International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 24 (2015) pp 44539-44544

A Secure Communication System Using RC6 and LSB

M. Saraireh
Associate Professor, Department of Computer Engineering, Mutah University, Karak, Jordan m_srayreh@mutah.edu.jo

Abstract
The exchange of the data has become one of the most significant problems due to the security attack issues. So to avoid this problem, more than one security techniques can be combined to introduce high level of security. This research presents a secure communication system using cryptography and steganography. This combination can provide robust communication system which can resist the attackers. In this paper, the RC6 is used to encrypt the original message, which provides high level of security, performance and speed. Then, the least significant bit (LSB) based steganography is used to embed the encrypted message in the cover image. To evaluate the performance and security of the proposed algorithm, the peak signal to noise ratio (PSNR) and histogram analysis are used. The simulation results indicate that, the proposed algorithm provides high level of security.

Keywords: Cryptography, Steganography, RC6, LSB, PSNR, Histogram.

Introduction

The security of transmitted data is considered as a critical issue in communication systems. So it is essential to have a communication system with high level of security. In this case, users can exchange sensitive data safely. This means that security, integrity, authenticity and confidentiality are satisfied over the transmission channel. Nowadays, a significant amount of information is exchanged every second over a non secured channel. Therefore, it should be protected from the attackers. So to protect the data; several techniques can be employed such as cryptography and steganography.

Usually the cryptography is defined as the science of keeping the information secure by employing the encryption process [1]. The encryption process is done in the transmitter party, while the decryption process is done in the receiver party to recover the original data. On the other hand the steganography is defined as the science of hiding a message within a different digital content; such as image or audio. Usually the hiding process is done in the transmitter while the extraction process is done in the receiver.

The difference between cryptography and steganography is the use of a key in the cryptographic algorithm but there is no need to use a key in steganograhy process. The cryptographic algorithms are categorized as private key algorithm and public key algorithm, where the private key algorithm employs the same key to encrypt and decrypt the message, while the public key algorithm employs different key to encrypt and decrypt the message.

Steganography hides the secrete data in a cover object. It can be implemented; firstly, the spatial domain based steganography, secondly, the transform domain based steganography. To increase the security of data exchange; a joint system can be design using cryptography and steganography.

Steganography system should satisfy the following condition to be useful [2]:

a) Invisibility: it means that the human should not notice the difference between the cover image and the stego image.
b) Security: The steganography process should support the security by embedding the secrete message in the stego image which should be very close to the cover image. To evaluate the steganography security Peak signal to noise ratio (PSNR) can be used to measure the difference between the cover image and the stego image where:

$$PSNR = 10 \log \frac{L^2}{MES} \quad (1)$$

L is the maximum value the samples and MES is the mean error square.

The article is organized as follows. The related work is presented in section 2. The proposed system is introduced in section 3. In section 4 the experimental results and discussions are presented and the conclusion is presented in section 5.

Related Work

Cryptography and steganography are employed to enhance the security of the communication system. In [3] the filter bank cipher is combined with a discrete wavelet transform based staganography, where the data is firstly encrypted using the filter bank cipher, and then the encrypted data is hidden in the cover image by modifying the wavelet coefficients. In [4] the authors modified the least significant bit based staganography to least significant bit matching steganography by providing the desired binary function rather than random choice. In [5] a combined data encoding and hiding process was presented. This combination eliminated the problem of image color changes after the hiding process. The development of the LSB based steganography technique was proposed in [6], this development based on hiding the secret message into the sharper edge regions of the cover image to avoid steganalysis based on statistical analysis. A novel image steganography based on integer wavelet transform was presented in [7], where multiple images can be hidden in a color cover image. In [8] a combination between RSA with asymmetric key and AES with symmetric key was used to encrypt the message and then it was hidden by using smart LSB pixel mapping. In [9] and [10] the proposed algorithms were implemented to deal with voice over IP (VOIP) applications, in those systems the information was hidden using an audio cover signal based on LSB based steganography. Also the hashing algorithms can be combined with steganography to incease the security as in

[11], where SHA-1 (Secure Hash Algorithm) was used to encrypt two dimensional data such as image.

Proposed Algorithm

The aim of this research is the implementation of a secure system using two powerful security techniques which are the cryptography and steganography. By using this design, the message to be transmitted should be encrypted firstly, and then it should be embedded, then it can be transmitted over a non secure channel. In this system, the encryption process can be done by using the RC6 which can offer high speed, low complexity and high level of security. While the embedding process can be done using the LSB based steganography. So the proposed scheme consists of four stages as shown in Figure 1which are encryption, embedding, extraction and decryption. The following algorithm describes these stages.

