PROPOSING A NEW METHOD FOR ENCRYPTING SATELLITE IMAGES BASED ON HASH FUNCTION AND CHAOS PARAMETERS

M. Sedighi [1*], S. K. Mahmoudi [2], A. S. Amini [3]

[1] Dept. of Geomatic Engineering, Islamic Azad University South Tehran Branch, P. O. Box: 1777613651, Tehran, Iran (m.sedighi.eng@gmail.com)
[2] Dept. of Geomatic Engineering, Islamic Azad University South Tehran Branch, P. O. Box: 1777613651, Tehran, Iran (komeil.mahmoudi@yahoo.com)
[3] Dept. of Geomatic Engineering, Islamic Azad University South Tehran Branch, P. O. Box: 1777613651, Tehran, Iran (sh_amini@azad.ac.ir)

Commission VI, WG VI/4

KEY WORDS: Remote sensing, Chaos mapping, Hash function, Encryption, Image processing.

ABSTRACT:

Due to the importance of providing security in satellite imagery and their transmission, in this paper, a new method for encrypting satellite images based on Hash key-based symmetric cryptographic algorithm is proposed which is developed by combining the generated key and chaos mapping parameters. The benefits of this algorithm are high security, high sensitivity and using dynamic encryption blocks. The proposed algorithm consists of three main parts: in the first section, the encryption key is created using the SHA[1]-512 Hash function. In the second section, the initial values and the parameters of the mapping Chaos are determined by the algebraic functions that are related to the primary key. In the third section, with the help of the encryption block, the encrypted image is finally obtained. The purpose of this article is to increase the security of encrypting satellite images by creating an unspecified encryption block to deal with a variety of attacks. In this regard, both aspects of security and performance of the proposed algorithm have been analysed and the results are evaluated

1. INTRODUCTION

In recent years, with the rapid development of computer technology, digital image processing technology has also rapidly developed and penetrated into all aspects of life, such as remote sensing, industrial detection, medicine, meteorology, communication, investigation, intelligent robots, etc. Therefore, image information has attracted widespread attention. Image data security is very important, especially in the special military, commercial and medical fields. Image encryption has become one of the ways to protect digital image transmission (Sukalyan et al., 2013)and(Khanzadi et al., 2014).

Cryptographic systems are categorized into two types of encryption: block cipher and Stream cipher. The Stream cryptographers try to encrypt the data by combining input data with a quasi-random number string. In block encryption, the encrypted data of the specified length, called blocks, is based on a set of nonlinear transforms, and the data is encoded into block blocks during encryption. In String Cryptography, The more random the strings are, the more powerful the cryptographic system and In block cryptography, the more complex and non-linear the cryptographic operations are, the more powerful the cryptographic algorithm, Therefore string encoders are faster and block encoders more powerful(Menezes et al.,1997)and (Lian, 2009).

2. METHODOLOGY

2.1. Chaos Functions

In recent years, many image encryption algorithms have been developed based on one of the ways of using Chaos mapping, Fourier transform, Cellular Automata and etc(Liao et al., 2010). Meanwhile, cryptographic algorithms based on Chaos theory, with respect to the good features of these functions, such as sensitivity to initial values, behavior to randomness and the accuracy of the mapping, while its random behavior, has led researchers to focus more than other methods(Wang et al., 2011)and(Akhshani et al., 2010).

Since 1990s, there have been a number of symmetric-key chaos-based image and plaintext encryption algorithms proposed to achieve the high diffusion and confusion for securing sensitive data. These algorithms are based on single chaotic map for generating secret key, used in encryption and decryption process (Hussain, 2016).

