

Elementary Matrix Operation Based Satellite Image Encryption

M.Sithi Benazir¹, Dr.A.Padmapriya M.C.A., M.Phil., Ph.D²

Research Scholar, Department of Computer Science and Engg., Alagappa University, Karaikudi, India¹

Assistant Professor, Department of Computer Science and Engg., Alagappa University, Karaikudi, India²

Abstract: Images are one of the prominent techniques to transfer the data between the sender and the receiver. Most of the information is transmitted in electronic form which needs more security. Cryptography is the art and science of transmitting the data to the receiver in unclear meaningless format. In order to ensure the information security, image encryption technology has aroused much interest in both research and application fields. Cryptography is the discipline of codes to encrypt data into an unreadable format that only the targeted recipient can decrypt and read. Encryption is a common technique to protect image security privacy. Matrix operations are widely used in many cryptography algorithms to solve the difficulty in means of speed and time. This paper embrace a new encryption method for satellite based images which are combined of versatile composition. The encryption for the satellite images in this paper consists of the division of image into matrix and then, the elementary row and column operations are considered. The results show enhanced performance in a variety of parameters. The grouping of basic matrix form and elementary row operations yields good results and better image encryption methods compared to existing works.

Keywords: Satellite image, Image Encryption, Matrix form, Elementary Row Operations, Elementary Column Operation.

I. INTRODUCTION

Image encryption techniques try to convert original image to another image that is hard to identify, to maintain the image confidential among users, it is essential that nobody could get to know the content without a key for decryption [3]. Images are widely used in different processes. Security has become important for many applications such as confidential transmission, video surveillance, military, medical applications etc. With the large-scale research in space sciences and space technologies, there is a enormous require of satellite image security system [4] for providing secure storage and transmission of satellite images over internet and common network surroundings. This carried innovative challenges to protect sensitive and critical satellite imagery from unauthorized access and illegal use in order to keep the storage and transmission process secure and reliable. To protect satellite images some cryptographic techniques are used [5]. Satellite communication was designed based on the Shannon information theory in which the entire data was transmitted in way of bit streams. Most important advantage of this mode of communication is that this includes an unbreakable encryption method with highly compressed image. Image is the two dimensional data which was used to carry more information than that of the text data. Encryption is one way to scramble the information, so that unauthorized person cannot understand that information [6]. Images in digital format is defined as a two dimensional rectangular array. Each element of the array is denoted as pixels. This pixel has the intensity values and the location address on the row and column wise. A satellite is an object that tracks another object, the term is frequently used to illustrate an artificial satellite [7]. The satellite images provide a

variety of information; the satellites pass on information to the base centre on the planet through telephonic messages, pictures from satellite TV and emergency snap shots retrieved from ships and aircraft. The satellite images are generated with the intent of creating an imaging network for even the most inhospitable regions on land and the oceans [8]. Earth observation (EO) satellites are satellites specifically designed to observe Earth from orbit this Earth Observation satellite takes images on earth by using the image sensors. Earth Observation satellites were used more effectively in disaster management support. Today meteorological satellites are broadly used to sense and follow severe storms and to support other weather-driven events [7]. Thus the encryption for the satellite images is considered as difficult to done. To enhance the security the images must be encrypted and then transmitted. This paper introduces a new algorithm to image encryption with basic mathematical operations. The paper is structured as follows. Section 1 consists of the basic introduction about the satellite images and basic cryptographic techniques. Section 2; highlight the related works of the satellite image encryption. Section 3 contains the proposed method for the satellite image encryption. Section 4 shows the results and discussions for the proposed method. Section 5 concludes the method with better performance.

II. RELATED WORKS

Naida.H.Nazmuden et al. [9] has proposed a new method for satellite image security by combining DWT-DCT watermarking and AES encryption. In this technique, the combined DWT-DCT watermarking algorithm's was performed. For watermarking, the preferred color model must be HSV (Hue, Saturation and Value) rather than

RGB because it is the most closely related color model with Human Visual System. Salt and pepper noise of input color satellite image can be removed by using their algorithm. Watermarked satellite image is obtained by implementing watermark embedding process. Original satellite image and secret image can be recovered back by using extraction process.

