined in a block then the block will have data of 24-bits or three characters. By default the lack of bits on each block will be filled by the bits of the next pixel so that each block will have a corresponding size of 32-bits.

In addition, RC6 algorithm is broadly divided into three algorithms, namely,

1. The Key Generation Algorithm. It is an algorithm used for key initialization that will be used in each round in both encryption operation and decryption operation.

2. Encryption Algorithm is an algorithm used for the changing operation of plaintext encryption into chipertext

3. Decryption Algorithm is an algorithm used for the changing operation of decryption to plaintext

The problem that occurs in RC6 algorithm is if the number of pixels does not match the division of the block so it needs a padding or the addition of bit 0 in the block register, if padding occurs then the data size of the encryption will change which affect the image size will change and will be very difficult in the rearrangement Encrypted data into image form. To overcome these problems then the modified RC6 algorithm was created.

The modified RC6 is done by changing the number of bits so that the constants of Pw and Qw are altered as well. For the RC6 algorithm, the value of Pw and Qw constants are 32 bits. The expansions of them have 8 digits with each digit containing 4 pixels. On the modified mode of RC6 algorithm, Pw and Qw constants only have 24 bits; so, there are 2 unused key expansions which means that the key expansion is reduced by 8 bits value. The difference in the registers is shown in the Figure 1.
In this paper, to compare between RC6 and modified RC6, some investigations are done by applying RC6 as well as modified RC6 to several digital images. The images used in this investigation are in the format of BMP, JPG, or JPEG.

The first stage was the encryption process. In this stage, the pixel value of the images was then read and converted into RGB value. This value was converted again to ASCII, and being encrypted by whether RC6 or modified RC6. When the encryption process occurred, the key was input into the data. After encryption process had done, the image was converted again into RGB value and then to pixel value, after that the image was saved in an encrypted form.

The second stage was the decryption process. The steps in this process are roughly the same as in the encryption process. After this process happened, the image had returned into its initial form.

3. Result and Discussion

3.1. Analysis of RC6 in the application of grayscale images

As have been reported by Ahmed et al that the use of RC6 in the grayscale digital images having size of 256 x 256 can be efficiently done [11]. It can be explained as the result of the limitation of the images size itself, i.e. 256 x 256. This number will ease the allocation of the value of every colors since every pixel has one value for each. That size limitation also makes the appearance of padding to be small or no padding since the total value of the size is calculated to be 4096; in other words, there are 16384 pairs of blocks, an even value. The same case also occurs when the images size is 512 x 512 since the total value of it is calculated to be 16384 as well.

3.2. Analysis of RC6 in the application of RGB images

In this study, RC6 algorithm is applied to two types RGB images, the first one is a picture that has an odd pixel size and the second one is an image that has even pixel size. The odd pixel being used is 591 x 616 in size and the even one is having size of 100 x 100.
An odd pixel size, 591 x 616, gives the total bit of 8737344, so the total block pairs are 68260.5. This number is not an integer, this padding is needed. As shown in the Figure 2, After the encryption process occurs, the type of image changes from JPG to BMP, it has padding at the edge of the picture (shown by an arrow). Then, after the decryption process happens, the picture cannot return to its original form because there is padding in it.

![Application of RC6 algorithm to a chosen plainimage which has size 591 x 616](image1.png)

**Fig.2** Application of RC6 algorithm to a chosen plainimage which has size 591 x 616

Therefore, an even pixel size is investigated, we use the size of 100 x 100 which gives the total block pairs to be 1875, an even value. Thus, after applying RC6 algorithm, the type of image changes from JPG to BMP. It does not have padding on the image because the total bit which exists in the picture meet the needs of the block; so, the original image can be returned. This process can be seen in the Figure 3.

![Application of RC6 algorithm to a chosen plainimage which has size 100 x 100](image2.png)

**Fig.3** Application of RC6 algorithm to a chosen plainimage which has size 100 x 100

### 3.3. Analysis of modified RC6 in the application of RGB images

Because of the problem of padding as mentioned above, we modify the RC6 algorithm that we called as modified RC6 (M-RC6). In this algorithm, we change the internal key generator based on the secret key ‘K’ to fill in the ‘S’ key table, where the size of the S key table is calculated as follows,

\[ t = 2 (r + 1) \text{ words} \quad (1) \]

