Encryption quality analysis of the RC5 block cipher algorithm for digital images

Article *in* Optical Engineering · October 2006

DOI: 10.1117/1.2358991

3 authors, including:

Hossam. Ahmed
Facu;ty of Electronic Engineering, Minoufiya University
25 PUBLICATIONS **289** CITATIONS
SEE PROFILE

Osama S. Faragallah
Menoufia University
160 PUBLICATIONS **1,284** CITATIONS
SEE PROFILE

Encryption quality analysis of the RC5 block cipher algorithm for digital images

Hossam El-din H. Ahmed
Hamdy M. Kalash
Osama S. Farag Allah
Menoufia University
Department of Computer Science and Engineering
Faculty of Electronic Engineering
Menouf-32952, Egypt
E-mail: Osam_sal@yahoo.com

Abstract. We investigate the implementation and application of the RC5 block cipher algorithm for digital images and provide testing, verification, and encryption efficiency of the RC5 block cipher for digital images. We describe briefly the basic design parameters of the RC5 block cipher and its implementation for digital images. A complete specification for the method of application of the RC5 block cipher to digital images is given. Several test images are used for inspecting the validity of the encryption and decryption algorithms. Also, we provide and introduce a mathematical measure for encryption efficiency, which we will call the encryption quality instead of visual inspection, and apply it to several images. The encryption quality of the RC5 block cipher algorithm is investigated along its several design parameters, such as word size, number of rounds, and secret key length, and the optimal choices for the best values of these design parameters are given. [DOI: 10.1117/1.2358991]

Subject terms: block cipher; image encryption; encryption quality.

Paper 050359RR received May 14, 2005; revised manuscript received Feb. 6, 2006; accepted for publication Mar. 28, 2006; published online Oct. 11, 2006.

1 Introduction

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 field of encryption is becoming very important in the present era in which information security is of utmost concern. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in Internet communication, multimedia systems, medical imaging, telemedicine, military communication, pay TV, confidential video conferencing, etc.

In this regard, a variety of encryption schemes have been proposed to mask the image data streams, such as (Data Encryption Standard DES),[1,2] optical encryption,[3–8] (International Data Encryption Algorithm IDEA).[9–11] and RSA.[12] However, these encryption schemes appear not to be ideal for image applications, due to some intrinsic features of images such as bulk data capacity and high redundancy, which are troublesome for traditional encryption.

In real-time communication, due to their low encryption and decryption speeds, these algorithms may introduce significant latency. From these encryption algorithms, RC5 was chosen because it has the following advantages over other algorithms[13]:

- RC5 is a simple, fast block cipher and is suitable for hardware or software implementation.
- RC5 is adaptable to process different word lengths.
- RC5 is iterative in structure, with a variable number of rounds.
- RC5 has a variable-length secret cryptographic key.
- RC5 has a low memory requirement and provides high security.
- RC5 uses a new cryptographic primitive, which is the heavy use of data-dependent rotations.

This paper focuses on the application of the RC5 block cipher to digital images, examining a mathematical measure for encryption quality that can be used to investigate the RC5 block cipher along its several design parameters, such as word size, number of rounds, and secret key length. The optimal values of these design parameters are obtained.

The rest of the paper is organized as follows: Current image encryption schemes are introduced briefly in Sec. 2. In Sec. 3, we compare these encryption algorithms and give a brief description of the architecture and specification of the RC5 block cipher algorithm. Image encryption/decryption with the RC5 block cipher is explored in Sec. 4. Testing, verification, and efficiency of application of RC5 to digital images are given in Sec. 5. Section 6 discusses encryption quality analysis of the RC5 block cipher for digital images, including measurement of encryption quality. Experimental results are also included in Secs. 5 and 6.

2 Image Encryption Algorithms

2.1 *Encryption Algorithm for Image Cryptosystems*

Chang, Hwang, and Chen[14] use one of the popular image compression techniques, vector quantization (VQ), to design an efficient cryptosystem for images. The scheme is based on VQ, cryptography, and other number theorems. The images are first decomposed into vectors and then sequentially encoded vector by vector.

