ISSN 2277-3061

The New Image Encryption and Decryption Using Quasi Group

Ankit Agarwal[1], Amit Varma[2], Durgesh Kumar[3]

[1, 2, 3]GNIOT Greater Noida, Uttar Pradesh, India

ABSTRACT

Multimedia communication is the new age of communication. The image communication is one of most popular multimedia communication. This type of communication always faces problem of security. The communication breaching rate is rising very rapidly. The image privacy is facing a bigger threat. In this paper, we represent a new approach for image encryption and decryption by using pixel shifting and based on Quasigroup(Latin Square) without performing translation, through which there is low computational requirement. In this we apply new type of encryption and decryption here we used Quasigroup as a key. Image pixel reshuffling is done randomly and non-repeated manner.

KEYWORDS:

Encryption; Decryption; Latin Square; Quasigroup.

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATION JOURNAL OF COMPUTERS AND TECHNOLOGY

Vol. 13, No. 9

editorijctonline@gmail.com

www.ijctonline.com, www.cirworld.com

INTRODUCTION

Multimedia communication through media devices such as phones or computers may include text, audio, music, images, animation and video. [4] It can be categorized into the following types:

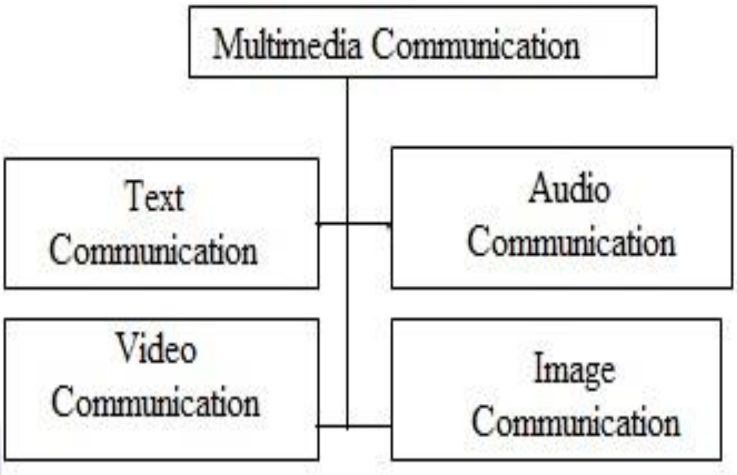


Figure:1

Text Communication

Text communication is one of the most common categories of multimedia communication. Text communication involves many areas of Internet usage such as browsing websites, communication through emails and instant messaging services. It is also the oldest form of multimedia communication, as the computers used to display text only. [5]

Audio Communication

Audio communication involves receiving a message through an audio format, such as listening to an online radio station or playing a music file. Audio communication often combines with other forms of multimedia communication. A slideshow, for example, can feature text, images and audio together. [5]

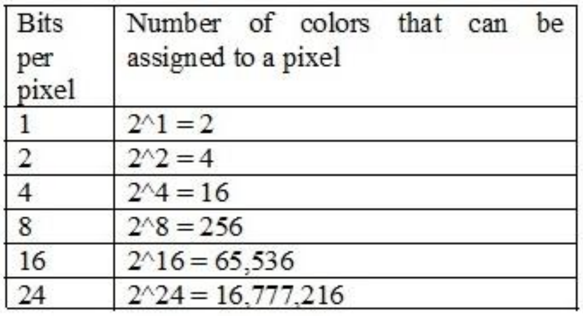
Video Communication

Video communication is a form of multimedia communication through video. It is a new type of communication which needs good internet speed. [5]

Image Communication

Image communication is different from above mentioned types. It is a legitimate form of multimedia communication that many of the users enjoy in their daily lives. Examples include browsing an online photo album, opening and viewing images attached to an email or those connected with stories on news websites. Sending an image online is known as image communication. [5]

The image is the combination of the pixels. A pixel is a physical point in a raster image, or the smallest addressable element in an 'all points addressable display device'; so it is the smallest controllable element of a picture represented on the screen. The number of distinct colours that can be represented by a pixel depends on the number of bits per pixel (bpp).



