International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Low Latency for File Encryption and Decryption Using BRA Algorithm for Secure Transmission of Data

Kalyani V. Gulhane[1], Prof. G. D. Dalvi[2]

[1]P.R.Pote (Patil) College of Engineering and Management, Amravati. 444605 (M.S)
[2]P.R.Pote (Patil) College of Engineering and Management, Amravati. 444605 (M.S)

Abstract: ***The need of reliable and effective security mechanisms to protect information systems is increasing due to the rising magnitude of identity theft in our society. Cryptography involves various techniques for taking user data, readable data, and transforming it into unintelligible form, for the secure transmission over the network, and then using a key to transform it back into readable data when it reaches its destination. The main aim of this study is to increase security in communication by encrypting the information using a key that is created through using an image. Often information security is major obstacle in different areas like bank, transaction, military, network application. Whenever we want to send file from one location to another location in the network, many unauthorized users are illegally access the information. There are different algorithms like Blowfish, DES, AES, RC5 that achieve more security but increases the complexity of the algorithm and also takes more time for encryption and decryption of files. Our algorithm proposes a method for low latency encryption-decryption algorithm that will take smallest amount of time for file encryption and decryption and provide more security. This algorithm can be applied on different types of files. In Byte Rotation Algorithm a random key generation technique is used.***

Keywords: Byte Rotation Algorithm, Encryption time, Decryption time, Key generation, Parallel process.

1. Introduction

Cryptography is the art of achieving security by encoding messages to make them non-readable. It ensures the information security such as confidentiality, data integrity, entity authentication and data origin authentication, also it means hidden writing, and it refers to the technique of using encryption to hide text. Encryption is changing the original data to a secret message, while Decryption is the reverse. Algorithm is the process of encryption and decryption of the data based on a mathematical procedure. Every algorithm and techniques has its own different advantages and disadvantages. Delay, throughput, energy consumption are the important QoS of the Sensor networks. Voice, video, images, and text are examples of real time applications that need to be transmitted quickly with a high level of security. Nowadays, there are many applications that provide real time Services, such as Skype and Tango. On the other hand, there are many suggested algorithms that can be used to protect these applications and to guarantee that unauthorized persons cannot access these services. The conventional methods of encryption can only maintain the data security. The information could be easily accessed by the unauthorized users for malicious purpose. Therefore it is necessary to apply effective encryption/decryption methods to enhance data security. The multiple encryption and multilevel encryption system provides sufficient security. But as security level is increased, the time for encryption and decryption along with the complexity of algorithm is also increased. Also speed and performance of these systems is low. This is the major cause of decreasing the speed and efficiency of the encryption system. In this work we will implement a new encryption algorithm "Byte–Rotation Algorithm" which enhances the security as well as speed of the encryption scheme.

2. Literature Review

Image security is of utmost concern as web attacks have become more and more serious. Image encryption decryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored. After the survey of various methods used for image encryption we came through a few of these like Image encryption using AES, DES, RSA, Blowfish etc.

Punam V. Maitri, Dattatray S. Waghole, Vivek S. Deshpande[1] investigated parameters of network security. In this system involve two algorithms. One is Byte-Rotation algorithm and second is Advance Encryption Standard algorithm. In BRA algorithm random key generation technique and symmetric key is used. Implementation of both algorithms is done by java programming language. File encryption and decryption time is also calculated by java programming language. The Byte-Rotation algorithm gives higher quality result as compared to AES algorithm.

Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra [2] proposed encryption and decryption for text and image using AES For text encryption 128 bit text inputs are synthesized and simulated on TMS320C6713 DSP processor using Code Composer Studio tool in simple C language code. For image encryption java code is synthesized and simulated by Java Application Platform SDK. Mainly Code Block Chaining (CBC) mode with PKCS 5 padding is used for image encryption. The proposed methodology is applied for ensuring the personal privacy in

the context of surveillance video-camera systems. Only authorized users that possess the key. Key can decrypt the entire encrypted image sequence. The proposed method has the advantage of being suitable for mobile devices, which currently use the JPEG image compression algorithm, due to its lower computational requirements.

