NOVEL HYBRID IMAGE ENCRYPTION (64-Bit) BASED ON RUBIK CUBE AND BLOCK CIPHER

Jasdeep Singh Chauhan
Student
Dept. of CSE Rayat Bahra Campus
Ropar

Amanpal Singh Rayat
Asst. Professor
Dept. of CSE, Rayat Bahra Campus
Ropar

Abstract: Cryptographic Encryption is a method, for the protection of useful information so that only those for whom it is intended can read and process it. Numerous applications are there which require the rapid and strong security against the unauthorized users. For example, securing Military related information, securing sensitive online transactions, securing online transmission of data for real time applications like stock market apps, electronic mails or data transmission of social applications and online personal photograph albums like applications demand for the high security as these are stored and transmitted throughout the internet. The image Encryption is one of the techniques used for alteration of the images into faint form so that the image cannot be seen by the prohibited person. In this paper we explore the Novel Hybrid technique to encrypt image by following the concept of Rubik Cube encryption phenomenon (stream cipher) and combine it with block cipher.

Index Terms: - Novel Hybrid, Encryption, Decryption, Rubik Cube, Symmetric key cryptography, Secure Force Algorithm, secret key.

I. INTRODUCTION

The use of multimedia data such as digital images, videos, audios etc. is increasing with the continuing growth in information technology. Such applications are like video conversation, online photograph albums, imaging systems and so forth. Nowadays, these applications play a vital role towards the various aspects of our daily life, including learning, business and for personal usage.

Digital data Image encryption algorithms try to convert original data image to another form of image that is hard to understand and recognize. One can say in other word, to keep the image confidential between authorized users, it is essential that nobody (un-authorized user) could get to know the content without a key for decryption. Moreover, special and reliable security in Storage and transmission of digital images are needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfill such a task, many image encryption methods have been proposed.

Image Encryption is generally the term used for translation of an original figure to the ciphered mode whereas converting the original figure from its ciphered form is known as Image Decryption. However, there are many schemes included for enciphering the data includes both textual data and digital data. On the basis of way of encryption carried out, there are two types of cryptographic encryptions:

- Secret key cryptography: Secret key cryptography is the set of steps in cryptography to carry out encryption with single key called secret key. The whole process of encryption is based on just one key. In this type of cryptographic encryption, both the sender and receiver are known to same secret key. The sender uses this key to encrypt the input data and receiver on the other hand uses the same key for decryption. This is also known as symmetric key encryption.

- Public key cryptography: In this type of cryptographic encryption there are two keys to carry out the whole process. The first key, also called public key, is used by sender to encrypt the message and is done by easy set of steps whereas another key is used for decryption is known to receiver only. This type of encryption is also known as asymmetric encryption.

The use of cryptographic techniques plays the great role in carrying out transmission of data over network with security. The cryptographic techniques need some set of rules called algorithms that are publicly defined yet considered to be secure. Now a day almost every kind of data is transmitted over the internet that includes both textual and digital data, so security plays great role in that to ensure information security and safety. There are many algorithms available for textual data encryption as textual data encryption is far easy and fast as compared to image or video data encryption as in case of multimedia data the bits are more dependent to each other and hard to process it with textual encryption.

The security of images or one can say digital data is the major concern of this paper. Traditional image encryption algorithms such as private key encryption algorithms (DES and AES), public key algorithms such as RSA (Rivest Shamir Adleman), and the family of elliptic-curve-based encryption algorithms (ECC), as well as the international data encryption algorithm (IDEA), may not be the desirable candidates for image encryption to better extent, particularly for fast and real-time communication applications. In recent years, several encryption schemes have been proposed [1–12]. These encryption schemes can be classified into different categories such as value transformation [1–4], pixels position permutation [5–8], and chaotic systems [9–12].

II. PROBLEM FORMULATION
The proposed work is basically a cryptographic security algorithm in which image is encrypted to a form that is not understandable and recognizable unless and until it is decrypted with security. The focus is mainly on major concepts in the whole process of encryption of image. The algorithm focuses on encryption level as good as Secure Force algorithm provides for textual data and on the other hand with less time consumed in encryption and decryption process. The comparison of SF with AES algorithm on FPGA platform is mentioned in [22].