Bits per pixel	Number of colors that can be assigned to a pixel
1	2^1 = 2
2	2^2 = 4
4	2^4 = 16
8	2^8 = 256
16	2^16 = 65,536
24	2^24 = 16,777,216

Figure:2

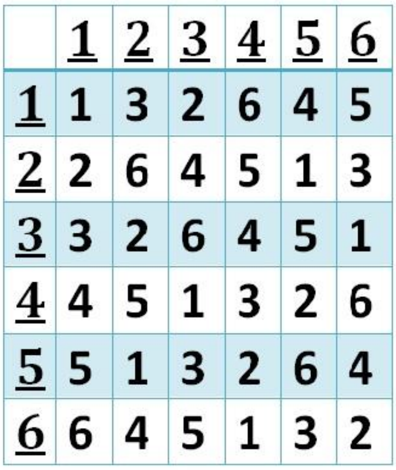
CRYPTOGRAPHY

Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. That's why it is becoming crucial to ensure the information security.

Cryptography is the most powerful tool for protecting information which includes data confidentiality, data integrity, and user authentication. Cryptography has a specific role in protecting confidential communication from unauthorized access. The algorithms used for cryptography applications are classified into two types: Asymmetric methods or public key cryptography and Symmetric methods or Symmetric key cryptography.

In this paper, cryptography algorithm is based on symmetric keys to increase security and prevent unauthorized access to the contents of encrypted images. The symmetric key used here is Special Latin square known as quasi group.

A quasigroup of n numbers is an nxn matrix in which any number occurs only once in each row and column. [1]Let's represent every entry with Vij, where Vij is unique in the i'th row and the j'th column as shown in the figure



	1	2	3	4	5	6
1	1	3	2	6	4	5
2	2	6	4	5	1	3
3	3	2	6	4	5	1
4	4	5	1	3	2	6
5	5	1	3	2	6	4
6	6	4	5	1	3	2

Figure:3

Quasi group states that, for each a and b, there exist unique elements x and y such that:

$$a * x = b \text{ and } y * a = b$$

According to the second principle of Auguste Kerckhoffs, Cryptography algorithm must not include any secret and hidden point. In fact the only secret point is the secret key and to stop decoding our data of the encrypted file through hacking the keys, there is no limitation for the number of keys to construct the cryptography [2, 3]

PROPOSED FRAMEWORK

Pixel Shuffling

Step 1: Select a main image (mxn) and a sample image (axb).

Step 2: Break the main image pixel into small block size of p x q such that p will be greater than 8 and smaller than 32(8<p<32) and q will be greater than 8 and smaller than 32 (8<q<32) and the number of blocks be N where N should be greater than 2.(for low computation requirement).

Step 3: Now form a new image and the size of image will be (m+a, n+b) and divide that image into N block of size p'x q' where p'>p and q'>q. Also form the record file. Give the number of each block from left to right and top to bottom.

Step 4: Now randomly pick a block from main image and as well as from a new image and pick the first pixel of the main image block and put randomly into new image block and record the address of the location as well as previous location of the block into the record file.

Step 5: Now put next pixel of that block into that new image block randomly and do that until all pixels are not placed into that new image block. Record the address of pixel into new image block location and the previous location pixel into record file. (As we know that all the blocks are of same length and size and the number of pixels are same in each block so we only record the location pixel of one block and the address of block position in a new image)

Step 6(a): Now pick another block of main image and make sure that every time we pick non-repeated and a random block.

- *Note the number of block and put the pixel into new image in randomly selected non-repeated block in a similar way used in previous block. The address of pixel position will be different but the position of pixel in a block will be same of previous block.*

Step 6(b): Do the above step for all blocks.

Step 7: Now, there will be an empty pixel positions in the new image. Fill these pixels by putting sample image pixels randomly.

Step 8: There formed will be new image.