2.2. Hash functions

Hash functions are a kind of conversion that receives a long string as an input and outputs a constant-length string. The resulting Hash is a representation of the entire text content or input string. And it can be considered a kind of "digital fingerprint" for that text. Cryptographic hedging functions are used to check the integrity of messages and digital signature of texts in a wide range of applications, such as authentication messages. SHA-2 is a collection of Hash functions. Designed by the United States National Security Agency and published by the National Institute of Technology and Standards in 2001 as the standard of information procession. This algorithm contains four Hash functions, with an output string of 224, 256, 384, and 512 bit lengths .(Konheim, 2010).

Figure 1 shows functional characteristics of four investigated Hash function.

(1) Secure Hash Algorithm

Terms	SHA-1	SHA-256	SHA-384	SHA-512
Size of hash value(Bit)	160	256	384	512
Complexity of the best attack	2^{80}	2^{128}	2^{192}	2^{256}
Equivalently secure secret-key cipher (Bit)	-	AES-128	AES-192	AES-256
Message size (Bit)	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Message block size (Bit)	512	512	1024	1024
Word size (Bit)	32	32	64	64
Number of words(Bit)	5	8	8	8
Number of digest rounds	80	64	80	80

Figure 1. Functional characteristics of four investigated Hash function (Seyedzade, 2011)

In this paper, a combination of Stream encryption by using Hash functions and block encryption has been used mapping Chaos.

3. PROPOSED METHOD

In this paper, with the help of the SHA-512 function, which has very high security, the user input key is converted to a string of 512 bits long, then this string is converted into a string of numbers in the form of a matrix using the ASCII[1] code.

$$\text{Input Key} = O_1\, O_2\, O_3\, O_4 \ldots O_P$$

P: can be any integer value

$$\text{Hash Code} = C_1\, C_2\, C_3\, C_4 \ldots C_M$$

M: fixed length of 512 bits.

Given the Hash functions, this matrix is unique in relation to the input key, and each other input key generates its own unique matrix. The matrix of the Keys is shown as figure 2.

Secret key	mohammad
hash Code	5d67e90ede0cd3ed091da39acf2be04da1 2324b18273902fa8fbdd3c6aea03dd4217 eb33a1838e616285f9a283188a1e792c64 2b79aad125538effdff227ad36
ASCII	51 101 100 48 57 49 100 97 51 57 97 99 102 50 98 101 48 52 100 97 49 50 51 50 52 98 49 56 50 55 51 57 48 50 102 97 56 102 98 100 100 51 99 54 97 101 97 48 51 100 100 52 50 49 55 101 98 51 51 97 49 56 51 56 101 54 49 54 50 56 53 102
Block size	512bits

Figure 2. The matrix of the Keys

Now, with the help of dividing this matrix into smaller matrices, the calculation of several statistical functions on these matrices and the combination of values obtained and the use of functions which, given the optimal range of each of the initial values and constant parameters of Chbyshev Chaos mapping, Tent, Cubic, Henon, Logistic, Tent, and Sine are pre-designed, the initial and constant values of each Hash map, as well as block length and cipher block number, are determined. Figure 3 shows breaking the encryption block into smaller matrices.

(1) American Standard Code for Information Interchange

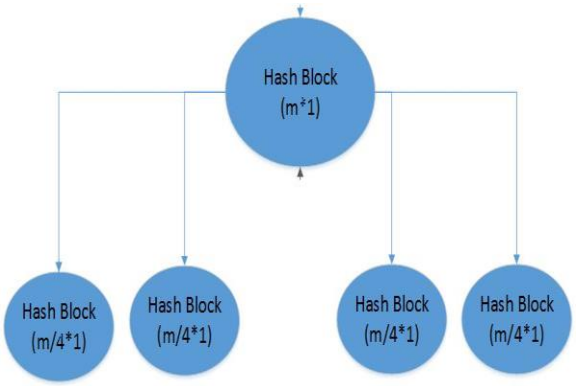

Figure 3. Break the encryption block into smaller matrices

Now, according to the acquired parameters, the blocks of each of the maps are formed and then, to increase the safety factor, these blocks are combined together with the help of the XOR key to form the end encryption block. Figure 4 shows chaotic maps used in the proposed algorithm.

