IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 9, September 2020

DOI 10.17148/IARJSET.2020.7904

# Progressive Image Encryption Using Cyclic Group

**D.Mohana[1], S.Nandhini[2]**

Associate Professor, Computer Science and Engineering, Coimbatore Institute of Technology, Coimbatore, India[1]

Student, Computer Science and Engineering, Coimbatore Institute of Technology, Coimbatore, India[2]

**Abstract:** Safety becomes an important problem for image communication and storage due to the exponential growth of digital communication and multimedia applications. Encryption is one of the ways of ensuring high-security photos used in many areas, such as medical research, military, etc.; Modern cryptography provides important techniques for data securing and multimedia data security. Recent years have seen the rapid advancement of encryption technologies, and many image encryption techniques have been employed to secure sensitive image data from unauthorised access. To ensure a higher degree of protection for images transmitted over the network, a non-chaos-based encryption technique has been introduced. A progression of the cyclic group is improved where the pixel dependent protection is used. A permutation-based technique is suggested with an iterative method in which the step of uncertainty and diffusion occurred. This allows for better security compared to the usual encryption methods focused on chaos. The bit shifting approach caused the pixel array to transform with the changes in the image's bit level value. It is possible to solve a network security-based attack and reduce third-party access.

**Keywords:** Image Encryption, Non-Chaotic Method, Permutation, Generator of Cyclic Group, Multiplicative Cyclic Group.

## I. INTRODUCTION

Network protection is the process of taking proactive measures to avoid unauthorized entry, misuse, failure, alteration, destruction or inappropriate disclosure of the underlying networking infrastructure. There are many individuals who are trying to damage our Internet-connected devices, invade our privacy, and make Internet services impossible. Because of the frequency and variety of current attacks, as well as the possibility of new and more disruptive future attacks, network security has become a core theme in cyber security. Implementation of network security measures enables devices, users, and programmers to conduct their essential functions within a safe environment.

### 1.1 SCOPE OF THE PROJECT

Many of us interact in cyber space in today's rapid growth of digital communication and electronic data exchange, without caring about the security of the same. The need for most of our private information and secrets to be shared in cyberspace. Digital image/video protection has become increasingly relevant in applications such as pay-per-view TV, confidential video conferencing, medical imaging and industrial or military imaging systems, online transactions, passwords, legal digital signatures, etc., in today's highly computerised and interconnected world. These applications need to track image access, and provide the means to verify image integrity. In certain cases, such information leakage seriously invades personal privacy, such as: the malicious spread of photographs in personal online albums or medical diagnostic photos of patients, and moreover, it can cause countless losses for a business or country, e.g. a hidden product design for a business or a governmental scanned document. To achieve secure image transmission over the internet, the encryption of an image is carried out. The encryption mechanism is commonly used in many areas such as image / video transmission, medical image transmission over the vulnerable network which can provide protection from unauthorised access. The encryption also has its applicability in telemedicine and military communication. Encryption is the process through which plain information can be translated into encrypted or secured data and can only be interpreted through decrypting it. The inverse encryption method is known as decryption, which uses an encryption key to decrypt the original information.

## II. PRESENT FRAMEWORKS

Chaotic maps are generally continuous, and can be discredited in encryption schemes as necessary. There are some well-known one-dimensional and multi-dimensional chaotic maps such as logistic map (1-D), tent map (1-D), cat map of Arnold (2-D), map of Lorenz (3-D) etc. Researchers have suggested improvements in chaotic maps or hybridization of more than one chaotic map to build new chaotic maps with improved properties in order to improve the chaotic properties. Thus, two types of pixel division are used to place the chaotic maps. For a chaotic map implementation, the pixels are

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 9, September 2020

DOI 10.17148/IARJSET.2020.7904

split like odd pixels and even pixels. A probabilistic dependent cipher with 2D image encryption and security is introduced. This paper explains how an even-odd encryption like that is. The pixel division technique adds the even and odd number of pixels where the image can be split and add as multiple shares to the distributed storage and the shares get encrypted. Thus, the method of implementation offers resilience over the statistical attacks. The encryption placed as the encryption system based on AES, where the key-based enhancement is made. Thus, the encryption reduces security threats on the server over third party threats. The accuracy of the encryption and the security against access and attacks from third parties is high.