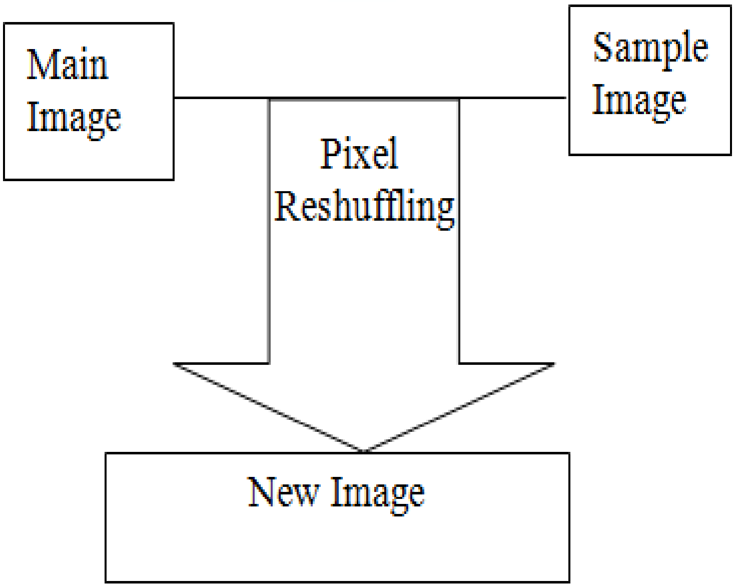


Figure:4

ENCRYPTION

In previous step, we reshuffled the pixel location and imposed the left pixel position by sample image pixel into the new image and we got a distorted image. Now we encrypt that image by using quasi group as key.

The steps of encryptions are:

Step 1: Convert the new image file into image byte array.

Step 2: Take input the quasi group of m*m (recommended 256*256). Here we use quasi group as a key and convert the quasi group into quasi byte array and divide it into m blocks

Step 3: Break that image byte array into m blocks.[8]

Step 4: Now perform the XNOR operation between the quasi group byte array and image byte array.

Here take one block of image byte array and perform the XNOR operation with each block of quasi byte array .

Step 5: Repeat the above step until all block of image byte array is encrypted.

Step 6: Now convert the encrypted byte array into logical file.

Step 7: Send the logical file through communication channel (unsecure channel) and record file with secured channel.

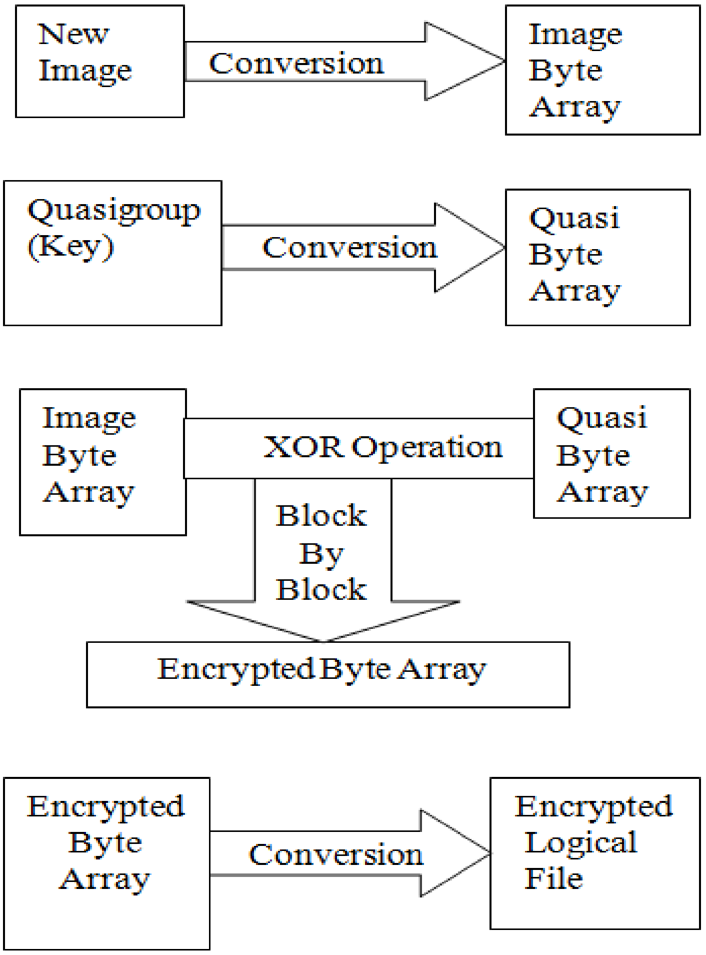


Figure:5

DECRYPTION

Decryption process is used at the receiver's end in order to get the required image from the received logical file.