0091-3286/2006/$22.00

2.2 *Mirror-Like Image Encryption Algorithm*

Guo and Yen[15] have presented an efficient mirror-like image encryption algorithm. Based on a binary sequence generated from a chaotic system, an image is scrambled according to the algorithm.

2.3 *Chaotic Image Encryption Algorithm*

Yen and Guo[16] have proposed a new image encryption scheme based on a chaotic system. In their method, an unpredictable chaotic sequence is generated and then used to re-create a binary sequence. According to the binary sequence, an image's pixels are rearranged.

2.4 *Lossless Image Compression and Encryption Using SCAN*

Maniccam and Bourbakis[17] have presented a methodology that performs both lossless compression and encryption of binary and grayscale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. SCAN is a formal language-based, two-dimensional, spatial-accessing methodology that can efficiently specify and generate a wide range of scanning paths or space-filling curves.

2.5 *Image Encryption Using Digital Signatures*

A technique was proposed to encrypt an image for secure-image transmission.[18] The digital signature of th e original image is added to the encoded version of the original image. Image encoding is done by using an appropriate error control code, such as a Bose-Chaudhuri-Hochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature can be used to verify the authenticity of the image.

2.6 *Color Image Encryption Using Double Random Phase Encoding*

Zhang and Karim[19] have proposed a method to encrypt color images using existing optical encryption systems for grayscale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, the image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their (Red-Green-Blue RGB) formats.

2.7 *Visual Cryptography for Color Images*

Visual cryptography uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Hou[20] has proposed three methods for visual cryptography. The gray-level visual cryptography method first transforms the gray-level image into a halftone image and then generates two transparencies of visual cryptography. Obviously, we cannot detect any information about the secret image from the two shared transparencies individually, but when they are stacked together, the result clearly shows the secret image. Method 1 uses four halftone images—cyan, magenta, yellow, and black—to share the secret image. The codes of the four shared images are fully disordered, and we cannot perceive any clue of the original secret image from any single shared image. Method 2 reduces the inconvenience of method 1 and requires only two shared images to encrypt a secret image. However, after stacking the shared images generated by method 2, the range of color contrast will be 25% of that of the original image. Method 3 loses less image contrast, which is better than method 2.

3 Comparison with the RC5 Block Cipher Algorithm

3.1 *Comparison of Current Algorithms*

A brief comparison of the current image encryption schemes is given in Table 1. Detailed properties of each method are introduced following.

A major advantage of the VQ algorithm, proposed by Chang, Hwang, and Chen,[14] is its simple hardware structure. The required bit rate of VQ is small. Since VQ compresses the original image into a set of indices in the codebook, we can save a lot of storage space and channel bandwidth. The simple hardware structure provides a fast decoding procedure.

The mirror-like image encryption algorithm[15] and chaotic image encryption algorithm[16] are similar in nature. Both algorithms use a binary sequence generated from the chaotic system to rearrange image pixels. These algorithms do not have any compression scheme and authenticity verification. However, they perform lossless image encryption/decryption, which transforms images into a chaotic state very quickly.

The algorithm that uses SCAN language[17] has lossless image compression and encryption abilities.

The image encryption using digital signatures[18] algorithm encrypts the image and embeds the digital signature in the image prior to transmission. This encryption technique provides three layers of security. In the first step, an error control code is used that is determined in real time, based on the size of the input image. Without the knowledge of the specific error control code, it is very difficult to obtain the original image. The dimension of the image also changes due to the added redundancy. This poses an additional difficulty to decrypting the image. Also, the digital signature is added to the encoded image in a specific manner. At the receiver end, the digital signature can be used to verify the authenticity of the transmitted image.

The color image encryption using double random phase encoding[19] technique introduces color information to optical encryption. An RGB color image is converted to an indexed image before it is encrypted using typical optical security systems. At the decryption end, the recovered indexed image is converted back to the RGB image.