Chaotic map	Governing equation
Chebyshev	$x_{n-1} = \cos(\lambda \cos^{-1}(x_n))$
Logistic	$x_{n+1} = \lambda x_n (1 - x_n)$
Cubic	$x_{n+1} = \lambda x_n (1 - x_n^2)$
Sine	$x_{n+1} = \lambda \sin(\pi x_n)$
Henon	$x_n = 1 + \lambda(x_{n-2} - x_{n-3}) + \alpha x_{n-2}^2$
Tent	$x_{n+1} = \begin{cases} x_n/\mu & \text{if } x_n \le \mu \\ 1 - x_n/1 - \mu & \text{if } x_n \ge \mu \end{cases}$

Fig. 4. Chaotic maps used in the proposed algorithm

In this step, the image bands are separated and placed together and a matrix is formed. By using the XOR key, the encryption block is formed and the input image matrix is combined to change the DN values of the image. Combination between mapping Chaos is shown as figure 5.

$$\begin{array}{llllll}
Chebyshev = & BK = & bk_1, & bk_2, & \ldots\ldots\ldots\ldots, & bk_n \\
 & & \oplus, & \oplus, & \ldots\ldots\ldots\ldots, & \oplus \\
Logistic = & LK = & lk_1, & lk_2, & \ldots\ldots\ldots\ldots, & lk_n \\
 & & \oplus, & \oplus, & \ldots\ldots\ldots\ldots, & \oplus \\
Cubic = & CK = & ck_1, & ck_2, & \ldots\ldots\ldots\ldots, & ck_n \\
 & & \oplus, & \oplus, & \ldots\ldots\ldots\ldots, & \oplus \\
Sine = & SK = & sk_1, & sk_2, & \ldots\ldots\ldots\ldots, & sk_n \\
 & & \oplus, & \oplus, & \ldots\ldots\ldots\ldots, & \oplus \\
Henon = & HK = & hk_1, & hk_2, & \ldots\ldots\ldots\ldots, & hk_n \\
 & & \oplus, & \oplus, & \ldots\ldots\ldots\ldots, & \oplus \\
Tent = & TK = & tk_1, & tk_2, & \ldots\ldots\ldots\ldots, & tk_n \\
 & & =, & =, & \ldots\ldots\ldots\ldots, & = \\
Keys = & K = & k_1, & k_2, & \ldots\ldots\ldots\ldots, & k_n
\end{array}$$

Figure 5. Combination between mapping Chaos (Usama 2010)

Then, the matrix derived from the encryption with the Hash function block is again combined with the help of the Hash matrix generated initially and the XOR key, and at the final stage of the output matrix, the incoming input matrix is cropped

and its various bands combined to encrypt the image The desired result. The block diagram of encryption/decryption process is given in Figure6.