Following are the decryption steps:

Step1: Convert the logical file into byte array.

Step 2: Take the key quasi group (m*m) that we used at the time of encryption. Convert that quasi group into byte array and divide it into m blocks.

Step 3: Now convert byte array into m blocks.[8]

Step 4: Now perform XNOR operation between the image byte array and quasi byte array block.

Here, take a block of image byte array and perform the XNOR operation with each block of quasi byte array [7]

Step 5: Repeat the above step until all blocks of image byte array are operated.

Step 6: Now, convert image byte array into logical file and start extracting the pixel of blocks from logical file by using the record file that we received from secure channel one by one.(As we record the address of pixel in the file we can get that very easily from there.)

Step 7: After completing the above step we will receive the required image.

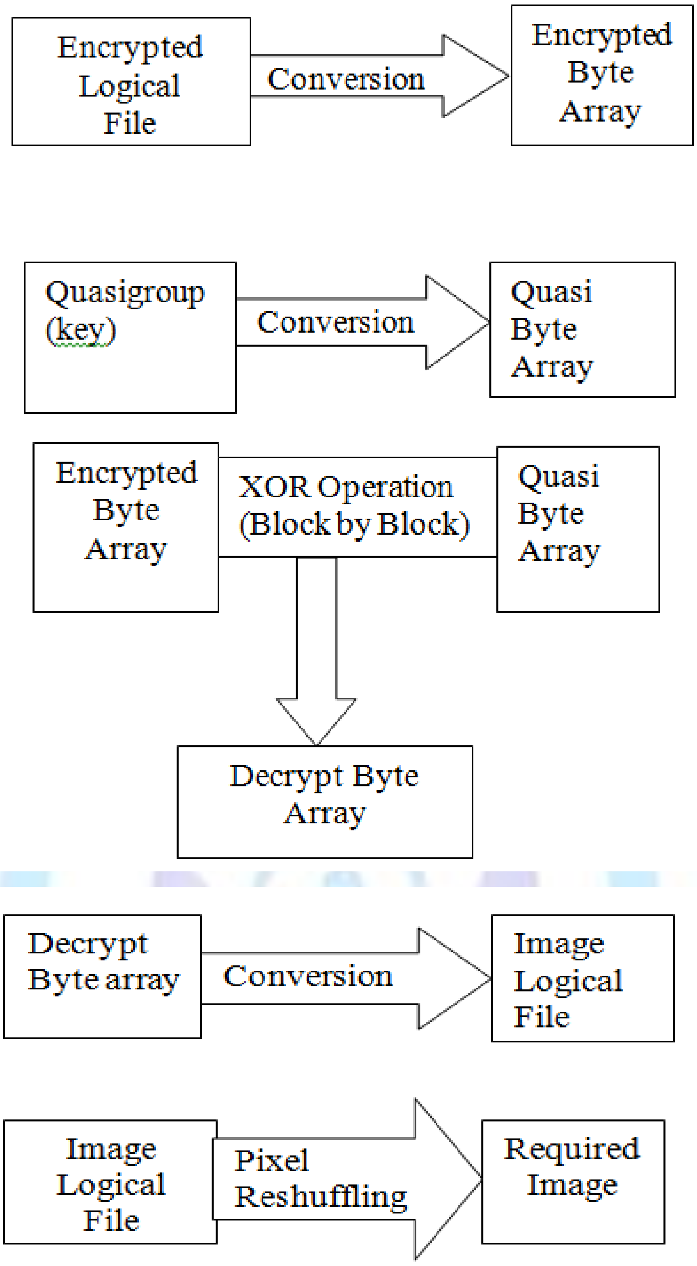


Figure:6

CONCLUSION

The Cryptography is a technique to secure the data and to preserve its authenticity and confidentiality. Cryptography make the data camouflage. Cryptography has been divided into two parts one is known as symmetric cryptography and another one is known as asymmetric cryptography. In this paper, we have shown a new algorithm of image symmetric key encryption by using the quasi group as a key. As described, it is a two-step process. In the first step, we have formed a new image by shifting the pixels from one image to another in a random order and storing the positions into record file. Here, we used a secure channel to send the record file to the user's end. The size of the random file will always be less than the image file sent through unsecure channel. The second step in our process is an encryption process where we have used a mathematical group known as quasi group as a key and convert it into byte array. During encryption and decryption techniques, we have used XOR operation between the file and quasi group. Since the used quasi group is same in both steps, so it is Symmetric Key Cryptography. We have used the quasi group to reduce the brute attack.