The most notable feature of the visual cryptography for color images approach is that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from some overlapping shared images, thus overcoming the disadvantage of complex computation required in traditional cryptography. The contrast of the stacked image is somewhat degraded, but the content of the image can still be easily identified.

Table 1 Comparison of current image encryption algorithms.

				Classification type				
Algorithm	Compression	Loss	Authenticity	Value transformation	Position permutation	Visual transformation	Advantage	Disadvantage
IEDS	No	No	Yes	Yes	No	No	Authenticity verification	Increment in image size. Does not have any compression scheme.
SCAN	Yes	No	No	Yes	No	No	Lossless compression, strong encryption	Compression-encryption takes longer time.
MIE	No	No	No	Yes	No	No	Lossless image encryption-decryption	Does not have any compression scheme and authenticity verification.
CIE	No	No	No	No	Yes	Yes		
VQ	Yes	No	No	No	Yes	No	Lossless compression, simple hardware structure, small bit rate of VQ	Does not have any authenticity verification.
DRP	No	No	No	Yes	No	No	Less complexity	Does not have any compression scheme and authenticity verification.
VC	No	Yes	No	No	No	Yes	No complex computation	

IEDS-Image encryption using digital signatures
SCAN-Lossless image compression and encryption using SCAN
MIE-Mirror-like image encryption
CIE-Chaotic image encryption
VQ-A new encryption algorithm for image cryptosystems
DRP-Color image encryption using double random phase encoding
VC-Visual cryptography for color images

3.2 *Architecture and Specification of the RC5 Block Cipher*

The RC5 block cipher is a fully parametrized family of encryption algorithms. It has a variable word size w, a variable number of rounds r, and a variable-length secret key b. A version of the RC5 block cipher is more accurately specified as RC5-$w/r/b$. The encryption and decryption algorithms are exceptionally simple, as shown in Refs. 21 and 22. The RC5 block cipher converts plaintext data blocks of 16, 32, and 64 bits into ciphertext blocks of the same length. It uses a key of selectable length b (0, 1, 2, …, 255) bytes.

The algorithm is organized as a set of iterations, called rounds r, that takes values in the range (0, 1, 2, …, 255), as illustrated in Fig. 1.

An expanded key array is created from the original key by means of a key schedule. The expanded key array is used with both encryption/decryption routines, and its length is dependent on the number of rounds. The operations performed on the data blocks include bit-wise

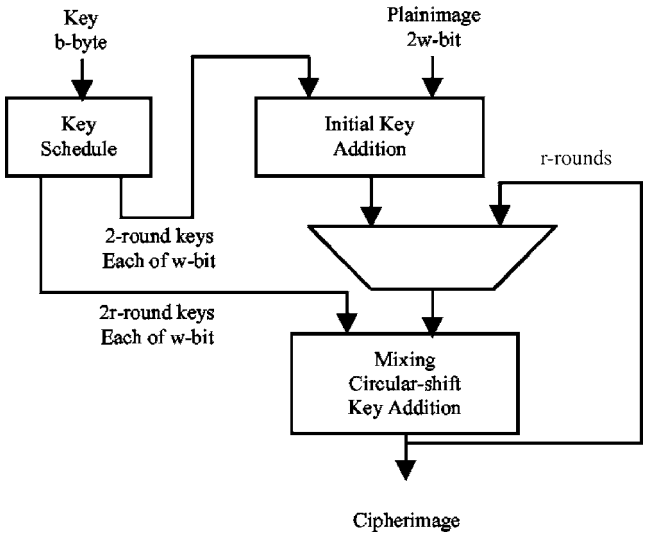

Fig. 1 RC5 encryption algorithm.

Table 2 Summary of RC5-*w*/*r*/*b* parameters.