In 2013 Panduranga et al. [6] have proficiently put forward a concept of selective image encryption in two ways. First method divides the image in to sub blocks, then selected blocks are applied to encryption process. Second method automatically detects the positions of objects, and then selected objects are applied to encryption process. Morphological techniques are used to detect the positions of the objects in given images. These two approaches are very much suitable for specific applications like medical image encryption and satellite image encryption.

In 2012 Praveen et al. [10] proposed a new fault tolerant technique based on AES, by using the Advanced Encryption Standard algorithm the single Event Upset problem can be entirely eliminated and the fault toleration can be achieved. The faults are rectified by using Hamming Error Correction code Algorithm. The proposed approach reduces the SEU while transmission of data from satellites with noise.

In 2012 Dr.Emad et al. [11] has proposed combines the compression and encryption techniques into two phases, encoding and decoding phase. The fractal compression technique is selected to compress the aerial images due its high compression capability and the Enhanced Hill Multimedia Cryptosystem (EHMC) is used for encryption to perform the goal. The first encoding stage compresses the input image based on the fractal algorithm giving high compression ratio. The second encoding stage encrypts the compressed input image by using the EHMC algorithm before transmitted it to the receiver at the decoding phase.

In 2009 H. H.Nien, et al. [12], explained about image encryption based on multi chaos system. The authors proposed a hybrid encryption technique for the color image based on the multichaotic-system which combines Pixel-Chaotic-Shuffle (PCS) and Bit-Chaotic-Rearrangement (BCR). The idea of applying chaos theory on image encryption is because of the behavior of chaos system exhibiting nonlinear dynamics and sensitivity to initial conditions. The test methods involving key space and correlation coefficient are adopted for the security analysis. Eventually, empirical images are adopted as examples to prove encryption performance of the authors proposed method.

III.SATELLITE IMAGE PROCESSING ✓

With the large-scale research in space sciences and space technologies, there is a great demand of satellite image security system for providing secure storage and transmission of satellite images. As the demand to protect the sensitive and valuable data from satellites has increased, protection of satellite images becomes very important. In this proposed method, Elementary matrix

operation is performed to protect the satellite images with increased confidentiality and secrecy.

An image is a digital component that was comprised of a two dimensional rectangular array [6]. The remotely sensed image was typically a picture consists if lot of picture elements (pixels) that are located at row and column at every bands of the image. For the satellite images, that are associated with each pixel is a number known as Digital Number (DN) or Brightness Value (BV) that depicts the average radiance of a relatively small area within a scene.



Fig 1. Sample Satellite Images

3.1 Proposed Image Encryption Algorithm

The proposed method is based on the elementary matrix operation. The input of the proposed system is satellite image which was the gray scale image. The given input gray scale image is converted into pixel matrix, and then the matrix rows are interchanged into columns and columns are interchanged into rows, multiply they each element by the key value of S.

Basic elementary operations plays most important role in matrix applications. The proposed work completely converts the basic image into matrix format for further processing to taken place. In matrix methods, existing three kinds of matrix operations such as Interchange two rows, multiply each element in the given row by a non-zero number and finally multiply a row or column by a non zero number and add the result to another row or column. When the changes are considered for row, they are called elementary row operations where as for columns are known as elementary column operations.

In our proposed work, the given image is converted into matrix. Each pixel is considered as an element to operate on. The basic notations used for matrix operations are as follows,

- ✓ Interchange rows i and j - $R_i \leftrightarrow R_j$
- ✓ Multiply row i by s, where $s \neq 0$ - $sR_i \rightarrow R_i$
- ✓ Add s times row i to row j - $sR_i + R_j \rightarrow R_j$
- ✓ To carry out an elementary row operation on A, an $r \times c$ matrix, takes the following steps.
- ✓ To find E, the elementary row operator, affect the operation to a row and column as identity matrix.
- ✓ To carry out the elementary row operation, pre multiply A by E.

3.2 Methodology

The color code value accepted only 256, so the mod 255 operation was performed to the process of encryption. The decryption is just the reverse process of the encryption method. After decryption method, the proposed method has strong capability to retrieve the original satellite image without any noise and the size of the decrypted image is

equal to original image. The fundamental algorithm for the proposed method with illustration was explicated below.