Rohit Kumar, Shekhar [3] proposed method such that they first encrypt the image using Genetic algorithm and then by using new cipher algorithm. They have also calculated the PSNR and MSE of reconstructed image of both methods and it is found that new cipher has higher PSNR and less MSE compared to Genetic algorithm. Thus the image quality of this new cipher is good.

Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma [4] presented an analysis and comparison of various parameters of DES and AES encryption schemes. An image size of 128*128 (e.g. cameraman, pepper, aero, etc.,) is considered as plain (Original) image and DES and AES encryption and decryption is performed using MATLAB. In addition to the theoretical comparisons between DES and AES they have analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image and cipher image respectively for both the algorithms. The correlation coefficient can provide the quantitative measure on the randomness of the encrypted images for both the algorithms.

Manika Sharma, Rekha Saraswat [5] proposed a cryptographic technique for color images where they are using color error diffusion with XOR operation. The shares are developed using Random number. The key generated for decryption process is sent securely over the network using RSA algorithm. This approach produces less distorted image and the size of the decrypted images is same as the original image. In this paper, the assumption is that the original image is produced from the three channel images R, G, B. Hence the quality of the original image depends on the quality of the channel images. Here, a Visual Cryptography scheme is proposed in which the quality of the decrypted image is improved as Color Error diffusion technique is used. To add more security to the secret sharing of the image Invisible Digital Watermarking is used which protects the secret image from the hacker. For the decryption process a key is used which includes the Number of share required to decrypt the secret image and the envelop images which are used in the encryption process. The key is sent through the network using RSA algorithm which is a secure method of sending key over the network.

Mrs. Smita Desai, Chetan A. Mudholkar, Rohan Khade, Prashant Chilwant [6] proposed encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish designed to increase security and to improve performance. This algorithm will be used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms. The proposed algorithm is designed and realized using Visual basic. Here they took an image & obtained the matrix and pixels of the chosen image & then encrypted the image matrix using blowfish algorithm. The result shows the original image, encrypted image and the decrypted image. The text in the image hided using a specific key and image hidden with a data is encrypted and decrypted by a 32 bit iteration loop. Blowfish cannot be broken until an attacker tries 28r+1 combinations where r is the number of rounds. Hence if the number of rounds are been increased then the blowfish algorithm becomes stronger. Since Blowfish has not any known security weak points so far it can be considered as an excellent standard encryption algorithm. It takes much less time for processing than any other encryption techniques. Also all types of image sizes & format can be encrypted (.jpg,.bmp). By using this algorithm, lower correlation & higher entropy can also be achieved.

3. Proposed Work

The cryptography is divided into two main categories, the first and the most common category is called classical cryptosystems encryption algorithms (also called single-key or symmetric) which uses a single shared key to encrypt and decrypt a message. The most common algorithms within this category are called Data Encryption Standard AES, Triple DES (data encryption standard), RSA, Blowfish etc. In this system we implemented Byte Rotation Algorithm which gives higher quality result in parameters like encryption time and decryption time as compared to others.

In architecture diagram shows sender side fig 1A, in which the image file is divided into small number of blocks and BRA encryption technique applied on small block of data to get encrypted image. This encrypted image is decrypted using BRA decryption algorithm and combines the divided blocks into image. At receiver side fig 1B, we get decrypted image i.e. recovered image.

The BREA algorithm has the following features:

1. It is a Symmetric Key Block Cipher Algorithm.
2. Each block size is of 16 bytes.
3. Size of Key matrix is 16 bytes.
4. Values of Key matrix are randomly selected.
5. Byte-Rotation technique is used.