Parameter	Definition	Values
w	Word size in bits	16, 32, 64
r	Number of rounds	0,1,2,…,255
b	Number of bytes in secret key	0,1,2,…,255

exclusive-OR of words, data-dependent rotations by means of circular left and right rotations, and two's complement addition/subtraction of words, which is modulo-2^w addition/subtraction, where *w* is the word size in bits. These operations always affect a complete 16-, 32-, or 64-bit data block at a time. A summary of the RC5 design parameters appears in Table 2.

4 Image Encryption and Decryption with the RC5 Algorithm

There are two inputs to the encryption function, the plainimage to be encrypted and the expanded secret key. For RC5 image encryption, all parts of the file header are determined to find the start of the image pixels data array, and the image header on which the encryption is performed is excluded. The image data bit stream (not including the Image) is divided into blocks of 64-bit length. The first 64-bit block of the image is entered as the plainimage to the encryption function of RC5. The second input to the RC5 encryption algorithm is the expanded secret key that is derived from the user-supplied secret key by means of the key schedule. The key schedule is an important component of a block cipher, since it computes the round keys from the user-supplied secret key. The next 64-bit plainimage block follows, and so on, with the scan path shown in Fig. 2, until the end of the image data bit stream. Figures 3 and 4 show flow charts for encryption with both the RC5-*w*/*r*/*b* and the key expansion (scheduler) algorithm.

In the decryption process, the encrypted image (cipherimage) is also divided into 64-bit blocks. The 64-bit cipherimage is entered in the RC5 decryption algorithm, and the same expanded secret key is used to decrypt the cipherimage, but the expanded secret key is applied in a reverse manner. Then the next 64-bit cipherimage block follows, and so on with the same scan path.

5 Test, Verification, and Efficiency of Application of the RC5 Block Cipher to Digital Images

In this section, some experimental results are given to check the efficiency of the RC5 block cipher for application to digital images. We try to apply the RC5 block cipher to several digital images. As stated previously, we must first extract the image header for the image to be encrypted/decrypted before application of the RC5 block cipher. So we must study the file format for the image to determine all parts of the file header and to determine the beginning of the data stream to be encrypted.[23–26] Then the RC5 block cipher is applied to the image.

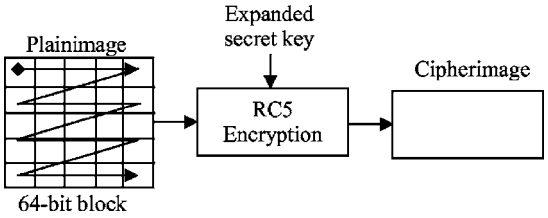

Fig. 2 RC5 image encryption process.