3.3 Algorithm for Encryption Scheme

- Step 1: Consider the input image, as satellite image.
- Step 2: Divide the every color band of the input image.
- Step 3: Convert each color band into matrix that was identity with pixel values as elements.
- Step 4: Now, from elementary row operation, convert each rows (i.e) Interchange the rows.
- Step 5: Interchange the columns of the rows.
- Step 6: Generate, key element, which was to be multiplied with the converted matrix.
- Step 7: Apply mod function (mod 256) with each pixel values to take respective matrix within 0 to 255.
- Step 8: The resultant matrix is the Remainder matrix with the encrypted image.

3.4 Algorithm for Decryption Scheme

- Step 1: Calculate Quotient matrix from the resultant matrix after the mod operation.
- Step 2: The reverse process is the decryption.
- Step 3: To get the encrypted pixel elementary the following calculation is performed
(Pixel Element) + (Quotient Matrix * 256)
- Step 4: Divide the resultant matrix by the key element generated.
- Step 5: Exchange the column elements.
- Step 6: Exchange the Row Elements.
- Step 7: Now, the original image was recovered.

A demonstrated example for the proposed method is as follows:

$$\text{Matrix } E = \begin{bmatrix} 10 & 20 \\ 30 & 40 \end{bmatrix}$$

Interchange E as E1 ↔ E2

$$= \begin{bmatrix} 30 & 40 \\ 10 & 20 \end{bmatrix}$$

Interchange Columns C1 ↔ C2

$$= \begin{bmatrix} 40 & 30 \\ 20 & 10 \end{bmatrix}$$

Multiply Matrix E by Key K

$$= \begin{bmatrix} 40 & 30 \\ 20 & 10 \end{bmatrix} * 30$$

The Resultant Matrix is

$$= \begin{bmatrix} 1200 & 900 \\ 600 & 300 \end{bmatrix}$$

Apply Mod (E mod 256)

$$= \begin{bmatrix} 1200 & 900 \\ 600 & 300 \end{bmatrix} \text{mod } 256$$

The remainder matrix

$$= \begin{bmatrix} 176 & 132 \\ 88 & 44 \end{bmatrix}$$

Consider the remainder matrix as the encrypted matrix. The decryption is the reverse process of the encryption. It is as follows:

$$E = \begin{bmatrix} 176 & 132 \\ 88 & 44 \end{bmatrix}$$

The remainder matrix

Multiply the mod value 256 with the quotient matrix obtained from remainder matrix.

$$= \begin{bmatrix} 256 \times 4 & 256 \times 3 \\ 256 \times 2 & 256 \times 1 \end{bmatrix} \\ = \begin{bmatrix} 1024 & 768 \\ 512 & 256 \end{bmatrix}$$

Add the Remainder matrix value with the obtained result

$$= \begin{bmatrix} 1024 + 76 & 768 + 132 \\ 512 + 88 & 256 + 44 \end{bmatrix}$$

The Acquired Original Matrix is

$$D = \begin{bmatrix} 1200 & 900 \\ 600 & 300 \end{bmatrix}$$

Divide the original matrix by key value 30

$$= \begin{bmatrix} 1200 & 900 \\ 600 & 300 \end{bmatrix} / 30$$

The resultant Matrix is

$$= \begin{bmatrix} 40 & 30 \\ 20 & 10 \end{bmatrix}$$

Interchange D as D1 ↔ D2

$$= \begin{bmatrix} 30 & 40 \\ 10 & 20 \end{bmatrix}$$

The Decrypted Matrix D after Interchanging the Column is

$$D = \begin{bmatrix} 10 & 20 \\ 30 & 40 \end{bmatrix}$$

Hence E=D.

IV. RESULTS AND DISCUSSIONS

4.1 Experimental Results

The proposed method executes the following results from their experimental analysis. Several tests were being considered so as to check the security aspect of the proposed cryptosystem.

The following parameters were considered to analyse the proposed scheme. The PSNR value was extracted from the results that are yielded. To analyse, for the proposed encryption scheme, three satellite images as the sample plain images are considered.

Their plain, cipher and decrypted images are shown in table1.