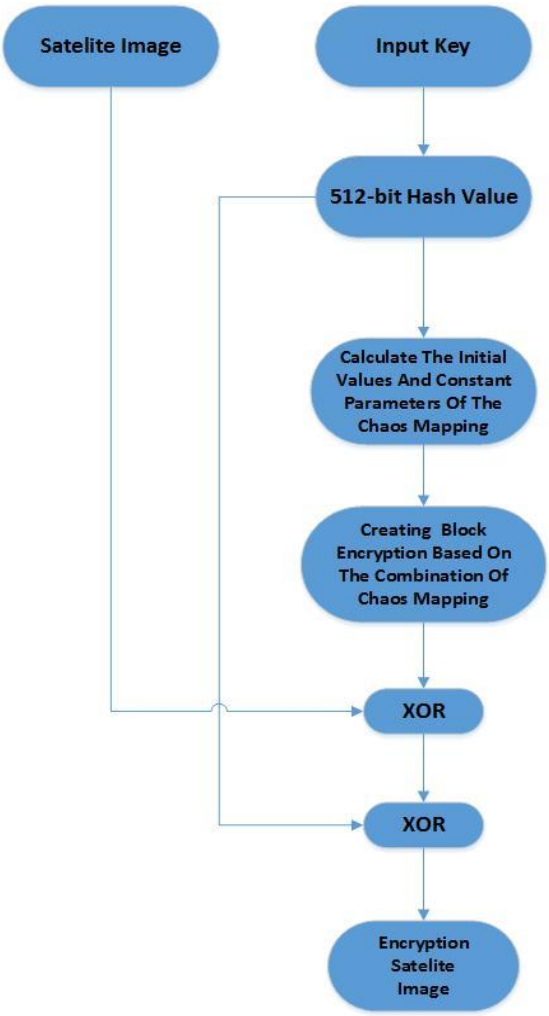

Figure 6. Block diagram of encryption process.

4.RESULTS

In order to evaluate the proposed algorithm, the results of the method were compared with several usual methods In this regard; the entropy information and key sensitivity and histogram analysis was studied and compared.

4.1. Information Entropy

An entropy test is the standard of uncertainty of a random variable that determines the information in the data. And the bigger it shows the increased randomness of the data. Table 1 shows comparing the result of entropy test between the proposed method and the others. the formula of information entropy is shown in Equation (1),(Zhu et al., 2018).

$$H(X) = -\sum_{i=0}^{255} p(x_i)\, log_2 p(x_i) \quad (1)$$

where x = a discrete random variable of gray color image p (xi) =the probability density function of the occurrence of the symbol xi.

Image Encryption Methods	Entropy
Proposed Method	7.9992
Zhu(2018)	7.9980
Wang(2015)	7.9753
Stoyanov(2015)	7.9958
Stoyanov(2014)	7.9789
Seyedzade(2011)	7.9895
Chai(2017)	7.9949

Table 1. Comparing the result of entropy test between the proposed method and the others methods.

4.2. key Sensitivity

Based on principles of cryptology, a good encryption algorithm should be sensitive to the plaintext sufficiently. The sensitivity of the encryption algorithm can be quantified as Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). Table 2 shows comparing the result of plaintext average test between the proposed method and the others. The formulas for the calculation of NPCR and UACI are as follows(Wu et al., 2011) :

$$NPCR = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j) \times 100 \quad (2)$$

$$\mathrm{UACI} = \frac{1}{W \times H}\left(\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{\left|C_{1(i,j)} - C_{2(i,j)}\right|}{255}\right) \times 100 \quad (3)$$

Suppose encrypted images before and after one pixel change in plain image are $C1$ and C 2. where D is a two-dimensional array ,having the same size as image $C1$ or $C2$, and W and H are the width and height of the image. The array $D(i, j)$ is defined by $C1(i, j)$ and $C2(i, j)$; if $C1(i, j) = C2(i, j)$, then$D(i, j) = 1$; otherwise, $D(i, j) = 0$ (stovanov et al., 2014).

Image Encryption Methods	NPCR%	UACI%
Proposed Method	99.61	33.50
Zhu(2018)	99.59	33.49
Wang(2015)	99.58	33.49

Table 2. Comparing the result of plaintext average test between the proposed method and the other methods.

4.3. Histogram Analysis

The image histograms show how pixels in an image are spread by drawing the number of pixels at each color intensity level(slimane et al., 2016). Comparing the histograms, we can find that the pixel values of the original image are concentrated on some values, while the distribution of the pixel values of the encrypted image are relatively uniform, which makes the statistical attack difficult(Liu et al., 2017). The results of the proposed histogram are presented in the following figures.