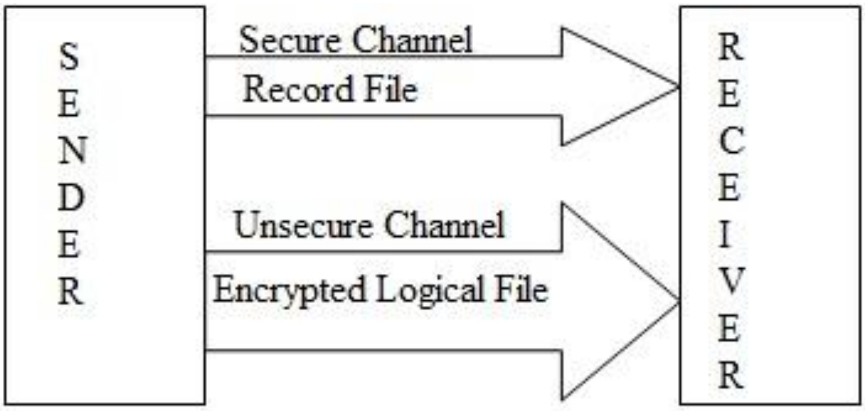


Figure:7

REFERENCES

[1] Ask (2014) “What is Multimedia Communication?”[Online].Available: http://www.ask.com/question/what-is-multimedia-communication.

[2] D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati Garg “An Innovative Approach to Enhance the Security of Data Encryption Scheme” International Journal of Computer Theory and Engineering, Vol. 2, No. 3, June, 2010 (1793-8201) p.-380-383.

[3] “eHow Types of Multimedia Communication” [Online].Available: http://www.ehow.com/info_12142877_types-multimedia-communication.html

[4] Kerckhoffs, A., la cryptographie militaire Journal des sciences militaires, 1883. IX: p. 161-191.

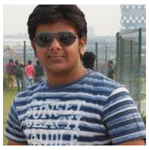
[5] Kerckhoffs, A., la cryptographie militaire. Journal des sciences militaires, 1883. IX: p. 5-83.

[6] Quasigroups in cryptology, V.A. Shcherbacov computer Science Journal of Moldova, vol.17, no.2 (50), 2009.

[7] Soltani, M., “*A NEW ROBUST CRYPTOGRAPHY ALGORITHM BASED ON SYMMETRIC KEY TO PREVENT UNAUTHORIZED ACCESS TO CONTENTS OF ENCRYPTED FILES*”. IJCSI International Journal of Computer Science Issues, 2013. 10(2): p. 444-452.

[8] Wikipedia “Pixel” [Online].Available: http://en.wikipedia.org/wiki/Pixel.

Authors' Biography with Photo



Ankit Agarwal was born in Ghaziabad,India in August 1992. He is currently pursuing his B.Tech. degree in the department of computer engineering at Greater Noida Institute of Technology which is affiliated to Uttar Pradesh Technical University. His research interests include image processing,cryptography ,data compression,design analysis and algorithm.

Amit Varma was born in Mainpuri,India in July1993. He is currently pursuing his B.Tech. degree in the department of computer engineering at Greater Noida Institute of Technology which is affiliated to Uttar Pradesh Technical University. His research interests include cryptography,design analysis of algorithm and soft computing.

Durgesh Kumar was born in Etawah,India in July1988. He passed his B.Tech. degree in the department of computer engineering at G.L.A Mathura which is affiliated to Uttar Pradesh Technical University.He also passed his M.Tech degree from Galgotia college of engineering Greater Noida.His research interests include cryptography and Networking.