The basic motivation to the proposed approach is to improve the fast and secure communication of multimedia data over internet transmission. For security of data many algorithms are developed but not every algorithm works smoothly when it comes to the point of fast transmission with high security. In this proposed algorithm the collective work of Secure Force algorithm which is a light weight and less calculative algorithm is combined with Rubik Cube algorithm to get better result in the form of good encryption with more security yet with better speed.

III. NOVEL HYBRID IMAGE ENCRYPTION BASED ON RUBIK CUBE AND BLOCK CIPHER.

With the improvement in the today internet communication technology, numerous applications are there with various encounters that includes power utilization, security problems, scalability and design simulation problems. There are networks called Wireless Sensor Networks which claims an algorithm to provide high and trustworthy security with small power utilization as of low resources available to them. The proposed Novel Hybrid algorithm is one of the nominees for fast and secure algorithms. The design of proposed algorithm delivers low and simple complexity architecture. To safeguard energy efficient execution, it is suggested to lower the number of encryption rounds [15] [16]. In Novel Hybrid algorithm each encryption round encompasses six modest arithmetic operations on 64-bit data to certify security followed by scrambling of data. These steps create the satisfactory amount of confusion and diffusion in data to challenge various types of attacks. The key expansion process, implemented at the decoder, involves the same very light weight process followed by descrambling and simple 16-bit diffusion and reform the original image and it contains simple mathematical operations such as multiplication, addition, rotation, permutation and other operations like transportation is there to produce keys for the encryption process. However, the keys generated must be transmitted securely to the encoder side for the encryption process. The process of Novel Hybrid algorithm consists of 4 major blocks. The detailed description of logical operations used of the proposed algorithm can be found in [1]. Key Expansion Block: Key expansion is the very first and primary method that is used to generate altered keys for encryption and decryption. There are different operations that are performed in order to create confusion and diffusion for more security. This whole process is to reduce the possibility of weak key as well as to increase the key strength and to ensure energy efficient implementation, it is suggested to lower the number of encryption rounds [13]. The round keys (Kr) are derived from the input cipher key by means of the key schedule. The whole process consists of two components: key expansion (where key is expanded to perform operations on it) and key reduction (where expanded key undergoes logical operations to make final key). The key expansion performs dividing 64-bit key into 16-bits keys to operate logical operation on them where as key reduction phase includes performing operation on 16-bits keys blocks to convert them to final 16-bit key in order to make it able for 64-bit data encryption. The block diagram of the key expansion block is shown in fig. 1.

Key Management Protocol: The key management protocol is there to accomplish transmission of key over the network to decoder end to ensure the safety of key. As the whole process of encryption and decryption depends on the same key so key security is must for the algorithm security. Encryption Block: The process of encryption is initiated with the key expansion block where keys generated are securely received by the encoder side through the communication channel which is assumed to be secured by following any protocol rules. Then process of encryption is carried out with simple operations with XOR, OR, AND, XNOR, left shift (LS), substitution (S boxes) and swapping operations, are performed to create high level confusion and diffusion. The detailed block diagram of the encryption block is shown in fig. 2.
Decryption Block: In the process of decryption the whole process of encryption is executed but in opposite manner with same key used in encryption process.

The execution of encryption process on hardware level holds many of the choices that are used in execution process including loop unrolling that may be full, partial and etc., pipelining, substitution box designs, data path width optimization etc. Though it is good to use but the complete parallel loop unroll architecture is chosen only at those locations where high throughput is required.

The Novel hybrid algorithm consists of three units; the key generation module, image input encryption module, and the encrypted image decryption module. The proposed algorithm termed Novel hybrid chains all the three modules together to form a whole single-unit. First, a key is passed and it is converted into 64-bit binary key then the generated key authorizes through the key generator which generates Final Key of 16 bits to encrypt 64-bits block of image in encryption phase. The generated key act as a input to the encryption block along with the plain text from the binary image and converts it into a cipher text of 64-bits by applying the encryption process. In that round key K1 will be used and in the final step, the encrypted message generated by the same key used. The same procedure of encryption is repeated again and again for high end recursive encryption. The large number of replication loops, the better is the encryption but on the same end the greater consumption of resources and more time consuming.