Figure 7. Original Image

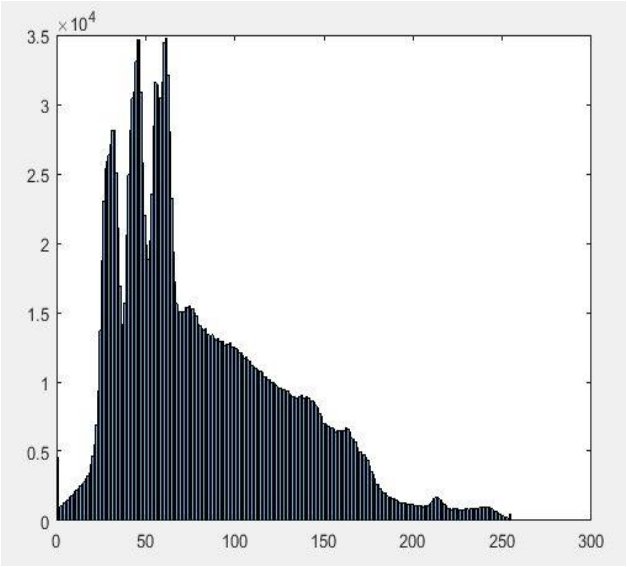

Figure 8. Histogram Original image

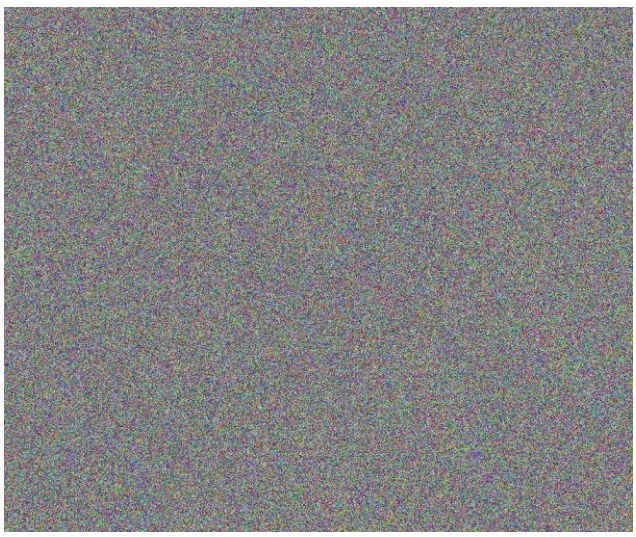

Figure 9. Encrypted Image

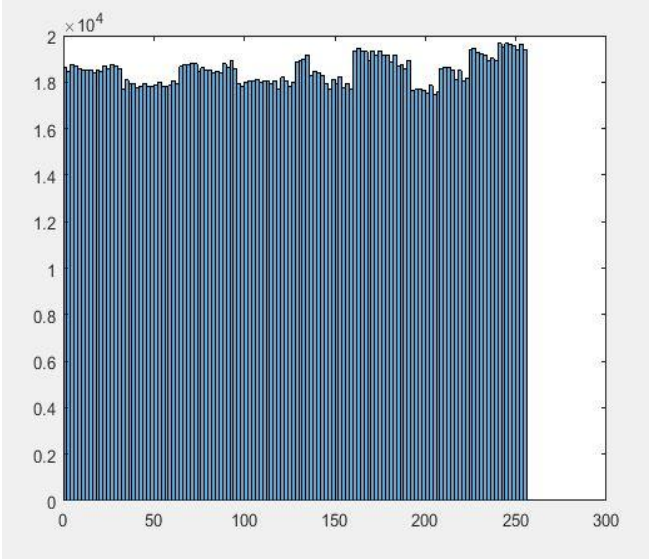

Figure 10. Histogram Encrypted Image

The results showed that application of the proposed method improves the operation of satellite image encryption.