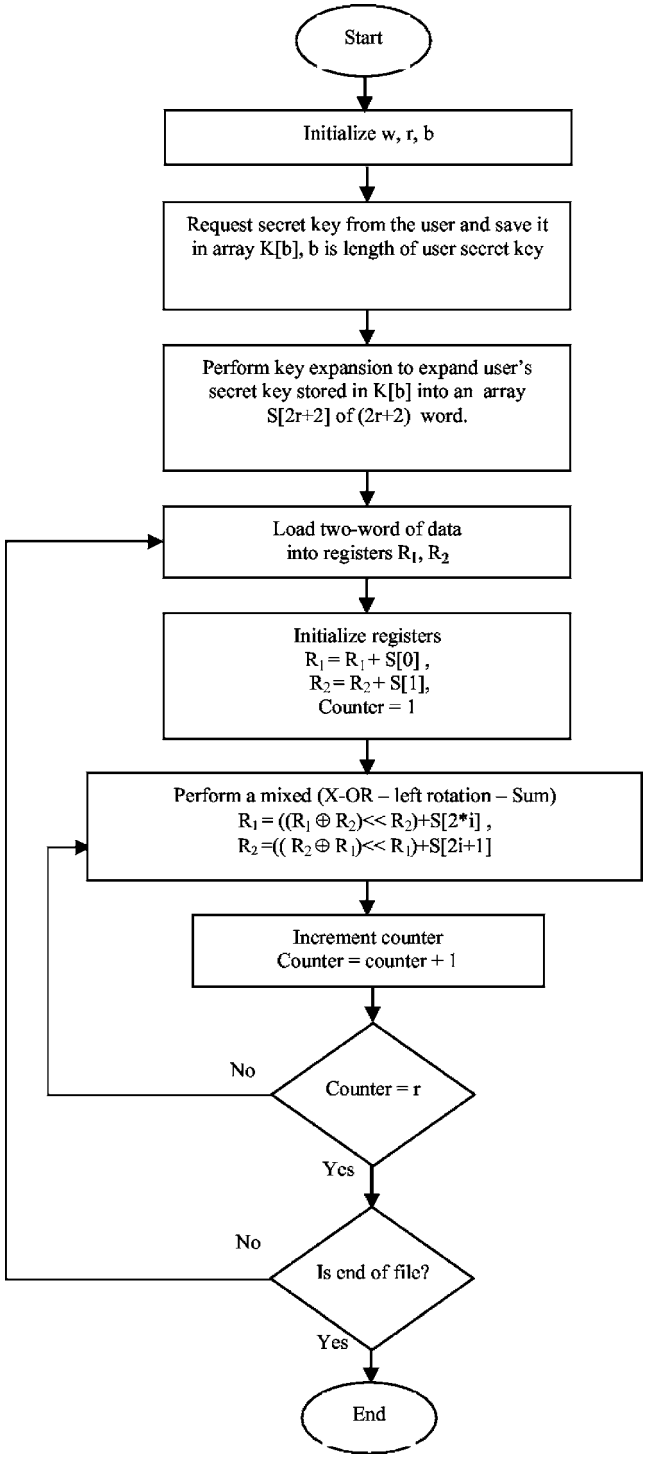

Fig. 3 Encryption flowchart with RC5-*w*/*r*/*b*.

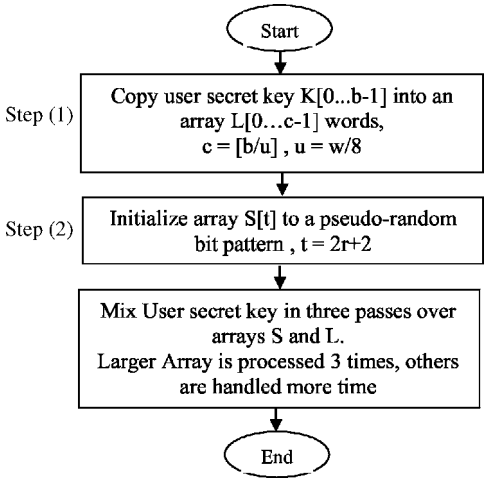

Fig. 4 Flowchart of key expansion (scheduler) algorithm.

We use the grayscale images Lena and Cman, each of size 256×256 and grayscale (0 to 255), as the original images (plainimages), and we use RC5-32/12/16.

Figures 5 and 6 show the result of the RC5 block cipher for the Lena and Cman images in both encryption and decryption. Visual inspection of Figs. 5 and 6 shows the possibility of applying the RC5 block cipher to digital images successfully in both encryption and decryption.

6 Encryption Quality Analysis of the RC5 Block Cipher

All previous studies on image encryption[27–30] were based on visual inspection to judge the effectiveness of the encryption technique used in hiding features. Visual inspection is insufficient in evaluating the amount of information hidden.[31–33]

The main goal here is to develop a mathematical model for the measurement of encryption quantity amount (encryption quality) and to determine the optimal version of RC5-$w/r/b$ that gives the best encryption quality for the RC5 block cipher. The optimality is defined as the choice of the most suitable and reasonable values for the RC5 design parameters that give better encryption quality taking into account the best trade-off between encryption quality and computational efficiency. The encryption quality of the RC5 block cipher is evaluated as a function of its design parameters w, r, and b. Such estimations will help in determining the optimal choices for the values of such design parameters that will give better encryption quality for the RC5 block cipher.

