International Journal of the Physical Sciences Vol. 6(17), pp. 4255-4263, 2 September, 2011
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS11.470
ISSN 1992-1950 ©2011 Academic Journals

Full Length Research Paper

Satellite Image Encryption for C4I System

Abdullah Sharaf Alghamdi[1], Hanif Ullah[1]*, Muhammad Usama Khan[2], Iftikhar Ahmad[1] and Khalid Alnafajan[1]

[1]Department of Software Engineering, College of Computer and Information Sciences, P. O. Box 51178, Riyadh 11543, King Saud University, Riyadh, Saudi Arabia.
[2]Prince Muqrin Chair for IT Security, King Saud University, Riyadh, Saudi Arabia.

Accepted 13 April, 2011

Global command and control system (GCCS-Joint) is a command, control, communications, computers and intelligence (C4I) system which consists of hardware, software, procedures and standards and which provides directory services, enterprise services and security services by exchanging imagery, intelligence, status of forces and planning information. In order to secure this exchange of imagery and information, we need more secure techniques and algorithms to be implemented. During the war, the commanders and forces needs the information and images of the exact location to which they are going to target and these images can be easily taken from the satellite. But the main problem of these satellite images is its transmission over the unsecure electronic media. This paper basically introduces a technique for the encryption and decryption of satellite imagery in order to securely transmit it during the war. The methodology used here for the process of encryption and decryption is that of chaotic maps. The research work is carried out by using the Henon and logistic maps.

Key words: Global command and control system (GCCS-Joint), security, satellite imagery, encryption, decryption.

INTRODUCTION

Due to the rapid developments in the field of computers and communications and due to the extensive use of images over the electronic media motivate the researchers and developers to introduce new techniques and algorithms for the secure transmission of the these images. Global command and control system (GCCS-Joint) is basically a C4i system which provides the services of exchanging imagery and other services to other systems of C4i. During the war, the commander and forces need the information about the targeted enemies areas and sensitive location maps to which they are going to target, and the images of these locations can easily be taken from the satellite. But the main problem is that of the secure transmission of the images over the internet because anyone can take valuable information from these images if they are not encrypted. Many researchers and developers have done a lot of work in this area and they have developed some good algorithms for the encryption and decryption of these images. The traditional techniques such as advanced encryption standard (AES), data encryption standard (DES) and RSA (Rivest, Shamir, and Adleman) are not good enough for the encryption of images and also they have enormous computational time while performing the process of encryption and decryption over images. Some chaotic based algorithms are introduced for the encryption of images and text (Baptista, 1998; Usama et al., 2010) by using the idea of creating relationship between the plain images and generated pseudo-random numbers which are further used to enhance the process of encryption and decryption. But the main problem is that they have used it either only for text or simple images, or not for satellite images. Some other chaotic based algorithms are used specifically for the encryption of satellite images (Usama et al., 2010) by using the concept of multiple chaotic maps for enhancing the process of key space, robustness and security.

The main concern of our research in this article is the use of chaotic sequences for the encryption of satellite images in the era of C4i system. Two types of maps, that is, Henon and logistic maps are used to carry out our

*Corresponding author. E-mail: hanif.ksu@gmail.com. Tel: 00966550023202/0599450402.

research work. Henon and logistic maps are further used in the process of key generation in order to make the process more complex and to achieve the high level of confusion and diffusion for encryption. The key generation process is based on simple Xor operation in order to make the process simple and easy for hardware and software implementation.

RELATED WORK

The work that we have seen related to our work is that of Yoon and Kim (2010) in which they have used the idea of large pseudorandom numbers generated from small permutation matrix. This permutation matrix is based on chaotic maps. They used the entire permutation matrix effectively for the encryption and decryption of images. The experimental results of the entire work concluded that the proposed system provides more security than the traditional algorithms used for the same purpose (Yoon and Kim, 2010; Berry and Vin, 1996; Fengling et al., 2006). Discrete experimental chaotic maps are used for improving the properties of confusion and diffusion. Based on discrete chaotic maps, they design a key scheme to resist statistic, differential and gray code attacks (Zhang et al., 2005).

Similarly, a new nonlinear chaotic algorithm is introduced which used the concept of power and tangent function instead of nonlinear function for the encryption and decryption of images. The algorithm works on one-time-one password, and provides the advantage of large key space and high level security with acceptable efficiency (Xin and Weibin, 2008). Moreover some researchers have used the idea of fast chaotic cryptographic scheme by iterating the logistic map instead of generating the random numbers. Also they used lookup table for the entire process. This method proves more time reduction during the process of encryption and decryption. Also the algorithm shows some practical implementation in the secure transmission of large multimedia files (Wong, 2002).

Similarly, the appropriate work that is more relevant to this work is that done by Usama et al. (2010) in their previous paper on the encryption of satellite images using the chaos-based concept. They used the idea of chaos-based symmetric key encryption. The entire algorithm uses a lot of chaotic maps in order to increase the key space, robustness and security of the satellite images. The algorithm proves that the entire process takes least time as compared to other encryption techniques like AES, DES and 3 DES.