5. CONCLUSIONS

In this paper, a new method for encrypting satellite images based on Hash key-based symmetric cryptographic algorithm is proposed which is developed by combining the generated key and chaos mapping parameters. The purpose of this article is to increase the security of encrypting satellite images by creating an unspecified encryption block to deal with a variety of attacks. To evaluate the proposed method, the results of this method were compared with several methods, in this regard; the histogram analysis and the entropy information and key sensitivity was studied and compared. In addition, the creation of cryptographic block with random and unpredictable dimensions is an advantage of this algorithm. The results showed that application of the proposed method improves the operation of satellite image encryption.

6. REFERENCES

Akhshani, A., Behnia, S., Akhavan, A., Hassan, H. A., Hassan, Z., 2010. A novel scheme for image encryption based on 2D piecewise chaotic maps," Journal of Optics Communications, Vol. 283, 3259–3266.

Chai, X.,2017. An image encryption algorithm based on bit level brownian motion and new chaotic systems.
Multimed. Tools Appl. 2017, 76, 1159–1175.

Hussain, A., 2016. Image compression and encryptionscheme via satellite, Journal of Vibration and Control, Vol.22, No.13, 3118-3122.

Khanzadi, H., Eshghi, M., Etemadi Borujeni, S., 2014. Image Encryption Using Random Bit Sequence Based on Chaotic Maps, Springer, vol. 39, no. 2. 1039–1047, February 2014.

Konheim, A.G., 2010 . HASHING FOR STORAGE: DATA MANAGEMENT. Hashing in Computer Science: Fifty Years of Slicing and Dicing. Wiley-Interscience.

Lian, S. A., 2009. block cipher based on chaotic neural networks. Neurocomputing. 72(4-6):1296-301.

Liao, X., Lai, S., Zhou, Q,. 2010 .A novel image encryption algorithm based on self-adaptive wave transmission,.Journal of Signal Processing, Vol. 90,2714-2722.

Liu, H., Kadir, A., Sun, X., 2017. Chaos-based fast colour image encryption scheme with true random number keys from environmental noise. The Institution of Engineering and Technology 2017, 324-332

Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.,1997. Handbook of applied cryptography discrete mathematics and its applications. 1th ed. London: Crc Press; 1997.

Seyedzade, S.M., Mirzakuchaki, S., Atani, R.E.,2011. A novel image encryption algorithm based on hash function. In Proceedings of the Iranian Conference on Machine Vision and Image Processing, Isfahan, Iran, 27–28 October 2011, pp. 1–6.

Slimane, N.B., Bouallegue, k., Machhout, M .,2016. Nested chaotic image encryption scheme using two-diffusion process and the Secure Hash Algorithm SHA-1. 4th International Conference on Control Engineering & Information Technology (CEIT-2016) Tunisia, Hammamet- December, 16-18, 2016.

Stoyanov, B., Kordov, K., 2014. Novel image encryption scheme based on chebyshev polynomial and duffing map. Sci. World J. 2014, 283639.

Stoyanov, B., Kordov, K., 2015. Image encryption using chebyshev map and rotation equation. Entropy 2015, 17, 2117–2139.

Sukalyan, S., Sayani, S.,2013. A Non-adaptive Partial Encryption of Grayscale Images Based on Chaos, First International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA), vol. 10, 663-671.

Usama, M., Khurram Khan, M., Alghathbar, K., Lee, C., 2010 . Chaos-based secure satellite imagery cryptosystem. Computers and Mathematics with Applications 60 (2010) 326_337.

Wang, X.-Y., Gu, S.-X., Zhang, Y.-Q., 2015, Novel image encryption algorithm based on cycle shift and chaotic system. Opt. Lasers Eng. 2015, 68, 126–134.

Wang, Y., Wong,K.W., Liao, X., Chen, G., 2011. A new chaos-based fast image encryption algorithm, Applied Soft Computing, Vol. 11, 514-522.

Wu, Y., Noonan, J. P., Agaian, S., 2011. NPCR and UACI randomness tests for image encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications. 2.31-38.

Zhu, S., Zhu , C ., Wang, W., 2018. A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256. MDPI,entropy2018.