The modification uses 2 magic constants, i.e., Pw and Qw which have function to generate the internal keys. The internal key generator of RC6 algorithm itself was altered from 32 bits to 24 bits; so the value of Pw and Qw also changes. In the RC6, the value of Pw is b7e15163, whereas the value of Qw...
is 9e3779b9. Due to the decrease of bit number from 32 to 24, the value of Pw becomes b7e151 and
the value of Qw becomes 9e3779. Thus, the blocks A, B, C, and D are changed as well. As shown in
the Figure, the modification of the bit number lets one pixel to be enough to fill in one block, so there
is no padding needed since the RGB components can be borrowed from their neighbor blocks.
Besides, modified RC6 can reduce the capacity or size of variables used during the process, thus
making the process to be more efficient in consuming the memory as well as to be faster.

![a) Original image  b) Encrypted image  c) Decrypted image](image)

**Fig.4 Application of modified RC6 algorithm to a chosen plain image**

We have attempted to apply this modified RC6 algorithm to some images and those images always
can be returned to their original form as shown in the Figure 4.

**IV. Conclusion**

1. RC6 algorithm uses four block blocks with each size of 32 bits, while modified RC6 uses four
registers block with each size of 24 bits. Thus, modified RC6 is more suitable for color images
because each color image pixel has 24 bits.

2. RC6 algorithm is well applied to a greyscale image. However, it is not suitable to be used in the
color images due to padding problems. It can only be used in some certain pixel sizes.

3. Modified RC6 can solve the padding problems that occur in digital images by changing the size of
each block on the A, B, C, D blocks from 32 bits to 24 bits, so that one pixel is sufficient to fill a
block. In the other word, no padding is required.

4. Modified RC6 can reduce the capacity or size of variables used during the process, thus making the
process to be more efficient in consuming the memory and to be faster.

**References**

[1] Howard Cheng and Xiaobo Li, “Partial encryption of compressed images and videos,” *IEEE
Trans. Signal Processing*, vol. 48, no. 8, pp. 2439-2451, 2000.
[2] Masaki Miyamoto, Kiyoshi Tanaka, and Tatsuo Sugimura, “Truncated Baker transformation and its extension to image encryption,” in *Proc. SPIE*, 1999, vol. 3814, pp. 13-25.

[3] Jiri Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” *Int. J. Bifurcation and Chaos*, vol. 8, no. 6, “Fast encryption of image data using chaotic kolmogrov flows,” *J. Electronic Imaging*, vol. 7, no., pp. 1259-1284, 1998.

[4] Philip P. Dang and Paul M. Chau, “Image encryption for secure internet multimedia applications,” *IEEE Trans. Consumer Electronics*, vol. 46, no. 3, pp. 395403, 2000.

[5] Josef Schringer, 2, pp. 318-325, 1998.

[6] C. Alexopoulos, Nikolaos G. Bourbakis, and N. Ioannou, “Image encryption method using a class of fractals,” *J. Electronic Imaging*, vol. 4, no. 3, pp. 251-259, 1995.

[7] Henry Ker-Chang Chang and Jiang-Long Liu, “A linear quadtree compression scheme for image encryption,” *Signal Processing: Image Communication*, vol. 10, pp. 279-290, 1997.

[8] National Bureau of standards. "Data Encryption Standard," Federal WXHL 255 Information processing standards Publication 46, US Government Printing Office, Washington, D.C., 1977.

[9] W. Stallings., "Network and Internetwork Security: Principles and Practice," Prentice-Hall, New Jersey, 1995.

[10] B. Schneier, "Applied Cryptography - Protocols, algorithms, and source code in C," John Wiley & Sons, Inc., New York, second edition, 1996.

[11] Ahmed, Hossam El-din H., Hamdy M. Kalash, and OS Farag Allah. "Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images." In *Electrical Engineering, 2007. ICEE’07. International Conference on*, pp. 1-7. IEEE, 2007.

[12] Li, Shujun, and Xuan Zheng. "Cryptanalysis of a chaotic image encryption method." In *Circuits and Systems, 2002. ISCAS 2002. IEEE International Symposium on*, vol. 2, pp. II-II. IEEE, 2002.

[13] R.L. Rivest, "RC5 Encryption Algorithm," Dr Dobbs Journal, vol. 226, pp. 146-148, Jan. 1995.

[14] R.L. Rivest, M.J.B. Robshaw, R.Sidney, and Y.L. Yin, "The RC6TM Block Chiper,” v.1.1, August 20, 1998.