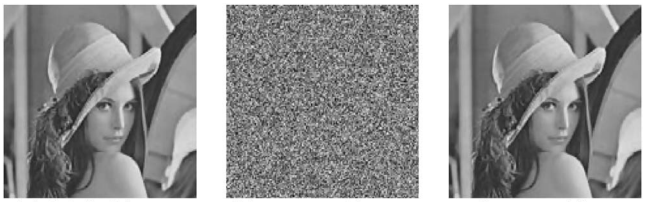

Fig. 5 Application of RC5 to Lena plainimage and its cipherimage.

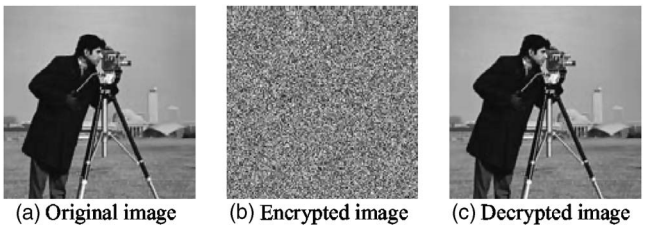

Fig. 6 Application of RC5 to Cman plainimage and its cipherimage.

6.1 *Measurement of Encryption Quality*

We propose the following strategy to approximate encryption quality measurement. With the application of encryption to an image, a change takes place in the pixel values as compared to those values before encryption. This means that the higher the change in pixel values, the more effective will be the image encryption and hence the encryption quality.

So the encryption quality can be expressed in terms of the total changes in pixel values between the original image and the encrypted one. A measure for encryption quality can be expressed as the deviation between the original and encrypted image. The quality of image encryption can be determined as follows.

Let F, F' denote the original image (plainimage) and the encrypted image (cipherimage), respectively, each of size $M*N$ pixels with L gray levels. $F(x,y)$, $F'(x,y)$ $\in\{0,\ldots,L-1\}$ are the gray levels of the images F, F' at position (x,y), $0\leqslant x\leqslant M-1, 0\leqslant y\leqslant N-1$. We will define $H_L(F)$ as the number of occurrences for each gray level L in the original image (plainimage), and $H_L(F')$ as the number of occurrences for each gray level L in the encrypted image (cipherimage). The encryption quality represents the average number of changes to each gray level L, and it can be expressed mathematically as:

$$\text{encryption quality} = \frac{\sum_{L=0}^{255} |H_L(F') - H_L(F)}{256}. \quad (1)$$

6.2 *Effect of the Number of Rounds on the Encryption Quality of the RC5 Block Cipher*

The effect of the number of rounds r on the encryption quality for the RC5 block cipher is investigated. The block size and secret key length are both constant, $w=32$ and $b=16$. The encryption quality (EQ) of the RC5 block cipher is computed as a function of r, as shown in Table 3. Results show that the RC5 block cipher has varied values for EQ at $r=4$, 8, and 12, and achieves its maximum value for the encryption quality after 16 rounds. Then any increment for r does not contribute to increasing the encryption quality of the RC5 block cipher. So we suggest the use of $r=16$ as a standard value, which will result in a maximum value for encryption quality.

Table 3 Encryption Quality (EQ) of RC5 as a function of number of rounds at $w=32$, $r=16$ for Lena and Cman images.

Number of Rounds r	Image name	
	Lena	Cman
4	726.1328	991.7266
8	725.7891	991.7266
12	724.8438	988.9609
16	721.7109	999.7422
20	721.7109	999.7422
24	721.7109	999.7422

6.3 *Effect of the Secret Key Length on the Encryption Quality of the RC5 Block Cipher*

The effect of the secret key length on the encryption quality for the RC5 block cipher is investigated at fixed block size and number of rounds, $w=32$ and $r=20$. Table 4 shows the computed results. These results show that the secret key length has a nonlinear effect on the encryption quality of the RC5 block cipher and that the amount of variation to the encryption quality (by increasing or decreasing) is small relative to a large change in the secret key length. In some cases, increasing the secret key length contributes to an increase or a decrease the encryption quality and vice versa, as shown in Table 4. From the results in Table 4, we suggest the use of a secret key length $b=16$, as this value gives a moderate value for encryption quality.