Algorithm

Input: Original message.
Output: Original message is encrypted and embedded in an image and recovered properly.
Start

1. Original message.
2. Original message encryption.
3. Implementation of LSB based steganography.
4. Embedding the encrypted message.
5. Generation of stego image.
6. Extraction of embedded encrypted message.
7. Encrypted message generation.
8. Decryption.
9. Original Message.

End

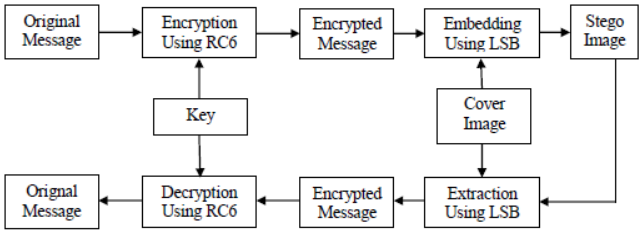


Fig.1. Block Diagram of the Proposed Algorithm.

A. Encryption and Decryption

The encryption process depends on the RC6 cryptographic as shown in Figure 2 algorithm [12]. RC6 is a symmetric cryptographic encryption algorithm. It is specified as RC6-w/r/b where the word size is w bits; encryption consists of a nonnegative number of rounds r, and b the length of the encryption key in bytes. RC6-w/r/b operates on units of four w-bit words using the following operations [12]:

A + B: integer addition modulo 2^w .
A – B: integer subtraction modulo 2^w.
A ⊕B: bitwise exclusive-or of w-bit words.
A × B: integer multiplication modulo 2^w.
A <<< B: rotate the w-bit word A to the left by the amount given by the least significant log w bits of B.
A>>> B: rotate the w-bit word A to the right by the amount given by the least significant log w bits of B.

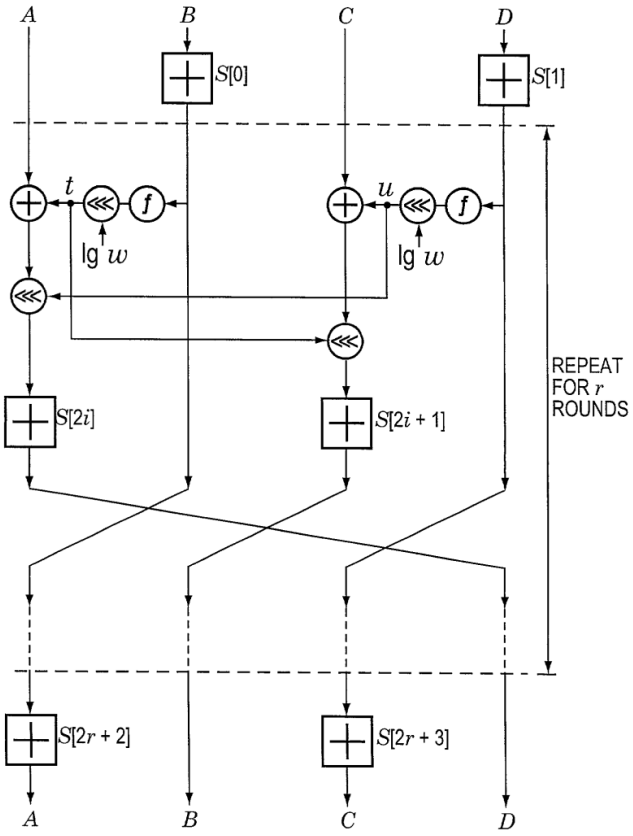


Fig.2. RC6 Algorithm.

B. Embedding and Extraction

LSB steganography is one of simplest embedding process in use to hide the message. It hides the data into an image called the cover image to generate the stego image. The embedding technique replaces the data in a given pixel with data in the cover image using the least significant bit of the pixels.

Experimental Results and Discussions

The performance of the proposed algorithm is assessed for different cover images, Cameraman, Lenna, Peppers, House and Baboon with size of 256×256 bits. Those cover images are used to embed the encrypted message. So first of all it is essential to encrypt the message using the RC6 algorithm, after that the embedding process is applied using the LSB to produce the stego image to be transmitted over the communication channel. At the receiver, the hidden encrypted message is retrieved to be decrypted to obtain the original message. The proposed algorithm is examined using PSNR and histogram analysis.