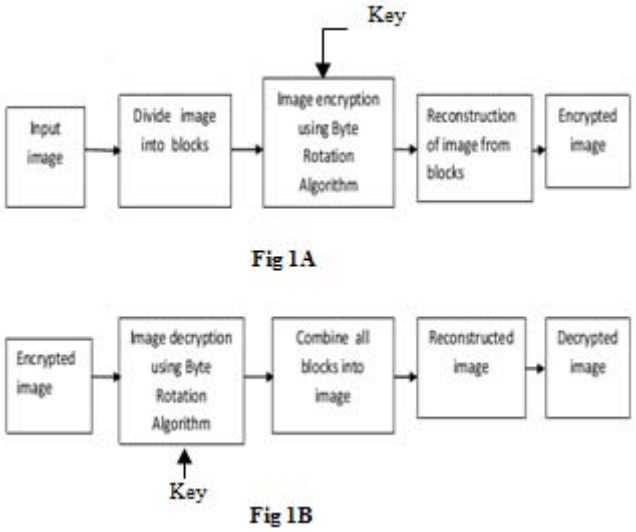


Figure 1: Block Diagram BRA

The steps of proposed Byte-Rotation Encryption Algorithm:

1. First stage is Image Encryption. An Image is selected i.e. Color or Gray.
2. Separate this image into three planes R(Red), G(Green), B(Blue) if it is color image.
3. Now for Red plane, select fixed block length of 16 byte from image pixels. Let that matrix be

$C_p =$

18	15	21	14
31	54	9	7
25	4	20	19
13	29	12	6

4. XOR matrix C_p with pixel value 255 such that,

$$C_{pr} = C_p \bmod 255$$

$C_{pr} =$

3	0	3	3
7	39	3	3
5	3	15	8
8	23	3	3

5. Then, Key matrix of size 16 bytes is randomly selected.

K_e = [k1, k2,....., k16]

Let the Key Matrix be

$K_e =$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

6. Addition of matrices C_{pr} and K_e

$C_{pk} = C_{pr} + K_e$

3	0	3	3
7	39	3	3
5	3	15	8
8	23	3	3

+

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The resultant matrix will be

$C_{pk} =$

4	2	6	7
12	45	10	11
14	13	26	20
21	37	18	19

7. Apply BREA algorithm.

7.1 Rotate matrix C_{pk} horizontally such that 1st row remains unchanged and rotate 2nd row << Right shift by one byte, 3rd row << Right shift by two byte and 4th row << Right shift by three byte. The resultant matrix will be

$C_h =$

4	2	6	7
11	12	45	10
26	20	14	13
37	18	19	21

7.2 Now the matrix is rotated vertically such that 1st coloumn remains unchanged, and rotate 2nd coloumn << Right shift by one byte, 3rd coloumn << Right shift by two byte and 4th coloumn<< Right shift by three byte.

$C_V =$

4	18	14	10
11	2	19	13
26	12	6	21
37	20	45	7

7.3 Again rotate the matrix horizontally such that 1st row remains unchanged, and rotate 2nd row<< Right shift by one byte, 3rd row<< Right shift by two byte and 4th row << Right shift by three byte.

$C_{hl} =$

4	18	14	10
13	11	2	19
6	21	26	12
20	45	7	37

7.4 The resultant matrix is encrypted matrix for Red plane.

Similarly calculate for Green and Blue plane. Combine all the three planes, we get matrix for encrypted image.

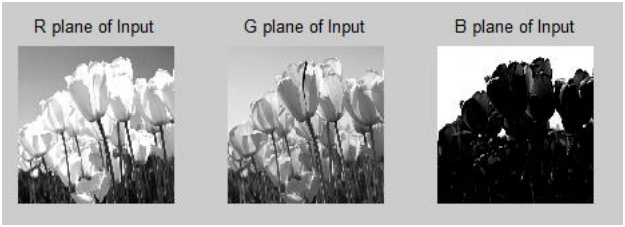
For Decryption, At the receiver end, the above stated BREA executed in reverse order to decrypt the encrypted image into original image.