From encryption the encrypted data is passed to the decrypted block which process the encrypted block with the reverse encryption process which also contains one decryption round, and it uses the same key K1 to apply the process of decryption on the encrypted message to get it back to a plain text. To examine the overall performance of the specific block of each decryption, encryption and key expansion block is executed separately. The thorough explanation of the sub-modules of Novel hybrid will be given in their particular sections.

Key Expansion Block

Key expansion is the foremost process that is used to produce keys for the process of decryption and encryption cycles to carry out. Different operations are executed counting various logical operations in order to create diffusion and confusion. This process is to lessen the opportunity of generation of feeble keys as well as to upsurge the strength of key. The round key (K1), that is derived from the input cipher key (Kr), whose length is same as length of image matrix, by means of the key schedule. The process involves of breaking 64-Bit key into 16 bit blocks of keys and taking XOR of first two sets and last two sets and then take XOR of the final two sets to produce final 16-bit key. Here the key generated is of size 16-bit whereas the block size of image to be encrypted is of 64-bit, for that we need to convert image matrix into rows of 8 count and columns count may vary that when converted to binary led to 64-bit column count.

Encryption Block

We have key Kr to start the procedure of encryption. The very first step of encryption contains the scrambling of image as needed to create diffusion and confusion of the original data image. For that the block of image is considered and processed row wise. Each row of the image is processed one after the another (serial wise). The scrambling of image is carried out by taking the submission of all elements of row, on which processing is done and take modulo 2 of the submission. The submission of image is carried out as:

\[
\alpha(i) = \sum_{j=1}^{N} I_{o}(i,j), \quad i = 1, 2, \ldots, M.
\]

Where I represent the image matrix and (i,j) represents the image matrix values and j varies from 1 to length of image matrix row represented by N. Then Modular 2 is calculated for a(i) and is processed by the following mentioned equation:

\[
\text{if } M_{\alpha(i)} = 0 \quad \rightarrow \quad \text{right circular shift} \\
\text{else} \quad \rightarrow \quad \text{left circular shift}.
\]

where \(M_{a(i)}\) represents the modular 2 of image matrix row elements.
If calculated modular 2 is zero, then the row is shifter towards right side by unit present in Kr key array and on the other hand if it is not zero then it is shifted to left by the units present in Kr key location.

The above mentioned steps are repeated for all rows of image matrix as represented to create confusion and diffusion.

The below image represents the output after scrambling is done on input image.

![Fig. 4. SCRAMBLED IMAGE.](image)

If calculated modular 2 is zero, then the row is shifter towards right side by unit present in Kr key array and on the other hand if it is not zero then it is shifted to left by the units present in Kr key location.

The above mentioned steps are repeated for all rows of image matrix as represented to create confusion and diffusion.

The below image represents the output after scrambling is done on input image.

![Fig. 4. SCRAMBLED IMAGE.](image)

Once the key expansion block generates the key as per needed to accomplish block cipher encryption on image with each block of 64-bits, the scrambled image is converted into binary form in order to encrypt it accordingly. In binary form image block contains 64 columns and n number of rows. The encryption of image is carried out row wise with each row size of 64-bits, four times the size of key in binary format. The process of encryption executes by breaking the binary scrambled image 64-bits data into 16-bits four blocks separately. As we have key of size 16-bits that is same size of each block created for image data. The very first and the fourth block of image data is operated with XNOR operation with input key and the output of these blocks are operated with highly permuted and substituted box to create a lot of confusion and operated with XNOR operation with second and third block of input image data to produce another second and third block of encrypted form. The output four blocks are swapped and interchanged with first by second and third by fourth to create more confusion. The four blocks are combined to make 64-bits encrypted data of image block. These steps are performed repeatedly over all the rows of binary image data to produce encrypted image data. The output of encrypted seems as follow:

![Fig. 5. BABOON IMAGE ENCRYPTION AND DECRYPTION BY PROPOSED ALGORITHM](image)

![Fig. 6. CAMERA-MAN IMAGE ENCRYPTION AND DECRYPTION BY PROPOSED ALGORITHM.](image)

IV. EXPERIMENTAL RESULTS AND TEST CASES

The encryption power of the proposed algorithm is calculated by the universal defined tests. These tests include:

**Visual Testing:** The resolution of visual testing is to highpoint the existence of resemblances or one can say correlation, association and relation between plain-image and shuffled and (or) ciphered image i.e., if the scrambled and (or) ciphered image does not or does contain any features of the plain-image.

![Fig. 7. DIFFERENT IMAGES SHOWS ENCRYPTION AND DECRYPTION BY PROPOSED ALGORITHM TO DEPICT VISUAL TESTING. INCLUDES IMAGES (FOOTBALL, LENA, BLACK, WHITE, ORAL FACES, RICE, BOY).](image)
From the above encrypted images, it is clearly represented that encrypted images are very different from original image and gives no clue about original image as per seen visually.

**Security Assessment check by Statistical Analysis Testing:**

There are mainly two statistical analyses performed to showcase the confusion and diffusion of the encrypted image scuffling and shuffling or used ciphering algorithm named Histogram Analysis test and examination of the inter-relation or correlation coefficient between adjacent or together pixels. The very first of it is Histogram Test: This histogram test is used to perform analysis of pixels’ distribution within an image, by representing those pixels’ number relative to each intensity level.

![Fig. 8. DIFFERENT IMAGES SHOWS ORIGINAL AND ENCRYPTED IMAGES HISTOGRAM GRAPHS. INCLUDES IMAGES (BABOON, BLACK, LENA, CHECKED)](image)

PIXELS CORRELATION TEST: Pixels correlation test is the renowned test that is generally performed in plain images to judge how toughly correlation exists between any subjectively chosen pixel with its adjacent pixels, that be vertically, diagonally or horizontally oriented. For the encrypted image with little dependency of pixels led to worthy encryption rather than produced image with high pixels’ dependency. Mentioned table represents the pixel correlation values of encrypted and original images.

![Table 1. PIXEL CORRELATION VALUES OF DIFFERENT IMAGES FOR BOTH ENCRYPTION AND DECRYPTION](table)

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>ENCRYPTED</th>
<th>ORIGINAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>cameraman.tif</td>
<td>0.0105</td>
<td>0.9402</td>
</tr>
<tr>
<td>Football.jpg</td>
<td>-0.0074</td>
<td>0.9561</td>
</tr>
<tr>
<td>Lena.jpg</td>
<td>-0.0116</td>
<td>0.9379</td>
</tr>
<tr>
<td>Rice.tif</td>
<td>0.0162</td>
<td>0.851</td>
</tr>
<tr>
<td>ORLFace.jpg</td>
<td>0.0045</td>
<td>0.8724</td>
</tr>
<tr>
<td>Boy.jpg</td>
<td>-0.011</td>
<td>0.9456</td>
</tr>
<tr>
<td>baboon.jpg</td>
<td>-0.0008</td>
<td>0.8631</td>
</tr>
<tr>
<td>checkboard.jpg</td>
<td>-0.013</td>
<td>0.8963</td>
</tr>
<tr>
<td>black.jpg</td>
<td>0.0115</td>
<td>NaN</td>
</tr>
<tr>
<td>White.jpg</td>
<td>-0.017</td>
<td>NaN</td>
</tr>
</tbody>
</table>

![Fig. 9. DIFFERENT IMAGES SHOWS ORIGINAL AND ENCRYPTED IMAGES CORRELATION COEFFICIENT. INCLUDES IMAGES (FOOTBALL, LENA, ORAL FACES, BABOON, BLACK, CAMERA MAN, CHECKED)](image)

