

DESIGN AND SIMULATION OF SECURE IMAGE ENCRYPTION ALGORITHM

Shweta P. Bhoyar¹, Prof. G. N. Wazurkar², Dr. N. N. Mhala³

¹ M.Tech, Electronics Department, Bapurao Deshmukh College of Engineering, Sewagram, Maharashtra, India

² Professor, Electronics Department, Bapurao Deshmukh College of Engineering, Sewagram, Maharashtra, India

³ Professor, Electronics Department, Bapurao Deshmukh College of Engineering, Sewagram, Maharashtra, India

ABSTRACT

Encryption is the coding of information from one form to another. This coding of information is done through various methods. In this papers, the wavelet transform and Rubik's cube encryption algorithm is used. By using Wavelet transform in combination with the Rubik's cube algorithm, the image which is encrypted is more secured. This papers shows the encryption and decryption by using the same secret key for both. Such type of encryption is called as symmetric encryption. Here the two pseudorandom vectors K_R and K_C are generated. This is to create the confusion and diffusion within the image. The parameters Number of pixels change rate (NPCR) and unified average changing intensity(UACI) are calculated.

Keyword: - Encryption, Wavelet Transform, Rubik's Cube Algorithm, Pseudorandom vector

1. INTRODUCTION:

Encryption has long been used to securely save and transfer data and protect it from possible attacks. With the rapid increase in transferring images over the internet and mobile phones, efficient and strong image encryption techniques are needed. Cryptography and steganography are two different approaches for achieving this privacy. In cryptography, original data is coded into unreadable ciphered form before storing or transmitting it. On the other hand, steganography embeds the original data into a cover media, such as images, audio or video, to hide its existence. In other words, steganography performs data hiding such that no one other than the intended recipient knows of its existence. This is in contrast to cryptography, where the existence of the data is not hidden but its content is obscured. Digital cryptosystems are typically divided into two generic types according to the key distribution: symmetric-key and asymmetric-key. Symmetric-key cryptosystems use the same secret key for encryption as well as decryption. Because of their efficiency, they are appropriate for handling large amounts of data at high speed. The key length of symmetric ciphers usually ranges from 128 to 256 bits. With respect to the encryption algorithm, cryptosystems are divided into block and stream ciphers. Block ciphers encrypt the original message by grouping the symbols in blocks such that each block is always encrypted/decrypted in the same way. Stream ciphers generate a pseudorandom stream of symbols using a deterministic public algorithm governed by a secret key. The message is mixed with this sequence, usually through a modulo 2 sum (exclusive or, XOR), resulting in the ciphered message.

The image encryption system uses fractal images as a highly variant source for encrypting other images. Although the concept of fractals includes a wide class of objects, many of the most popular fractal images can be obtained through IFS. IFS have received a lot of attention because of their appealing combination of conceptual

simplicity, computational efficiency and great ability to reproduce natural formations and complex phenomena. There are miscellaneous programmes, which are freely available on the internet, for generating and rendering IFS fractals. In general, the process of generating a fractal can be simplified into three stages. In the first stage, all initialisations take place. In the second stage, the iteration formula is applied repeatedly under a condition of termination. Finally, the third stage performs post-processing on the resulting vector (pixel rendering). In this system, each fractal can, first, be shifted in both horizontal and/or vertical directions. Then, some selected fractals are XORed with the source image to produce a modified image. To strengthen the encryption system, delay and multiplexing blocks are added to help in making the encrypted image look random. The delay block serves as the memory of the encryption system, which utilises the previous encryption result. The multiplexing block selects which colour channels of the delayed and modified images are XORed together to produce the final encrypted image. To evaluate how each system block contributes to the encryption process, we start by using only one fractal image and analysing the encryption results. After that, the system is examined using multi-fractal images and the analysis results are given. The encrypted images are analysed using correlation coefficients, differential attack measures, histogram distributions and NIST statistical test suite.

2. OVERALL ANALYSIS OF RESEARCH WORK:

Some researchers used chaotic pixels substitution (in order to achieve desired diffusion factor) and Rubik's cube, principle based, pixels permutation (in order to achieve desired confusion factor)[4]. To confuse the relationship between original and encrypted images, the XOR operator is applied to odd rows and columns of image using a key. The same key is flipped and applied to even rows and columns of image[3]. A new method to develop secure image-encryption techniques using a logistics –based encryption algorithm. In this technique, a Haar wavelet transform was used to decompose the image and decorrelate its pixels into averaging and differencing components. The logistic based encryption algorithm produces a cipher of the test image that has good diffusion and confusion properties. Many papers propose a chaotic system using two traditional chaotic maps: the Logistic map and Sine map or combination of both[6]. The logistic based encryption algorithm produces a cipher of the test image that has good diffusion and confusion properties. In some papers encryption system with two major parts, chaotic pixels substitution (in order to achieve desired diffusion factor) and Rubik's cube, principle based, pixels permutation (in order to achieve desired confusion factor). The performance assessment tests attest that the proposed image encryption scheme is fast and highly secure. Although a much smaller key space is used, but still large enough to face against exhaustive attack, with a smaller key size, the proposed encryption scheme presents better results, compared to those of previously proposed ones. Many test images are used to demonstrate the validity of the proposed algorithm. The results of several experiments show that the proposed algorithm for image cryptosystems provides an efficient and secure approach to real-time image encryption and transmission.