4. Experimental Results

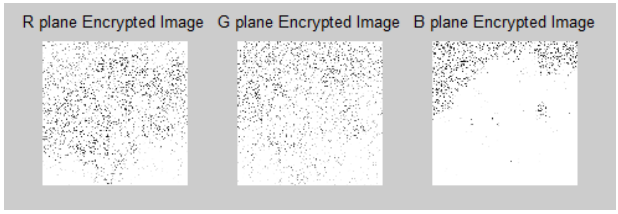
In this paper we have simulated the image processing part of Encryption and Decryption in MATLAB software.

4.1 Brea Encryption

Input image



Separation of Planes into R, G, B



Encryption of R, G, B planes

Encrypted Image

4.2 Brea Decryption

Decryption of R, G, B planes

Decrypted Image

Following table shows the execution time required for different types of images.

Table: Calculation of Execution Time for Different types of Images

Image No	Time Required for Encryption (sec)	Time Required for Decryption (sec)
Img1.jpeg	1.40276	1.40276
Img2.tiff	0.46094	0.46094
Img3.bmp	1.38562	1.38562
Img4.png	1.40370	1.40370

5. Conclusion and Future Work

A low latency for file encryption and decryption technique for secure transmission of data is discussed. This system gives the effective and efficient strategy of making most out of the advantage of Byte Rotation algorithm. The performance of the system enhances speed of encryption and decryption. Also the performance parameters such as PSNR, MSE and Normal Correlation are calculated. Thus the quality of the image after decryption is good. Thus the system is justified for its use in securing files.

In future, we can increase security by generating more random number of keys also we can increase the block size from 16 byte to 32 byte or 64 byte.

References

[1] Punam V. Maitri, Dattatray S. Waghole, Vivek S.Deshpande "Low latency for file encryption and decryption using Byte Rotation Algorithm", Proceedings of IEEE International conference on International Conference on Pervasive Computing, 2015.
[2] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra "Text and Image Encryption Decryption Using Advanced Encryption Standard" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May – June 2014.
[3] Rohit Kumar, Shekhar "Comparison of Genetic Algorithm Of Image Encryption with New Cipher Algorithm" International Journal of Emerging Trends in Engineering Research Volume 2, No.11, November 2014.
[4] Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma "Analysis and Comparison between AES and DES Cryptographic Algorithm" International Journal of

Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012.
[5] Manika Sharma, Rekha Saraswat "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 10, April 2013 Simple Visual Cryptographic technique is insecure.
[6] Mrs. Smita Desai, Chetan A. Mudholkar, Rohan Khade, Prashant Chilwant "Image Encryption and Decryption Using Blowfish Algorithm" International Conference on Emerging Trends in Technology, Science and Upcoming Research in Computer Science DAVIM, Faridabad, 25th April, 2015.
[7] Naveen Kumar S K, Sharath Kumar H S, Panduranga HT "Encryption Approach for Images using Bits Rotation Reversal and Extended Hill Cipher Techniques" International Journal of Computer Applications, Volume 59– No.16, December 2012.
[8] Pia Singh, Prof. Karamjeet Singh "Image Encryption and Decryption Using Blowfish Algorithm In MATLAB". International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
[9] Lini Abraham, Neenu Daniel "Secure Image Encryption Algorithms: A Review", International Journal of Scientific & Technology Research Volume 2, ISSUE 4, APRIL 2013.
[10] W. Stallings, Cryptography and Network Security: Principles and Practices, Prentice Hall, 1999.
[11] Atul Kahate, Cryptography and Network Security, 2nd Ed., Tata McGraw hill, 2009.

Author Profile

Kalyani V. Gulhane is a student of Master of Engineering in Electronics and Telecommunication at P. R. Pote College of Engineering Amravati, and graduated from G.H. Raisoni College of Engineering, Amravati, India.

Prof. G.D. Dalvi received his M. Tech degree from SSCOE & T, Durg, India. He is a Principal of P. R. Pote College of Polytechnic, Amravati in department of Electronics and Telecommunication Engineering, Amravati, India.