Security Assessment test by Differential Analysis: The Differential analysis related to cryptography undertakes that the invader is able to craft small changes in the input plain image and judges the output that is the processed version of image. By doing that, scuffling, shuffling and (or) encryption key(s) and (or) the meaningful interrelationship between original images from that the original image can be generated. Therefore, a necessary property of the proposed modified algorithm is to be sensitive to the small changes in plain-image. Thus the attack by differential process can miss its efficiency led it to useless practically as if even one minor change in the original image led to significant change in its processed versions.
Another analysis test to ensure encryption goodness is analysis based on differential parameters. These includes two parameters – Number of Pixels Change Rate (NPCR) and Unified Average Changing Rate (UACI). To approach the performances of ideal image encryption algorithms, the value of NPCR must be large as possible i.e. nearer to 100 percent or can say close to unity, while UACI value generated must be around 33% to be more good. The more it is nearer to 33% the better is the encryption. Following table represents the NPCR and UACI values calculated for encryption process done on different images.

<table>
<thead>
<tr>
<th>IMAGES</th>
<th>NPCR</th>
<th>UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>cameraman.tif</td>
<td>99.59</td>
<td>30.8527</td>
</tr>
<tr>
<td>Football.jpg</td>
<td>99.61</td>
<td>31.316</td>
</tr>
<tr>
<td>Lena.jpg</td>
<td>99.68</td>
<td>28.4551</td>
</tr>
<tr>
<td>Rice.tif</td>
<td>99.49</td>
<td>27.9647</td>
</tr>
<tr>
<td>ORLFace.jpg</td>
<td>99.71</td>
<td>28.7727</td>
</tr>
<tr>
<td>myimage.jpg</td>
<td>99.18</td>
<td>35.1524</td>
</tr>
<tr>
<td>baboon.jpg</td>
<td>99.6</td>
<td>26.9939</td>
</tr>
<tr>
<td>checkboard.jpg</td>
<td>95.5</td>
<td>48.6261</td>
</tr>
<tr>
<td>black.jpg</td>
<td>99.2</td>
<td>50.9527</td>
</tr>
<tr>
<td>White.jpg</td>
<td>99.63</td>
<td>47.8185</td>
</tr>
<tr>
<td>Average</td>
<td>99.559</td>
<td>33.48548</td>
</tr>
</tbody>
</table>

Security Analysis by Entropy Assessment: Image entropy is a quantity which is used to describe the business of the image i.e. the amount of information which must be coded by the compression algorithm. The ideal value of entropy of image is calculated as 8-bits, for gray-scale images of 256 levels. Nearer the entropy better is the encryption held by algorithm. The proposed algorithm for the encryption of an image must give entropy nearer to 8-bits to make it more efficient as in practice, the resulted entropy is smaller than the ideal one. As we know the smaller is the entropy, the greater the degree of predictability i.e. the poor security led to threatens encryption system’s security. Computing the entropy value of the encrypted image, which is very close to the ideal value of 8 (more accurately 7.9992, much closer than values resulted under different algorithms), we can say that the proposed encryption algorithm is highly robust against entropy attacks. For the proposed algorithm the entropy is calculated for five loops as follow:

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>NPCR</th>
<th>UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>cameraman.tif</td>
<td>99.58</td>
<td>32.8154</td>
</tr>
<tr>
<td>Football.jpg</td>
<td>99.12</td>
<td>33.0303</td>
</tr>
<tr>
<td>Lena.jpg</td>
<td>99.59</td>
<td>33.4188</td>
</tr>
<tr>
<td>Rice.tif</td>
<td>99.77</td>
<td>33.3683</td>
</tr>
<tr>
<td>ORLFace.jpg</td>
<td>99.67</td>
<td>33.0593</td>
</tr>
<tr>
<td>myimage.jpg</td>
<td>99.15</td>
<td>33.6345</td>
</tr>
<tr>
<td>baboon.jpg</td>
<td>99.52</td>
<td>33.3772</td>
</tr>
<tr>
<td>checkboard.jpg</td>
<td>99.66</td>
<td>33.8985</td>
</tr>
<tr>
<td>black.jpg</td>
<td>99.13</td>
<td>33.3443</td>
</tr>
<tr>
<td>White.jpg</td>
<td>99</td>
<td>32.43</td>
</tr>
<tr>
<td>Average</td>
<td>99.419</td>
<td>33.23766</td>
</tr>
</tbody>
</table>

The above stated table depicts the NPCR and UACI values of encryption images with original key and key with one-bit difference. Another test contains decryption of image with original key and key with one-bit difference. The following figures represents the proposed algorithm is key sensitive and even one-bit change in key do not produce image nearer to original image.