CHARACTERISTICS OF THE CHAOTIC MAPS

This research work is mainly concern with secure satellite image encryption and decryption using chaotic sequences. More specifically, chaotic maps are used for secure satellite image communication over shared network environments and distributed using any storage media like CDs, DVDs and/or hard disks (Muhaya et al., 2009; Usama et al., 2010).A particularly interesting candidate for chaotic sequences generators are logistic and Henon map. The chaotic behaviour of these maps can be verified easily with different desirable properties. These properties can be accessible with the help of rigorous mathematical analysis and experiments as shown subsequently

Henon map analysis

The Henon map is a discrete-time dynamical system which can be used in cryptography because of chaotic effect. Henon map is one of the well studied dynamical systems because of its simplicity and chaotic behaviour. It is a simple two-dimensional map with quadratic non-linearity (Álvarez et al., 2002; Long and Huang, 2010). Mathematically, the Henon map is defined by the following equation:

$$x_n = 1 + \lambda(x_{n-2} - x_{n-3}) + ax_{n-2}^2$$

The Henon map depends on two parameters, a and λ. The pseudorandom behaviour of the Henon map have values of $1.07 \leq a \leq 1.09$ and $\lambda = 0.3$. For these basic values, the Henon map is chaotic. For other values of a and λ, the map can be behaved like chaotic, recurring, irregular or unpredictable behaviour. An overview of the type of behaviour of the map at different parameter values may be obtained from its orbit diagram. The Henon map takes a point (x, y) in the plane and maps it to a new point. For many values of a_0 and b_0, the dynamics of this map are chaotic. We consider the range $1.07 \leq a \leq 1.09$ and $\lambda = 0.3$; the analysis diagrams are shown in Figure 1.

To examine the behaviour of the Henon map, the parameter value lambda λ can be divided into three segments as $\lambda \in (0,0.28)$, $\lambda \in (0.29,0.32)$ and $\lambda \in (0.33,1)$ with initial condition $x_2 = 0.56$ and $x_3 = 0.34$. These parameters λ and initial values x_2 and x_3 may be used as a secret key for cryptography system.

When $\lambda \in (0,0.28)$, as shown in Figure 1a, the calculation results come to the same value after several iterations without any chaotic behaviour.

When $\lambda \in (0.29,0.32)$, it becomes a chaotic system and random behaviour with periodicity disappeared, as showed in Figure 1b.

When $\lambda \in (0.33,1)$, the phase space concludes several points only, as showed in Figure 1c, the system

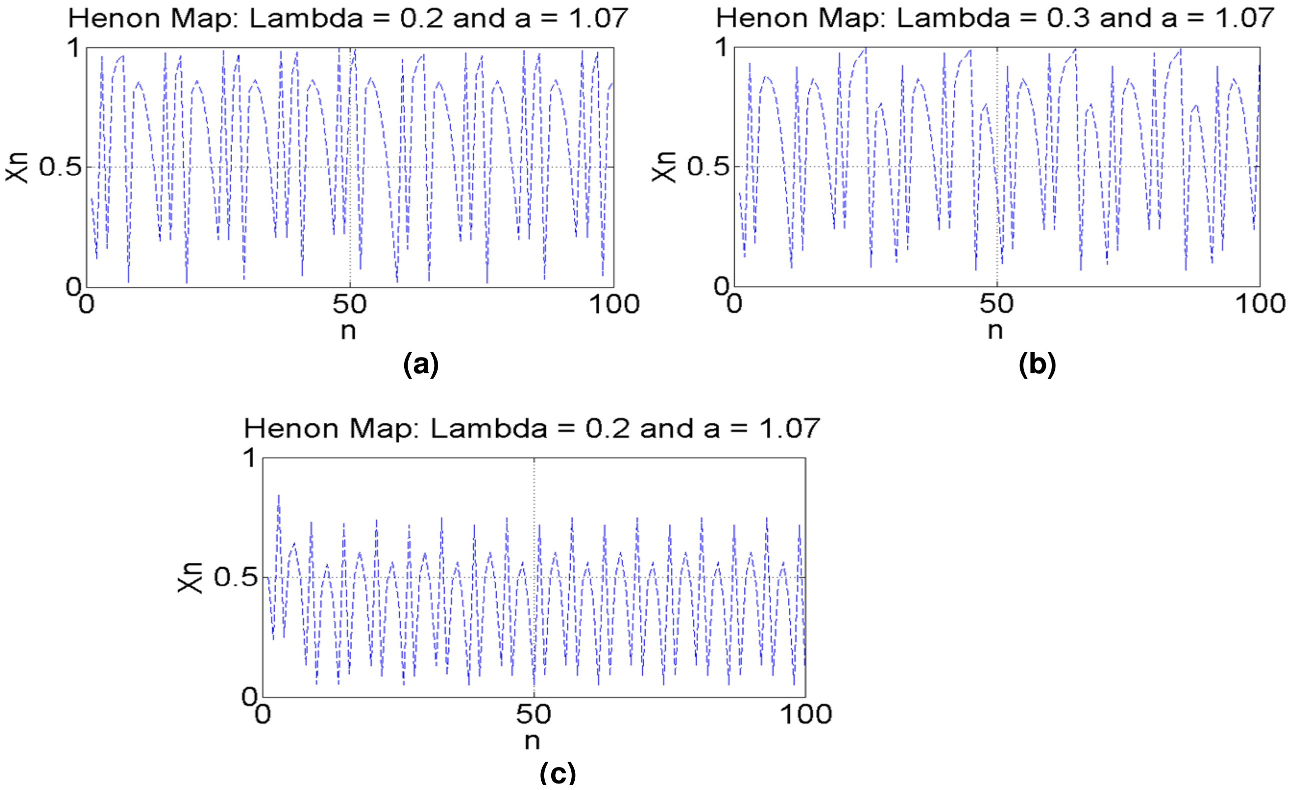

Figure 1. Analysis results of Henon map. (a) Iteration property when $\lambda = 0.2$; (b) Iteration property when $\lambda = 0.3$, and (c) Iteration property when $\lambda = 0.8$.

appears periodicity.