Table 1: Experimental Results

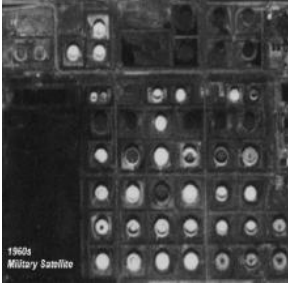
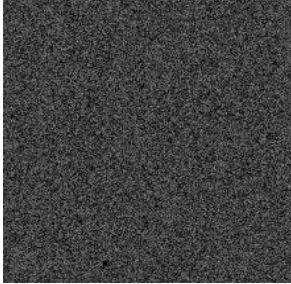
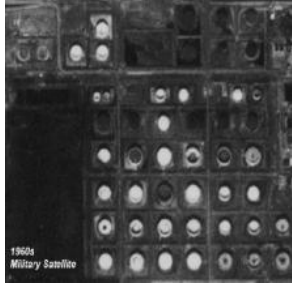






Input Image	Encrypted Image	Decrypted Image
		
		
		

TABLE 2: PSNR VALUES OF PLAIN IMAGE AND ENCRYPTED IMAGE

Image Name	Size(in KB)	Resolutions	PSNR(db)
1	768	512*512	10.62
2	628	638*398	9.99
3	733	537*466	8.88

The proposed method effectively protects against the decryption of exhaustive attack method.

TABLE 3: RESULTS OF ELAPSED TIME MEASURED DURING ENCRYPTION AND DECRYPTION

Image Name	Encryption time (in ms)	Decryption time (in ms)
1	518	512
2	341	352
3	393	406

The performance of the algorithm was measured by some important quality aspects for better PSNR, and lower MSE. A good encryption scheme must possess high encryption quality and low execution time.

V. CONCLUSION

Satellite sensed data is important to a broad range of disciplines since it consists of geographically dispersed images. The proposed cryptosystem, for the satellite images, keeps the quality of the image well and also robust against various attacks of encryption. The comparability of the recovered encrypted image with the original image

can quantitatively analyze with the aid of parameter, peak signal to noise ratio (PSNR). From the experimental results it is clearly demonstrated that the proposed cryptosystem expresses very low execution time which in turn reduces the computational complexity. The PSNR values calculated by the proposed method show the security enhancement of various file sizes with different

resolutions. The proposed algorithm provides efficient encryption for the image data, the time and throughput is also very high, with good performance in image quality and PSNR values.

REFERENCES

- [1] M. Kiran Reddy et al, "Implementation and Analysis of a Novel Block Cipher", International Journal of Computer Applications, Vol no. 8, pp. 34-36, March 2014.
- [2] T.Sivakumar et al, "A Novel Image Encryption Approach Using Matrix Reordering", WSEAS Transactions On Computers , Vol no. 12, pp. 407-418, Nov 2013.
- [3] Luo Yu-Ling et al, "A self-adapting image encryption algorithm based on spatiotemporal chaos and ergodic matrix", Chin. Phys. B Vol. 22, No. 8 (2013) 080503.
- [4] Gelan Yang et al, "Image Encryption Using the Chaotic Josephus Matrix", Mathematical Problems in Engineering , Volume 2014, Article ID 632060, 1-13 pages.
- [5] Komal D Patel, "Image Encryption Using Different Techniques:A Review", International Journal of Emerging Technology and Advanced Engineering, Volume 1, pp. 30-34, Nov 2011.
- [6] H.T.Panduranga and SK.Naveen kumar, "Selective image encryption for Medical and Satellite Images", in International Journal of Engineering and Technology, Vol 5 No 1, pp: 115 – 121, Feb-Mar 2013
- [7] <http://www.wordiq.com/definition/Satellite>.
- [8] www.buzzle.com/articles/nasa/-satellite-images.html.
- [9] Naida.H.Nazmudeen and Farsana.F.J, "A New Method for Satellite Image Security Using WT-DCT Watermarking and AES Encryption", International Journal of Innovative Research in Science, Engineering and Technology, Volume number 3, pp. 69-76, July 2014.
- [10] Praveen.HL and H.S.Jayaramu et al , "Satellite Image Encryption using AES", International Journal of Computer Science and Electrical Engineering , Vol. 1, pp. 56-60, 2012.
- [11] Dr. Emad S. Othman et al, "Compression and Encryption Algorithms for Image Satellite Communication, International Journal of Scientific & Engineering Research , Volume number 3, pp. 1-4, sep 2012.
- [12] H. H.Nien, W. T. Huang, S. C. Chen, C. H. Liu, . Y. Wu, Y. R. Tian and C. K.Huang, Y. H. Hsu, "Hybrid Image Encryption Using Multi-Chaos-System", in ICICS 2009.