3. METHODOLOGY USED:

- Pre-processing of input image.
- Decomposition of image using wavelet transforms.
- Encryption using Rubik's cube principle.
- Decryption using Rubik's cube principle.
- Reconstruction using inverse Wavelet transforms.
- Performance evaluation

4. WAVELET TRANSFORM:

In the proposed work the Haar wavelet transform is used to create the shuffling of the image. By this shuffling of the image the image creates complexity and more is the complexity better is the encryption. Wavelet transform decomposes the gray scale image into four patterns of different frequencies i.e. LL, LH, HL, HH. After that, these patterns are shuffled. When the wavelet transform is applied to the image and the results are shown in figure 1.

5. RUBIK'S CUBE ALGORITHM

5.1 Encryption

1. I_0 : α bit gray scale image.
Image size is $M \times N$.
2. Generate random vectors K_R & K_C of length M & N resp.
3. $K_R(i)$ & $K_C(j)$ elements take a random value of set $A=\{0,1,2,3,\dots,2^\alpha-1\}$. K_R & K_C - must not have constant value.
4. Determine no. of iteration. $ITER_{MAX}$ & initialize the counter $ITER$ at 0.
5. Increment counter by 1, $ITER=ITER+1$.
6. For each row of i of image I_0 .
 - a. Compute the sum of all elements in row i
 - b. Compute modulo 2
 - c. Apply left or right circular shift
7. For each column of j of image I_0 .
 - a. Compute sum of all elements in column j
 - b. Compute modulo 2
 - c. Apply up or down circular shift
8. Step 6 and 7 will create a scrambled image denoted by I_{SCR}
9. Using vector K_C – Bitwise XOR operator is applied to each row of scrambled image I_{SCR}
10. Using vector K_R – Bitwise XOR operator is applied to each column of scrambled image I_{SCR}
11. If $ITER= ITER_{MAX}$ then,
Encrypted image I_{ENC} is created and
Encryption is successfully done
Otherwise it goes back to step 5.
 K_R and K_C : SECRET KEY
But here, $ITER_{MAX} = 1$: fast encryption

5.2 Decryption

1. Initialise $ITER = 0$
2. Increment the counter by 1, $ITER = ITER + 1$
3. Bitwise XOR operation on vector K_R of the encrypted image I_{ENC}
4. Bitwise XOR operation on vector K_C
5. For each column j of scrambled image I_{SCR}
 1. Compute sum of all element
 2. Compute modulo 2
 3. Apply up- down circular shift
6. For each row i of scrambled image I_{SCR}
 1. Column sum of all elements
 2. Compute modulo 2
 3. Apply left or right circular shift
 4. If $ITER=ITER_{max}$ then,
Image is decrypted. Otherwise it goes back to step 2
7. Here decryption is completed.

6. RESULTS:

Results can be tested for various images. Following is the outputs of the above explained methodology. The output results shows the colored image which is converted into gray scale image. After the conversion of the gray scale image wavelet transform is applied to the image which then results to the shuffled image. Rubik’s cube encryption algorithm is applied and the output shown in figure 1 is obtained.