Hence, the Henon map does not satisfy uniform distribution property. When $\lambda \in (0,0.28)$ and $\lambda \in (0.33,1)$, the points concentrate on several values and could not be used for encryption purpose. From the experimental results, we can easily conclude that Henon map behaves like chaotic and can be useful of any cryptosystem while we use desirable parameters and initial values. For example, when we performing encryption and decryption the suitable initial conditions are $x_2 = 0.56$ and $x_3 = 0.34$, similarly constant parameter must have values between $1.07 \le a \le 1.09$ and $\lambda = 0.3$.

Logistic map analysis

The Logistic map is one-dimensional discrete chaotic map which can originate chaotic behavior using simple non-linear dynamical equation (Grassi, 2002; Long and Huang, 2010). Mathematically, the Logistic map is defined by following equation:

$$x_{n+1} = \lambda x_n (1 - x_n)$$

Where x_n is a number between zero and one (0, 1) and x_0 represents the initial value (at $n = 0$). The parameter λ is a positive number, that is, $\lambda \in (0,4), n = 0,1,.....$ (Devaney, 1989), and represents a combined rate for reproduction and starvation. The Logistic map can cause problems when initial conditions and parameter values lead to negative results and have weaknesses. To examine the behavior of the Logistic map, the parameter value lambda λ can be divided into three segments as $\lambda \in (0,3)$, $\lambda \in (3,3.6)$ and $\lambda \in (3.6,4)$ with initial condition $x_0 = 0.3$. These parameters λ and initial value x_0 may be used as a secret key for encryption.

When $\lambda \in (0,3)$, as shown in Figure (2a), the calculation results come to the same value after several iterations without any chaotic behavior.

When $\lambda \in (3,3.6)$, the phase space concludes several points only, as showed in Figure (2b), the system appears periodicity.

When $\lambda \in (3.6,4)$, it becomes a chaotic system with periodicity disappeared, as showed in Figure (2c). Hence,