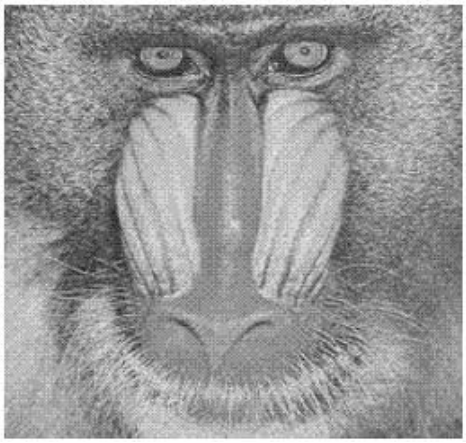
To compare between the cover image and the stego image PSNR is employed. PSNR is measured in decibels (dB). Also, PSNR is employed to evaluate the quality of the stego image. In this case, if PSNR of gray scale image smaller than 36 dB, the human can notice difference between the cover image and the stego image [13], but if PSTR is larger than 36 dB, the

human cannot notice the difference. The PSNR can be calculated using equation (1), and the results for different cover images are summarized in Table 1. Note that, the values of PSTR are greater than 36 dB, this means that, the proposed system is secure.

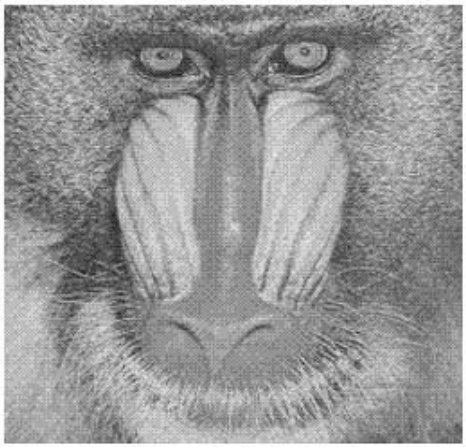
TABLE.1. Peak Signal to Noise Ratio Results

Cover Image	PSNR
Baboon	42.8
Peppers	42.6
Lenna	43.3
Cameraman	42.9
House	43.1

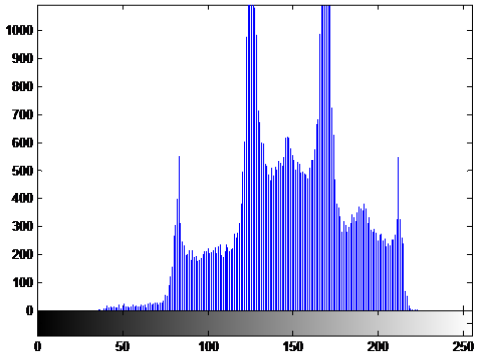
Another analysis can be used to evaluate the efficiency of the proposed system; it is called the histogram analysis. If the histogram before and after the embedding process remains the same, then the embedding algorithm is efficient, otherwise it is considered inefficient. In this paper the histograms for different cover images are plotted, then the histogram for their corresponding stego images are plotted as shown in the Figures 3, 4, 5, 6 and 7. The figures show that the histograms of the cover images and the stego images are the same and do not have any significant change. This means that, the proposed system is efficient which can resist the attacks and statistical changes.



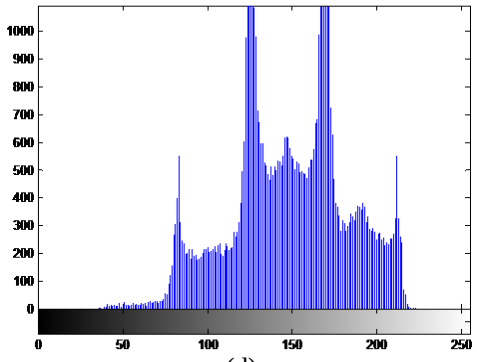
(a)



(b)



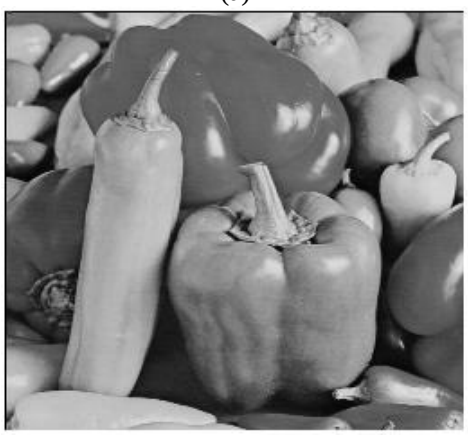
(c)