## III. PROPOSED SYSTEM AND DESIGN

Non chaos based cyclic group image encryption is proposed. XOR algorithm is enhanced for the encryption and decryption of an image which is to be protected from the third-party access. The correlation of the image is changed by row level and column level permutation. Then, the BLP and BLT is processed to change the intensity value or to add any noise.

### 3.1 ADVANTAGES OF PROPOSED SYSTEM OVER EXISTING SYSTEM

- Differential attacks can be resolved by the framework proposed.
- Compared with the current techniques, the implementation of the proposed approach is quite strong.
- The image is restored without distortion;
- This allows the picture to be safely protected from unknown attacks.

### 3.2 ARCHITECTURE

A system architecture or system architecture is the conceptual model which defines a system's structure, behavior, and more views. A description of architecture is a systematic description and representation of a system, structured in a manner that facilitates thinking about the system's structures and behaviors. System architects or solution architects are the people who know what components to use for the particular use case, do the best trade-offs in the overall system with knowledge of the bottlenecks. Typically, in system architecture, solution architects with more years of experience appear to be successful because system design is an open-ended problem, there is no right solution. It's just tests with the right trade-offs made with trial and error.

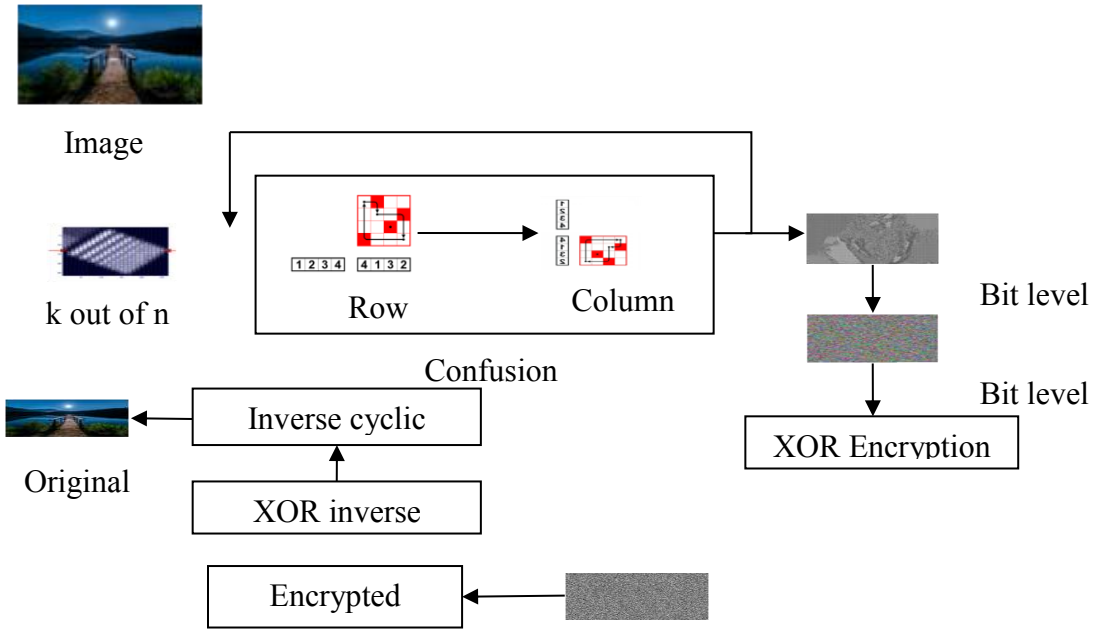


Fig.1 Block Diagram of the System

### 3.3 MODULES

### A. MODULE 1: IMAGE ACQUISITION

Pick the hidden image which should be uploaded. The picture can be any of the formats that support it. The different support formats are JPEG, PNG & BMP.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 9, September 2020

DOI 10.17148/IARJSET.2020.7904

### B. MODULE 2: PIXEL SPLIT

The pixel is defined by the dimensional height and width of the image. In

$$p = h*w$$

To get hidden shares, progressive visual cryptography is implemented from k out of n area based.The multiple images in the image move through (k, n) the number of pixels.

$$K = n$$

This method assists in pixeling the values in bit stage.This contributes to row and column permutation.