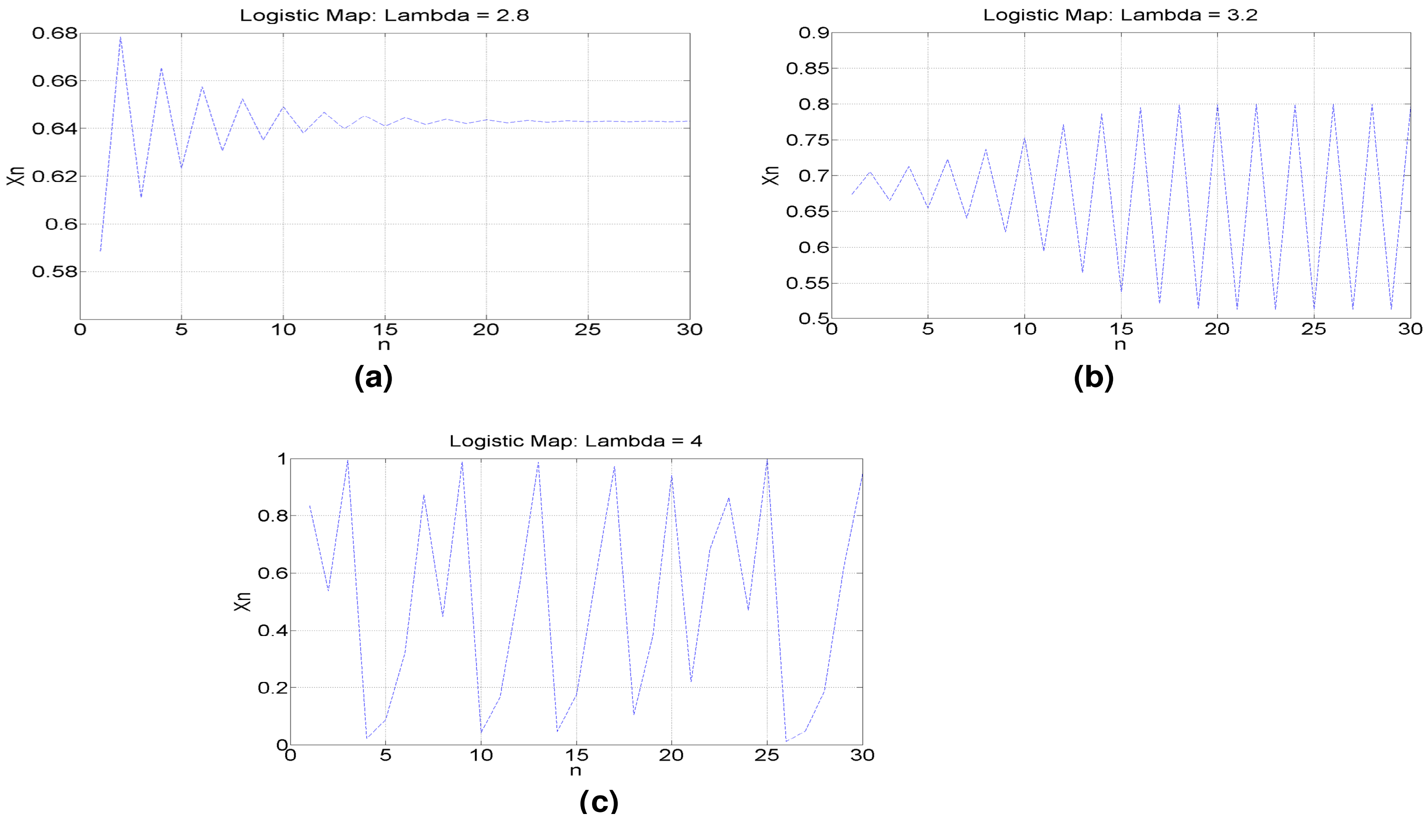

Figure 2. Analysis results of logistic map. Iteration property when (a) Iteration property when $\lambda = 2.8$; (b) Iteration property when $\lambda = 3.2$, and (c) Iteration property when $\lambda = 4$.

the Logistic map does not satisfy uniform distribution property. When $\lambda \in (0,3.6)$ the points concentrate on several values and could not be used for encryption purpose. Cryptosystems based on Logistic map has small key space and weak security.

HenLog random key generator (HenLog-RKG)

In this section, the concept of using HenLog-RKG has been proposed. The HenLog-RKG is based on Henon and Logistic chaotic maps. The act of using Henon and Logistic maps in key generation process is to achieve the high level of confusion and diffusion for encryption. The key generation process is based on simple XOR operation that's why proposed algorithm is simple and easy for hardware and software implementation. The proposed HenLog-RKG is a symmetric random-key generator which can generate variable length secret keys of different sizes e.g. 128, 192 and 256 bits. The single secret key is defined using equation 1 as:

$$K = b_1 b_2 b_3 b_4 b_5 .... b_{S/8} \quad (1)$$

Here S is the size of the key K in bits. The one-dimensional Henon and Logistic chaotic maps have been used in this process (governing equation and control parameters of each map with values in the chaotic range are given in section A and C). Original chaotic sequences using above mentioned chaotic maps consists of decimal fraction values. However satellite images are all in digital form. So chaotic maps are defined to generate the secret key in bytes format, the hexadecimal mode is used for it. Then satellite images can be encrypted by using simple XOR operation with the random bytes sequence. The variable length key size (which is 128, 192 and 256 bits) is suitable for proposed encryption and decryption algorithm. The secret keys SK_i are generated using the following Equations 2 and 3:

$$N = \sum_{i=1}^{S/8} (K_i / 256) \quad (2)$$

$$SK_i = N - \lfloor N \rfloor \quad (3)$$

Where K_i is the i^{th} key value in decimal equivalent of the

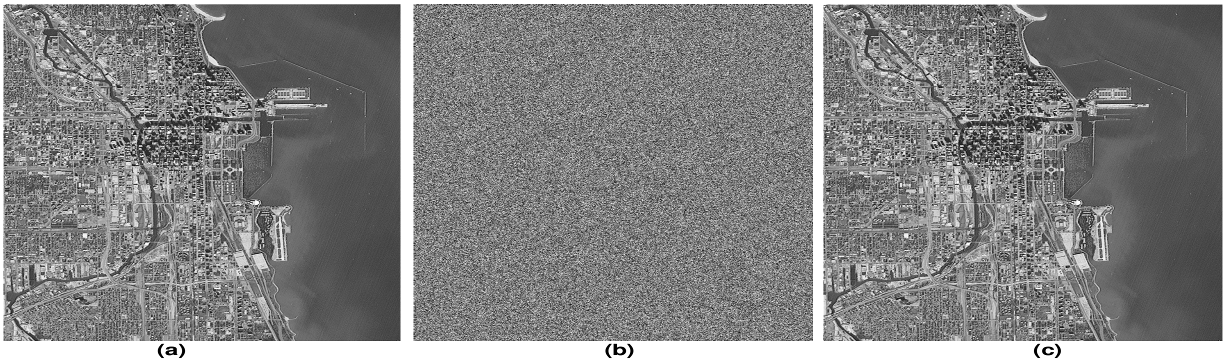

Figure 3. Application of proposed algorithm on Chicago satellite image. (a) Original image; (b) Encrypted image; (c) Decrypted image.

secret key, $\lfloor N \rfloor$ is the floor of the value N , S is the key size and SK is secret key. The key generation steps are as follows:

Step 1: Takes user key and n number of keys as input parameters to generate the two random sequences lK and hK from Henon and logistic chaotic maps, respectively. Step 2: Performs XOR operation to merge random sequences using Equation 4:

$$K_i = lK_i \oplus hK_i \tag{4}$$

Here, $i = 1,2,3,.........,n$ where $n \geq 1$ and K is final generated secret key in byte format.