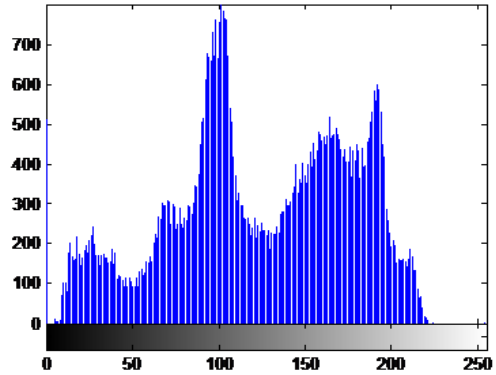
(d)

Fig.3. a) Baboon Cover Image. b) Stego Image. c) Histogram of Baboon Cover Image. d) Histogram of Baboon Stego Image.

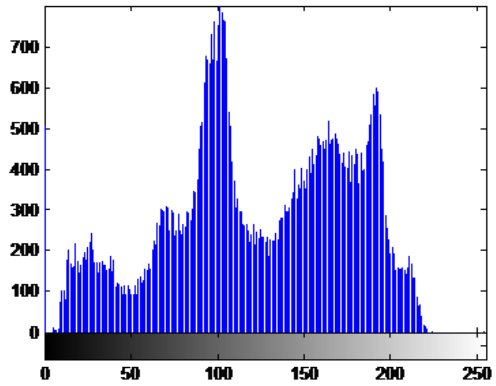
(a)



(b)



(c)

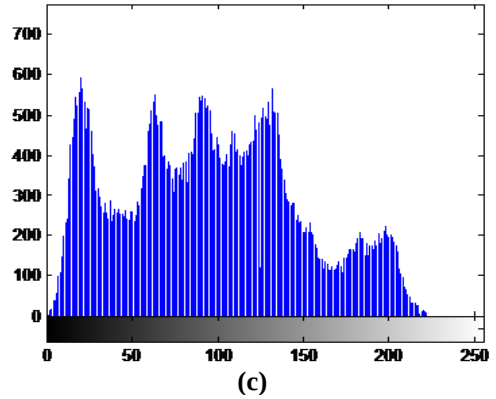


(d)

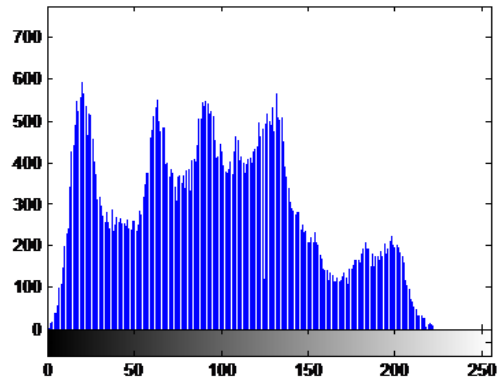
Fig.4. a) Peppers Cover Image. b) Stego Image. c) Histogram of Peppers Image. d) Histogram of Stego Image.

(a)

(b)



(c)

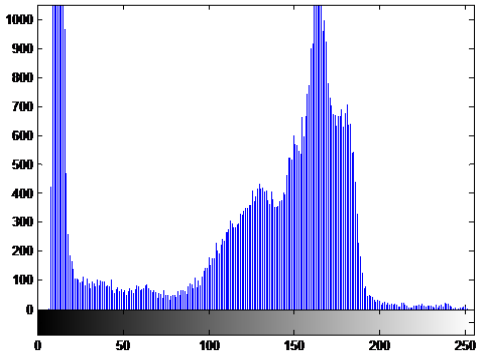


(d)

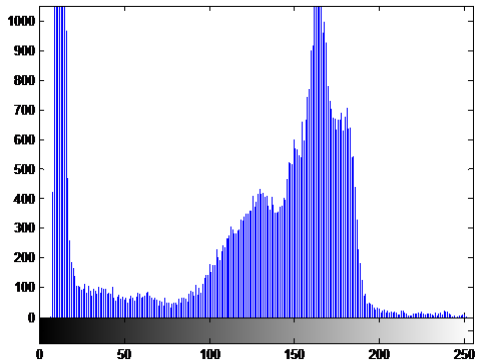
Fig.5. a) Lenna Cover Image. b) Stego Image. c) Histogram of Lenna Image. d) Histogram of Stego Image.