Table 4 Encryption Quality (EQ) of RC5 as a function of secret key length at $w=32$, $r=20$ for Lena and Cman images.

Secret key length (b)	Image name	
	Lena	Cman
8	724.7031	991.8359
16	722.0391	995.9375
24	725.7813	992.8906
32	725.6094	988.1563
48	720.0078	994.3984
64	722.8203	993.3281
80	723.5781	993.9844
96	726.3906	989.9141
112	722.2813	991.7188
128	724.4688	994.9688
160	721.1719	996.9766
192	728.2422	990.3203
255	724.7031	989.2266

Table 5 Encryption Quality (EQ) of RC5 as a function of word size at $w=16$, $r=16$ for Lena and Cman images.

Word size w(bits)	Image name	
	Lena	Cman
16	362.8672	499.7422
32	722.0391	995.9375

6.4 *Effect of Block Size on the Encryption Quality of the RC5 Block Cipher*

The effect of block size on the encryption quality for the RC5 block cipher is investigated at a fixed number of rounds and secret key length, $r=16$ and $b=16$. The theoretical calculated results and the practical results are shown respectively in Table 5 and Figs. 7 and 8 for the Lena and Cman images. These results clearly show that the encryption quality of the RC5 block cipher increases with increasing block size and vice versa, so increasing the block size contributes to increase the encryption quality of the RC5 block cipher. So we suggest the use of $w=32$, which will result in a block size of $2w$ (64-bit block size) as an optimal choice for word length, as it contributes to achieve a maximum value for encryption quality of the RC5 block cipher. Also the agreement or compatibility between the theoretical and the practical results proves the correctness of the proposed derived formula for the encryption quality.

7 Conclusions

The paper introduces an implementation of the RC5 block cipher, which can work efficiently with digital images.

A mathematical evaluation for encryption efficiency called encryption quality is proposed and may be considered for comparing the effectiveness of the different encryption techniques to digital images instead of visual inspection.

(a) Original image (b) Encrypted image with w =16 (c) Encrypted image with w = 32

Fig. 7 Results of RC5 block cipher applied to Lena image with $b=16$, $r=16$.

(a) Original image (b) Encrypted image with w =16 (c) Encrypted image with w = 32

Fig. 8 Results of RC5 block cipher applied to Cman image with $b=16$, $r=16$.

Several design parameters of the RC5 block cipher are investigated, including word size, number of rounds, and secret key length. Comparative analysis and encryption quality evaluation criteria are achieved using simulation programs. The effect of number of rounds, secret key length, and data block size on encryption quality is evaluated and compared using several test values. The results obtained show that the RC5 block cipher achieved the best encryption quality for word size $w=32$, number of rounds $r=16$, and secret key length $b=16$. Based on these results, the optimal version of the RC5-$w/r/b$ block cipher, taking into account the best trade-off between encryption quality and computational efficiency, is estimated to be RC5-32/16/16.