PROPOSED ENCRYPTION ALGORITHM

Since 1990s number of symmetric-key block ciphers based-on chaotic techniques have been proposed (Álvarez et al., 2002; Long and Huang, 2010; Usama et al., 2010; Matthews, 1989; Habutsu et al., 1991; Kotulski and Szczepanski 1997; Baptista, 1998; Alvarez, 1999; KOTULSKI et al., 1999; Wong et al., 2001; Wong, 2002; Pareek et al., 2003; Wong et al., 2003) for text and multimedia data. These techniques are based-on widely-used single chaotic map used to build the block cipher. The proposed encryption algorithm is based on HenLog-RKG for satellite images. The algorithm is a symmetric-key block cipher that takes chaotic sequence as secret key (generated using HenLog-RKG) to encrypt the satellite imagery and data. The algorithm is capable of using cryptographic keys 128, 192, and 256 bits to encrypt and decrypt satellite imagery in blocks of 128, 192 and 256 bits. The input and output satellite images (as shown in equations 5 and 6, respectively) for the algorithm each consist of sequences of 128, 192, and 256 bits (values of 0 or 1) and will be referred to as blocks and the sequence of bits. The secret key for algorithm is a sequence of 128, 192 or 256 bits as shown in Equation 7 The block size of the input data and key must be equal to accomplish the encryption/decryption operation:

$$O = O_1 O_2 O_3 O_4 O_5 ....O_n \tag{5}$$

$$C = C_1 C_2 C_3 C_4 C_5 ....C_n \tag{6}$$

The secret key can be represented as:

$$K = K_1 K_2 K_3 K_4 K_5 ....K_{BS/8} \tag{7}$$

where, BS is the block size in bits and n is the number of blocks. After, initial parameter initializations, a simple XOR operation with key values and image blocks are performed. The encryption and decryption process is shown as:

$$
\begin{array}{rcccccccccc}
 & \multicolumn{4}{c}{\longrightarrow} & \multicolumn{4}{c}{\longrightarrow} & & \\
keys = & k_1, & k_2, & ...., & k_n, & k_1, & k_2, & ...., & k_n & & \Bigg\downarrow \\
 & \oplus, & \oplus, & ...., & \oplus, & \oplus, & \oplus, & ...., & \oplus & & \\
Blocks = & b_1, & b_2, & ...., & b_n, & b_{n+1}, & b_{n+2}, & ...., & b_m & & \\
 & =, & =, & ...., & =, & =, & =, & ...., & = & & \\
Cipher = & c_1, & c_2, & ...., & c_n, & c_{n+1}, & c_{n+2}, & ...., & c_m & &
\end{array}
$$

The encryption/decryption process continues till the original/cipher image is completely encrypt/decrypt. The experiment and analysis results are given in 'Experimental results and analysis' to prove the strength of the proposed cryptosystem.

EXPERIMENTAL RESULTS AND ANALYSIS

Results of some experiments are given to prove high level of security and performance of the proposed algorithm for satellite images. The proposed algorithm has been investigated by using the SPOT Satellite Image as shown in Figure 3a (the image is in GeoTIFF format). This is the SPOT satellite imagery of downtown Chicago, IL (USA) at 10 m resolution have 652094 bytes size. The projected coordinate system is State Plane NAD 1927. The image has been enhanced by contrast optimization process and a light Laplace spatial filter. So, it should not require any further processing, in any display environment. The 256-bits secret key "123456GHIJKLMNOPQRSTUVWXYZ[/]^ _`" (in ASCII) is used for encryption and decryption process. The encrypted and decrypted satellite images are depicted in Figure 3b and c, respectively. As shown, the encrypted

