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

M. Sedighi1*, S. K. Mahmoudi2, A. S. Amini3

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_aminiz@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-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 nonlinear 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
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 code.

**Input Key = O₁ O₂ O₃ O₄ … Oₚ
P: can be any integer value**

**Hash Code = C₁ C₂ C₃ C₄ … Cₘ
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.

<table>
<thead>
<tr>
<th>Secret key</th>
<th>hash Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>mohammad</td>
<td>5d67e90de0cd3ed91da39acf2be0da1</td>
</tr>
<tr>
<td></td>
<td>5c34b1827392fca8ef6d36a6a033d4217</td>
</tr>
<tr>
<td></td>
<td>eb33a18386e6162859fa283188ae792c64</td>
</tr>
<tr>
<td></td>
<td>2b79aad125538e9df2ff227ad36</td>
</tr>
</tbody>
</table>

**ASCII**

<table>
<thead>
<tr>
<th>Block size</th>
<th>512bits</th>
</tr>
</thead>
</table>

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**

<table>
<thead>
<tr>
<th>Governing equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chebyshev</td>
</tr>
<tr>
<td>Logistic</td>
</tr>
<tr>
<td>Cubic</td>
</tr>
<tr>
<td>Sine</td>
</tr>
<tr>
<td>Henon</td>
</tr>
</tbody>
</table>
| Tent              | \( x_{n+1} = \left\lfloor x_n / \mu \right\rfloor \) if \( x_n < \mu \)
|                   | \( 1 - x_n / (1 - \mu) \) if \( x_n \geq \mu \) |

**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.

**Figure 5. Combination between mapping Chaos (Usama 2010)**

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.

**Figure 3. Break the encryption block into smaller matrices**

(1) American Standard Code for Information Interchange
and its various bands combined to encrypt the image. The desired result. The block diagram of encryption/decryption process is given in Figure 6.

![Block diagram of encryption process](image)

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).

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

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

<table>
<thead>
<tr>
<th>Image Encryption Methods</th>
<th>Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed Method</td>
<td>7.9992</td>
</tr>
<tr>
<td>Zhu(2018)</td>
<td>7.9980</td>
</tr>
<tr>
<td>Stoyanov(2015)</td>
<td>7.9958</td>
</tr>
<tr>
<td>Stoyanov(2014)</td>
<td>7.9789</td>
</tr>
<tr>
<td>Seyedzade(2011)</td>
<td>7.9895</td>
</tr>
<tr>
<td>Chai(2017)</td>
<td>7.9949</td>
</tr>
</tbody>
</table>

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): 

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

$$UACI = \frac{1}{W \times H} \left( \sum_{i=1}^{W} \sum_{j=1}^{H} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right) \times 100$$  \hspace{1cm} (3)

Suppose encrypted images before and after one pixel change in plain image are $C_1$ and $C_2$. where $D$ is a two-dimensional array having the same size as image $C_1$ or $C_2$, and $W$ and $H$ are the width and height of the image. The array $D(i, j)$ is defined by $C_1(i, j)$ and $C_2(i, j)$; if $C_1(i, j) = C_2(i, j)$, then $D(i, j) = 1$; otherwise, $D(i, j) = 0$ (Stoyanov et al., 2014).

<table>
<thead>
<tr>
<th>Image Encryption Methods</th>
<th>NPCR</th>
<th>UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed Method</td>
<td>99.61</td>
<td>33.50</td>
</tr>
<tr>
<td>Zhu(2018)</td>
<td>99.59</td>
<td>33.49</td>
</tr>
<tr>
<td>Wang(2015)</td>
<td>99.58</td>
<td>33.49</td>
</tr>
</tbody>
</table>

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