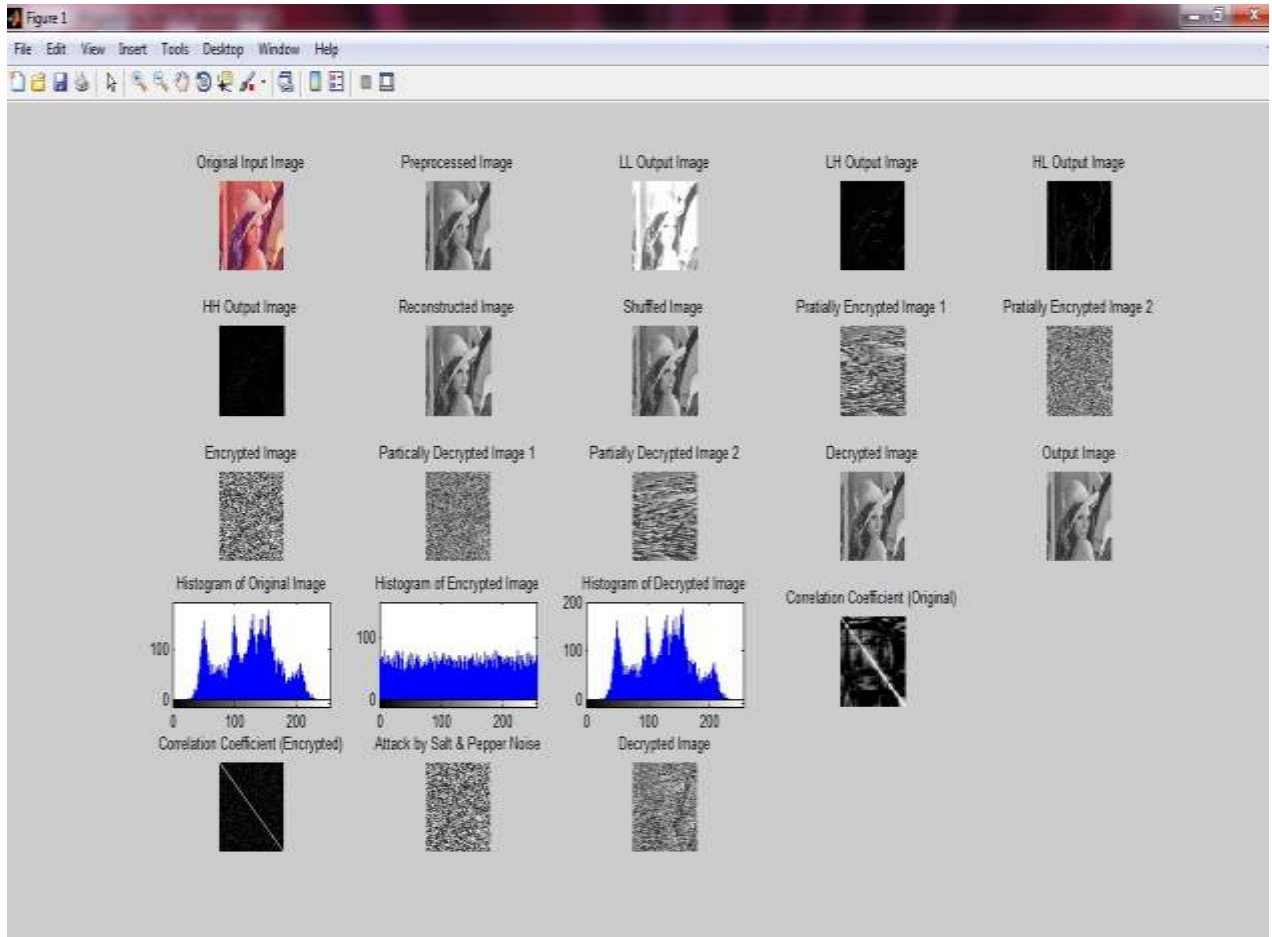


Fig -1: Output : Lena image

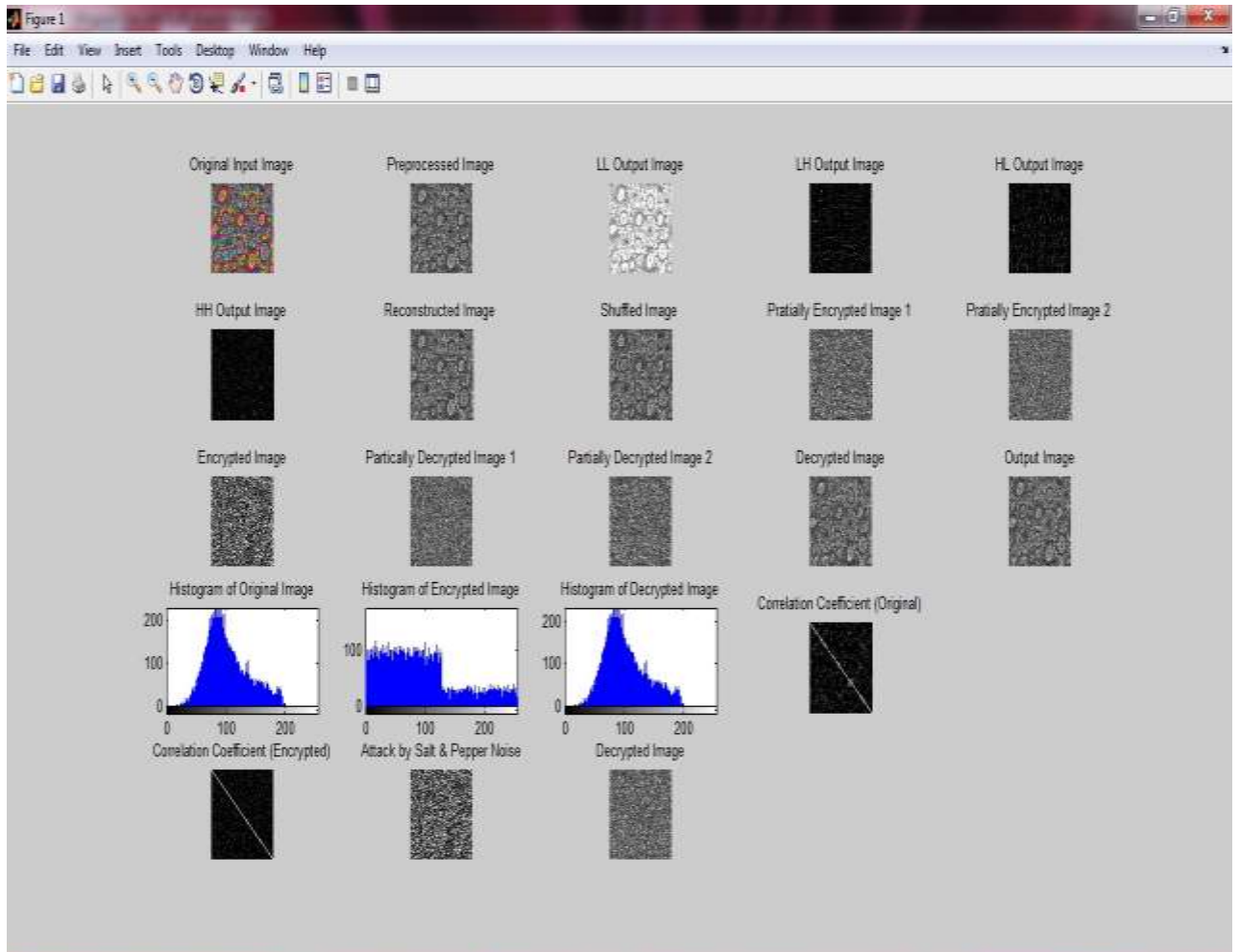


Fig -2: Output : Complex image

7. PARAMETERS EVALUATED:

For Lena image:

parameters	original image: Lena	encrypted image: Lena
entropy	7.4114	7.9863
correlation coefficient	0.962	0.00834

Table -1: Output of image: Lena

Number of pixel change rate (NPCR) = 99.62%

Unified average changing intensity (UACI) = 13.42%

For Complex image:

parameters	original image: complex	encrypted image: Complex
entropy	7.34	7.76
correlation coefficient	0.3026	0.002

Table -2: Output of image : Complex

Number of pixel change rate (NPCR) = 99.46%

Unified average changing intensity (UACI) = 13.84%


8. CONCLUSIONS:

In this project, we have used two types of encryption i.e. wavelet transform and Rubik's Cube Principle to obtain more secure image. Here it can be concluded that by using wavelet transform and Rubik's Cube Principle there is improvement in confusion properties of algorithm that results in highly secure image. Improvement of parameters is the main motive of the project. Hence by improving the values of parameters NPCR and UACI the result shows improvement over previous researches.

9. REFERENCES