References

1. National Bureau of Standards, "Data Encryption Standard," Federal Information Processing Standards Publication 46, US Government Printing Office, Washington, DC (1977).
2. National Bureau of Standards, "Data Encryption Standard Modes of Operation," Federal Information Processing Standards Publication 81, US Government Printing Office, Washington, DC, (1980).
3. Ph. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**, 767–769 (1995).
4. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," *Appl. Opt.* **37**, 8181–8186 (1998).
5. L. G. Neto and Y. Sheng, "Optical implementation of image encryption using random phase encoding," *Opt. Eng.* **35**, 2459–2463 (1996).
6. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.* **24**, 762–764 (1999).
7. P. C. Mogensen and J. Gluckstad, "Phase-only optical encryption," *Opt. Lett.* **25**, 566–568 (2000).
8. M. Madjarova, M. Kakuta, M. Yamaguchi, and N. Ohyama, "Optical implementation of the stream cipher based on the irreversible cellular automata algorithm," *Opt. Lett.* **22**, 1624–1626 (1997).
9. W. Stallings., *Network and Internetwork Security: Principles and Practice*, Prentice-Hall, NJ (1995).
10. Bruce Schneier, *Applied Cryptography—Protocols, Algorithms, and Source Code in C*, 2nd ed., John Wiley & Sons, New York (1996).
11. W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice-Hall, NJ (1999).
12. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, New York (1997).
13. R. L. Rivest, "RC5 encryption algorithm," *Dr. Dobb's J.* **226**, 146–148 (1995).
14. C.-C. Chang, M.-S. Hwang, and T.-S. Chen, "An new encription algorithm for image cryptosystems," *J. Syst. Softw.* **58**, 83–91 (2001).
15. J.-I. Guo and J.-C. Yen, "A new mirror-like image encryption algorithm and its VLSI architecture," Department of Electronics Engineering, National Lien-Ho College of Technology and Commerce, Taiwan.
16. J.-C. Yen and J.-I. Guo, "A new chaotic image encryption algorithm," Department of Electronics Engineering, National Lien-Ho College of Technology and Commerce, Taiwan.
17. S. S. Maniccam, N. G. Bourbakis, "Lossless image compression and encryption using SCAN," *Pattern Recogn.* **34**, 1229–1245 (2001).
18. A. Sinha and K. Singh, "A technique for image encryption using digital signature," *Opt. Commun.* **1**, 1–6 (2003).
19. S. Zhang and M. A. Karim, "Color image encryption using double random phase encoding," *Microwave Opt. Technol. Lett.* **21**(5), 318–322 (1999).
20. Y.-C. Hou, "Visual cryptography for color images," *Pattern Recogn.* **36**, 1619–1629 (2003), www.elsevier.com/locate/patcog
21. B. S. Kaliski and Y. L. Yin, "On the security of RC5 encryption algorithm," RSA Laboratories Technical Report TR-602, Version 1.0 (1998).
22. R. Baldwin and R. Rivest, "RFC 2040: The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS algorithms," Oct. 30, 1996, available at ftp://ds.internic.net/rfc/rfc2040.txt.
23. H. R. Myler and A. R. Weeks, *The Pocket Handbook of Image Processing Algorithms in C*, Prentice-Hall, NJ (1993).
24. W. Pennebaker and J. Mitchell, *JPEG Still Image Data Compression Standard*, Van Nostrand Reinhold, New York (1993).
25. S. Lian, J. Sun, and Z. Wang, "Perceptual cryptography on JPEG2000 compressed images or videos," in *IEEE Proc. of the Fourth International Conference on Computer and Information Technology* (2004).
26. D. C. Key and J. R. Levine, *Graphics File Format*, Winderest Books/McGraw-Hill, New York, 1992.
27. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," *Appl. Opt.* **39**, 6595–6601 (2000).
28. B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett.* **28**, 269–271 (2003).
29. T. J. Naughton and B. Javidi, "Compression of encrypted three-dimensional objects using digital holography," *Opt. Eng.* **43**, 2233–2238 (2004).
30. S. Fukushima, T. Kurokawa, and Y. Sakai, "Image encipherment based on optical parallel processing using spatial light modulators," *IEEE Photonics Technol. Lett.* **3**, 1133–1135 (1991).
31. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Security analysis of optical encryption," *Proc. SPIE* **5986**, 25–34 (2005).
32. P. P. Dang and P. M. Chau, "Image encryption for secure Internet multimedia applications," *IEEE Trans. Consum. Electron.* **46**(3), 395–403 (2000).
33. I. E. Ziedan, M. M. Fouad, and D. H. Salem, "Application of data encryption standard to bitmap and JPEG images," in *Proc. 12th National Radio Science Conference (NRSC2003)*, C16/1–C16/8 (2003).

Biographies and photographs of the authors not available.