The below mentioned figures contains ‘Original’ image that is the original image and Decrypted image that is decrypted by original key and Decrypted1 and Decrypted2 are produced by key with one-bit difference. It depicts that in proposed algorithm even a bit difference in key do not bring original back from encrypted image.
Fig. 9. DIFFERENT IMAGES SHOWS ORIGINAL AND DECRYPTED VISUAL ANALYSIS PROCESSED BY ORIGINAL KEY AND TWO ANOTHER KEYS WITH ONE-BIT DIFFERENCE. INCLUDES IMAGES (LENA, BOY, WHITE, RICE, ORAL FACES, CHECKED, CAMERA-MAN, BLACK, BABOON).

Encryption Time: Encryption time depicts the time take by algorithm during encryption process. Encryption time plays important role in designing the algorithm. Lower the encryption time better the algorithm encryption and vice versa. The encryption time for proposed algorithm for different images and for different cycles figured out below:

V. RESULT COMPARISON

The evaluation of SF algorithm was agreed out on certain well know constraints used by numerous authors [17], [18], [19], [20] and [21]. Although SF shows good results and its performance is comparable to other algorithms [14], [22], [23], [24] and [25] in terms of computation cost, but it is still not as claimed. The following table represents the comparison of proposed algorithm with Rubik Cube and Secure Force Algorithm on different parameters:
Table 6. COMPARISON OF VARIOUS PARAMETERS FOR SECURE FORCE, RUBIK CUBE AND PROPOSED ALGORITHM.

<table>
<thead>
<tr>
<th>COMPARISON</th>
<th>PROPOSED ALGO</th>
<th>RUBIK CUBE</th>
<th>SECURE FORCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTROPY (ORIGINAL IMAGE)</td>
<td>7.0565</td>
<td>7.0565</td>
<td>7.0565</td>
</tr>
<tr>
<td>ENTROPY (FINAL IMAGE)</td>
<td>7.9821</td>
<td>7.6256</td>
<td>7.9813</td>
</tr>
<tr>
<td>NPCR</td>
<td>99.66</td>
<td>99.38</td>
<td>99.62</td>
</tr>
<tr>
<td>UACI</td>
<td>34.8005</td>
<td>24.7476</td>
<td>34.5138</td>
</tr>
<tr>
<td>ENCRYPTION TIME (Per Cycle)</td>
<td>0.5845</td>
<td>0.0792</td>
<td>2.9558</td>
</tr>
</tbody>
</table>

From the above demonstrated table it is clear that the Entropy, NPCR and UACI is better than both and more nearer to secure force algorithm whereas the execution encryption time for Rubik cube is still better than both but as its Entropy, NPCR and UACI is far less than proposed algorithm and Secure Force, the execution time for proposed algorithm is considered better without compromising the security and speed of execution of algorithm.

VI. CONCLUSION

In this paper I implement Novel Hybrid image encryption algorithm by applying cryptographic and logical functions on the input image. This paper focuses of processing images with less encryption consuming time without compromising the encryption security. The output decrypted image is same as that of original image without any loss of information. The encryption process managed in this algorithm is 64-bit encryption algorithm. Another advantage of this algorithm is the whole security depends on one small size key, which is easy to manage and easy to transmit.

VII. REFERENCES


26. MATLAB, The MathWorks, Inc

VIII. AUTHOR’s PROFILE

Jasdeep Singh Chauhan. Born in 1991 Received Bachelor of Technology degree in 2013 from Lovely Professional University, chehru Punjab, India. He has done his Master of Technology in 2016 from Rayat Bahra Campus, Ropar, Rail Majra, Punjab, India.