- [1]. Liu Hongjuna, Wang Xingyuana, "Color image encryption based on one-time keys and robust chaotic maps", in Elsevier Journal Computers and Mathematics with Applications, vol 59, 2010, pp 3320 – 3327.
- [2]. Salwa Kamal Abd-El-Hafiz, Ahmed G. Radwan, Sherif H. Abdel Haleem, Mohamed L. Barakat, "A fractal-based image encryption system", in IEEE Transaction on Image Processing, vol. 8, issue 12, 2013, pp. 742 – 752.
- [3]. Khaled Loukhaoukha, Jean-Yves Chouinard, Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", in Hindawi Publishing Corporation Journal of Electrical and Computer Engineering, volume 2012.
- [4]. Adrian-Viorel Diaconu, Khaled Loukhaoukha, "An Improved Secure Image Encryption Algorithm Based on Rubik's Cube Principle and Digital Chaotic Cipher", in Hindawi Publishing Corporation Mathematical Problems in Engineering, volume 2013.
- [5]. Nidhi Sethi, Deepika Sharma, "A New Cryptology Approach for Image Encryption", in 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012.
- [6]. C.L. Philip Chen, Tong Zhang, Yicong Zhou, "Image Encryption Algorithm Based on A New Combined Chaotic System", in IEEE International Conference on Systems, Man, and Cybernetics, 2012.

BIOGRAPHIES

	<p>SHWETA P. BHOJAR Student: MTECH (ETRX) Bapurao Deshmukh College Of Engineering Sewagram Wardha Email-id: sweetybhojar@gmail.com</p>
---	---