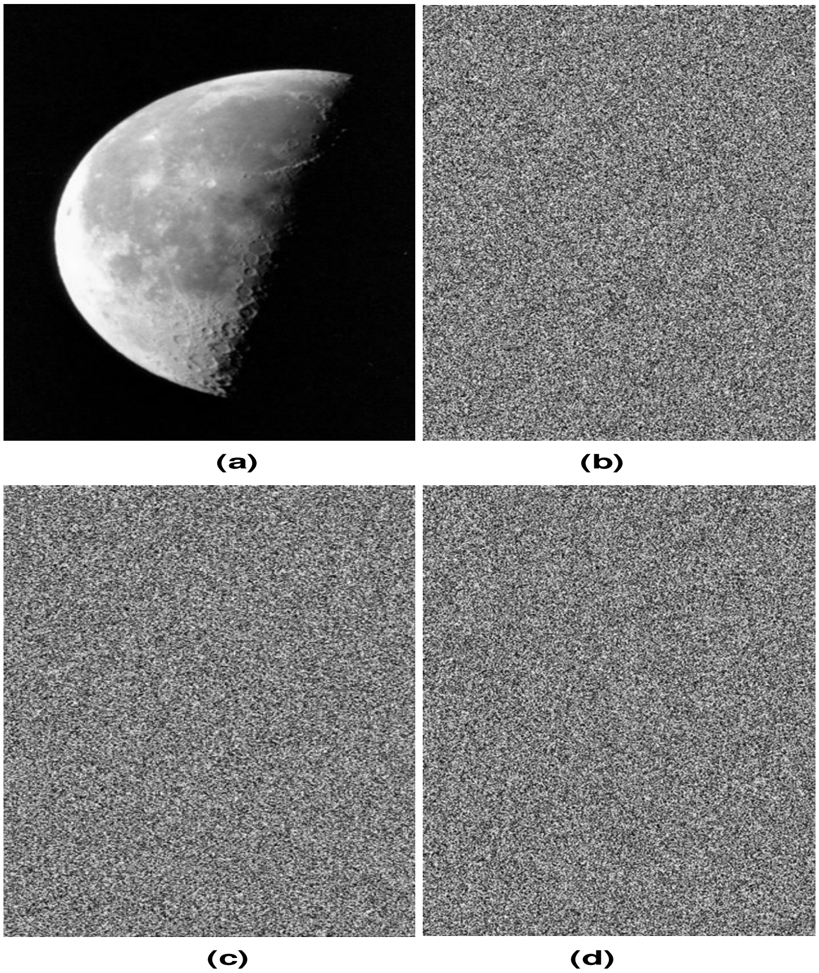

Figure 4. Key sensitive test: Result 1. (a) Original image; (b) Encrypted image with key “12345678901234567890123456789012; (c) Encrypted image with key “22345678901234567890123456789012";(d) Encrypted image with key “12345678901234567890123456789033".

image is totally unreadable and invisible. The decryption method takes as input the encrypted image, together with the same secret key.

Key sensitivity test

A good cryptosystem should be sensitive to the secret keys to make brute-force attacks infeasible. For the proposed algorithm, key sensitivity testing and analysis have been performed. Assuming that a 256 bits secret key is used. This means that the key consists of 32 characters. A typical key sensitivity test has been performed according to the following steps:

1. First, a 358 × 537 moon satellite image (as shown in Figure 4a) is encrypted using the secret key ‘123456789012 34567890123456789012’.
2. Then, the starting bits of the secret key are changed, so that the original key becomes, say ‘223456789012345678 90123456789012’ in this example, which is used to encrypt the original image. The output encrypted satellite image is shown in Figure 4b.
3. Then, the last bits of the secret key are changed, so that the original key becomes, say‘12345678901234567890 1203456789033’ in this example, which is used to encrypt the original image. The output encrypted satellite image is shown in Figure 4c.
4. Finally, the aforementioned three images, encrypted by the three slightly different keys are compared.

Test results 1

Visually all these encrypted images (as shown in Figure 4) are different and have no similarity with each other although there is a slight difference in the three keys. Also, the results of information entropy and correlation

Table 1. Key sensitivity experiment results.

Satellite image	Entropy	Correlation
Figure 4b and c	7.9997	0.00023558
Figure 4b and d	7.9997	0.0018
Figure 4c and d	7.9997	0.00039816

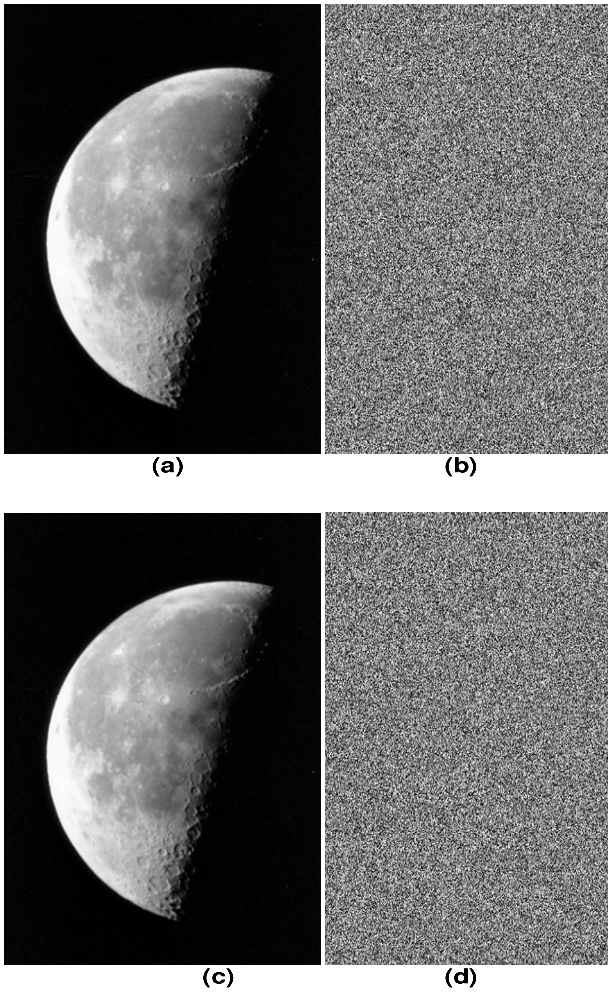

Figure 5. Key sensitive test: Result 2. (a) Original image; (b) Encrypted image with key “12345678901234567890123456789012; c) Decrypted image with key “12345678901234567890123456789012; (d) Decrypted image with key “11145678901234567890123456789012.

analysis have been given in Table 1 to prove the key sensitivity of proposed algorithm.