(a)

(b)



(c)

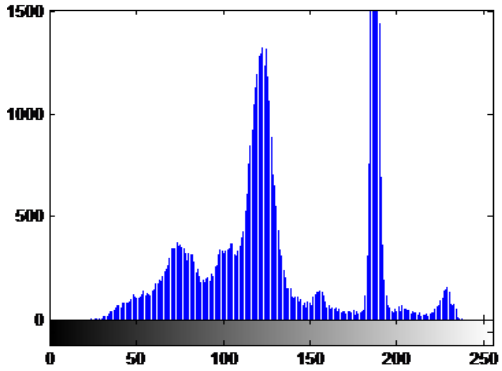


(d)

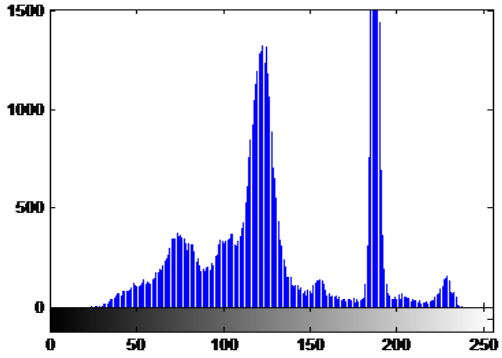
Fig. 6. a) Cameraman cover image. b) Stego Image. c) Histogram of Camerman Image. d) Histogram of Stego Image.

(a)

(b)



(c)



(d)

Fig.7. a) House Cover Image. b) Stego Image. c) Histogram of House Image. d) Histogram of Stego Image.

Conclusion

In this paper, two different security techniques are combined to produce a high security model. So the RC6 based cryptography is used for the encryption which provide high level of security and speed, and the LSB based steganography is used for the embedding process which also provide a high processing speed. PSNR and histogram are used to evaluate the efficiency of the proposed algorithm. The results indicated that, the PSNR are greater than 36 dB which means that the embedded data is invisible. Also, the histograms of the cover image and the stego image are very similar to each other, which ensure the efficiency of the proposed algorithm.

References

[1] Saleh Saraireh, Mohammad Saraireh & Yazeed Alsbou " Secure Image Encryption Using Filter Bank and Addition Modulo 2^8 with Exclusive OR Combination " International Journal of Computer Science and Security (IJCSS), Vol. (7), No. (2), 2013.

[2] Katzenbeisser, S. and Petitcolas, F.A.P., Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London, 2000.

[3] Saleh Saraireh "A Secure Data Communication System Using Cryptography and Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol. 5, No. 3, 2013.

[4] Jarno Mielikainen, "LSB Matching Revisited", IEEE signal processing letters, Vol. 13, No. 5, 2006.
[5] Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in images", IEEE, 2nd International conference on Computing, Communication and Networking Technologies, 2010.
[6] G.Karthigai Seivi, Leon Mariadhasan and K. L. Shunmuganathan, " Steganography Using Edge Adaptive Image " IEEE, International Conference on Computing, Electronics and Electrical Technologies, 2012.
[7] Hemalatha S, U Dinesh Acharya, Renuka A and Priya R. Kamath, " A Secure and High Capacity Image Steganography Technique", Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, 2012.
[8] Septimiu F. M., Mircea Vladutiu and Lucian P., "Secret data communication system using Steganography, AES and RSA", IEEE 17th International Symposium for Design and Technology in Electronic Packaging, 2011.
[9] H. Tian, K. Zhou, Y. Huang, D. Feng, J. Liu, "A Covert Communication Model Based on Least Significant Bits Steganography in Voice over IP", IEEE The 9th International Conference for Young Computer Scientists, pp. 647-652, 2008.
[10] Y. Huang, B. Xiao, H. Xiao, "Implementation of Covert Communication Based on Steganography", IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1512-1515, 2008.
[11] Cheddad, A, Condell, Joan, Curran, K and McKevitt, Paul, "Securing Information Content using New Encryption Method and Steganography", IEEE Third International Conference on Digital Information Management, 2008.
[12] Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin, “The RC6 Block Cipher” 1998.
[13] El Safy, R.O, Zayed. H. H, El Dessouki. A, (2009), “An adaptive steganography technique based on integer wavelet transform,” ICNM International Conference on Networking and Media Convergence, pp 111-117, 2009.

Author

Mohammad Saraireh is an associate professor at the Faculty of Engineering, Computer Engineering Department, Mutah University, Jordan. His area of expertise is in quality of service in wireless computer networks and computer Networks, artificial intelligence applied to computer networks, communication systems, cryptography and network security.