Test result 2

Moreover, when a 32 character secret key is used to encrypt an image while another trivially modified key is used to decrypt the ciphered image, the decryption also completely fails. Figure 5 clearly shows that the image encrypted by the key “12345678901234567890123456789012” is not correctly decrypted by using the key “223456 78901234567890123456789012” there, which has also

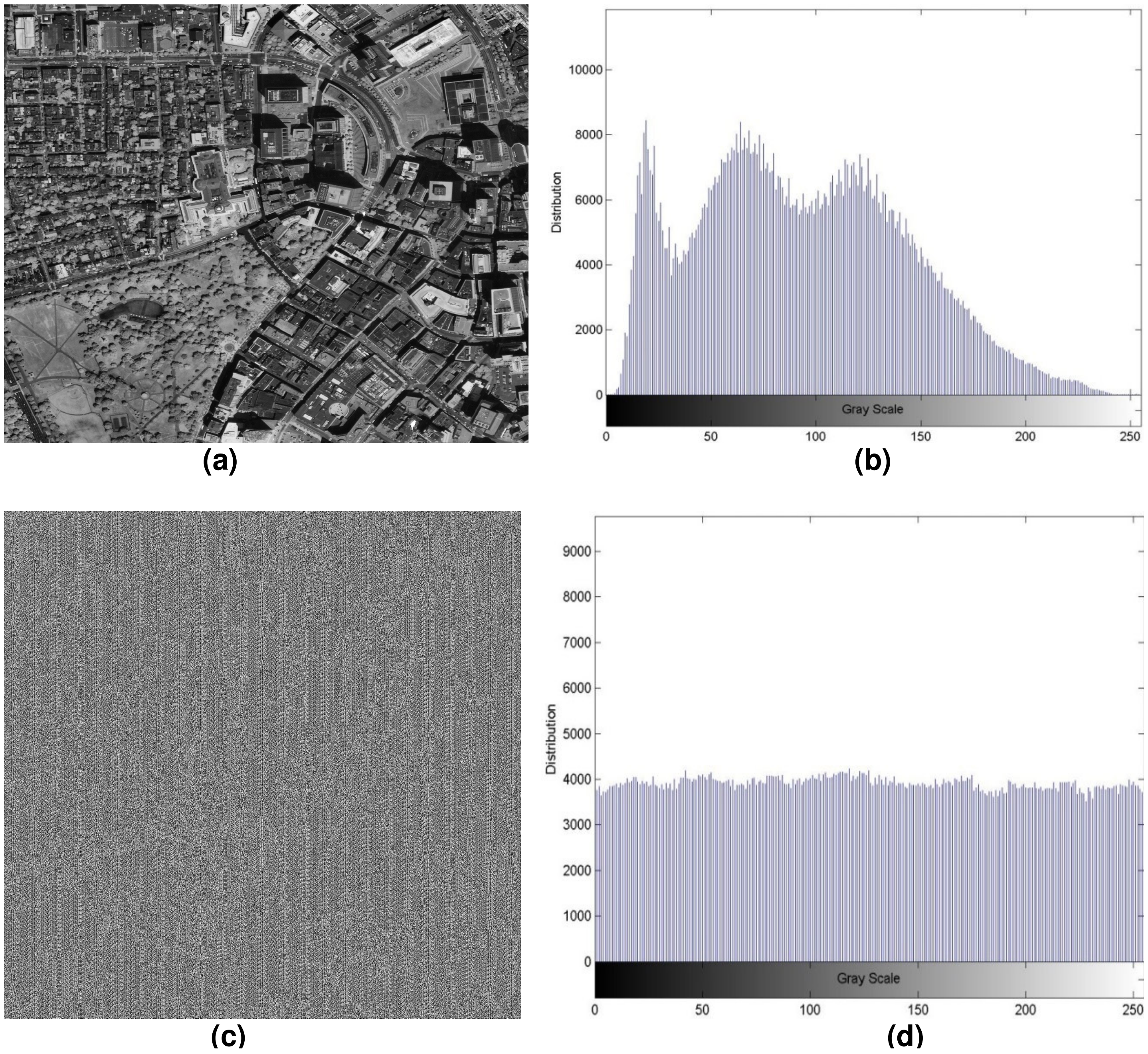

Figure 6. Histograms of the Boston satellite image; (a) Original image; (b) Histogram of original Image; (c) Encrypted image; (d) Histogram of encryption image.

only one bit difference between the two keys.

Histogram analysis

The superior level of confusion and diffusion properties in cryptosystem is highly recommended in order to provide the security against the strong and powerful statistical attacks. Statistical analysis techniques have been performed on the proposed algorithm for satellite images to prove the acceptable level of confusion and diffusion properties. This has been shown by performing histogram and correlation analysis on various satellite images. Several satellite images of different sizes that have different contents were selected, and their histograms calculated. One typical example among them is shown in Figure 6. From the figure, one can see that the histogram of the ciphered image is fairly uniform and is significantly

Table 2. Performance analysis experiment results.

Satellite image	Image size in (KB)	Dimension	Format	Encryption time (s)	Decryption time (s)
Chicago Figure 3a	635	699 × 929	Geo Tiff	0.125	0.125
Moon Figure 4a	179	358 × 537	Geo Tiff	0.09375	0.094
Boston Figure 6a	979	1000 ×1000	Geo Tiff	0.1875	0.172

different from that of the original image.

Performance analysis

Apart from the security and reliability concern, some other issues on satellite image encryption are also important. These include the performance and efficiency of the cryptosystem for real-time applications to perform encryption and decryption. The test application of proposed algorithm is implemented using Microsoft C#.Net and Matlab programming languages and performance has been measured on a 3.0 GHz Pentium-IV with 3 G-bytes of RAM running Windows XP. The proposed algorithm has been executed on three different satellite images that have different dimensions, sizes, geo information, resolutions etc. The experiment results of encryption and decryption process are given in Table 2 to prove the algorithm acceptable performance. Thus, the proposed algorithm requires negligible computation time and suitable for real-time application of satellite imagery.

Conclusion

This paper is based on the encryption and decryption of satellite imagery used by the commanders and forces in the C4I system. The algorithm uses the idea of chaotic maps that is Henon and logistic maps in order to encrypt and decrypt these images, used by the global command and control system (GCCS-joint) which provides a lot of services including the exchange of images to the C4i system. The entire algorithm uses the concept of HenLog-RKG which is based on Henon and logistic chaotic maps. These maps are used for the key generation process and its purpose is to achieve the high level of confusion and diffusion during the entire process. The performance analysis of the algorithm shows the proposed system can be used efficiently for real time applications to perform encryption and decryption.

ACKNOWLEDGEMENT

The authors cordially thank the Research center of the college of computer and information sciences, King Saud University for supporting this work.

REFERENCES

Alvarez E, Fernandez A, García P, Jiménez J, Marcano A (1999). New approach to chaotic encryption. Phys. Lett. A, 263(4-6): 373-375.

Álvarez G, Montoya F, Romera M, Pastor G (2004). Cryptanalyzing a discrete-time chaos synchronization secure communication system. Chaos Solitons Fractals, 21(3): 689-694.

Baptista MS (1998). Cryptography with chaos. Phys. Lett. A, 240(1-2): 50-54.

Berry J, Vin HM (1996). Imagery and information over the Defense Red Switch Network. MILCOM, Confere. Proceed. IEEE, 2: 552-555.

Devaney R (1989). An Introduction to Chaotic Dynamical Systems. Redwood, Addison-Wesley.

Fengling H, Xinghuo Y, Songchen H (2006). Improved Baker map for image encryption. Int. S. on Sys. and Cont. in Aero and Astro, pp. 1273-1276.

Grassi G, Miller DA (2002). Theory and experimental realization of observer-based discrete-time hyperchaos synchronization. Cir. and Sys. I: Fund. Theory and App. IEEE Trans., 49(3): 373-378.

Habutsu T, Nishio Y, Sasase I, Mori S (1991). A secret key cryptosystem by iterating a chaotic map. Proc. of the 10th annual int. conf. Theory appl. cryp. tech. Brighton, UK, Springer-Verlag, pp. 127-140.

Kotulski Z, Szczepański J, Gorski K, Paszkiewicz A, Zugaj A (1999). Application of Discrete Chaotic Dynamical Systems in Cryptography — DCC Method. Int. J. Bifurcat. Chaos (IJBC), 9(6): 1121-1135.

Long M, Huang L (2010). Design and Analysis of a Novel Chaotic Image Encryption. ICCMS, pp. 517-520.

Matthews R (1989). On the Derivation of a “Chaotic” Encryption Algorithm. Cryptologia. 13(1): 29 - 42.

Muhaya FB, Usama M, Khan MK (2009). Modified AES using chaotic key generator for satellite imagery encryption. Proc. 5th int. conf. Emerging intelligent comp. tech. app. Ulsan, South Korea, Springer-Verlag, pp. 1014-1024.

Pareek NK, Patidar V, Sud KK (2003). Discrete chaotic cryptography using external key. Phys. Lett. A, 309(1-2): 75-82.

Usama M, Khan MK, Alghathbar K, Lee C (2010). Chaos-based secure satellite imagery cryptosystem. Comp. Math. Appl., 60(2): 326-337.

Wong WK (2002). A fast chaotic cryptographic scheme with dynamic look-up table. Phys. Lett. A, 298(4): 238-242.

Wong WK, Ho SW, Yung CK (2003). A chaotic cryptography scheme for generating short ciphertext. Phys. Lett. A, 310(1): 67-73.

Wong WK, Lee LP, Wong KW (2001). A modified chaotic cryptographic method. Comp. P. Comm., 138(3): 234-236.

Xin Z, Weibin C (2008). A new chaotic algorithm for image encryption. ICALIP, pp. 889-892.

Yoon JW, Kim H (2010). An image encryption scheme with a pseudorandom permutation based on chaotic maps. Comm. Non. Sci. Num. Sim., 15(12): 3998-4006.

Kotulski Z, Szczepanski J (1997). Discrete chaotic cryptography (DCC): New method for secure communication. Proc. NEEDS, pp. 1-11.

Zhang L, Liao X, Wang X (2005). An image encryption approach based on chaotic maps. Chaos, Solitons Fractals, 24(3): 759-765.