### C. MODULE 3 : CONFUSION PHASE

The procedure takes place in two processes in the uncertainty step module:

- Row level permutation
- Column level permutation

This module is used to adjust row wise and column wise pixel locations. The change in pixel permutation will make it a high level operation.

### D. MODULE 4: DIFFUSION PHASE

In the two implementation phases, the diffusion step is carried out. Within the picture, the stage of disarray allows major changes, so it is difficult to discern. But, both pictures have the same histogram from which data may be leaked from the initial image. Dissemination stage adjusts the appreciation of the pixels using BLP and BLT. These activities deliver vigorous and safer execution.

- Bit Level Permutation
- Bit Level Transformation

### E. MODULE 5: XOR ENCRYPTION

A simple binary operation that is used in encryption techniques is an exclusive OR operation. Using a hidden key the image will be encrypted after the image processing functions get over the image. In the 8x8 block transformation system, the encryption process is enforced.

- Original Image : 1110 1000 0011
- Secret key : 0010 1010 0000
- Encrypted (XOR) : 1100 0010 0011

### F. MODULE 6: XOR DECRYPTION

After encryption of the image the authenticated user requires to get the original image. Image substitution method and the cyclic group reversal property.

- Encrypted Image : 1100 0010 0011
- Secret key : 0010 1010 0000
- Decryption : 0001 0111 1100
- Inverse Cyclic Group : 1110 1000 0011

## IV. SNAPSHOTS OF THE DESIGN

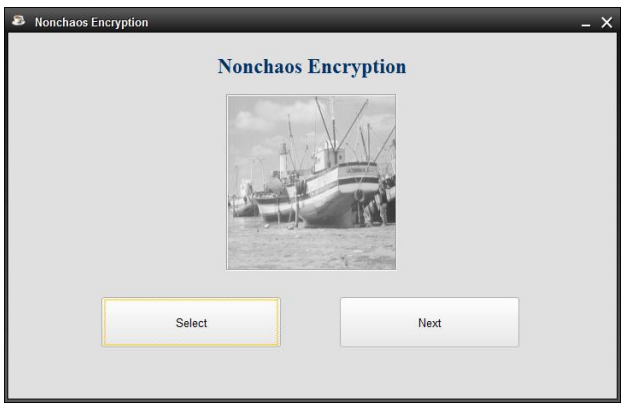


Fig 2. Input Image

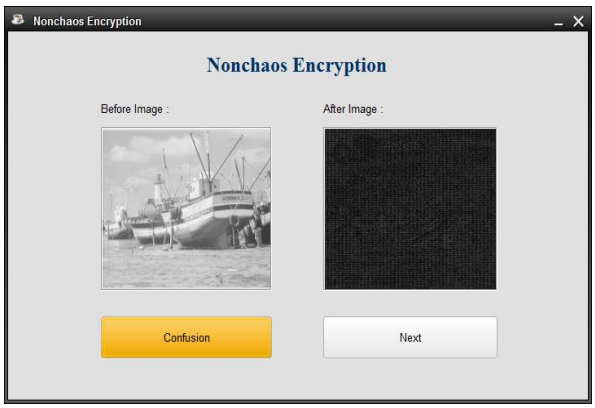


Fig 3. Confusion Phase

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 9, September 2020

DOI 10.17148/IARJSET.2020.7904


Fig 4. Diffusion Phase-(BLP&BLT)


Fig 5. Encrypted Image

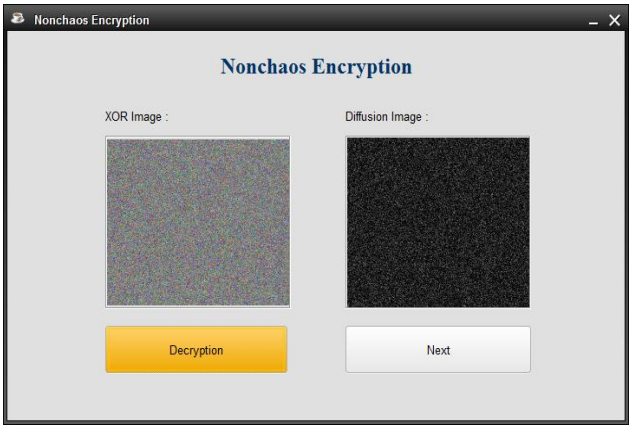


Fig 6. Inverse XOR & Reverse Diffusion

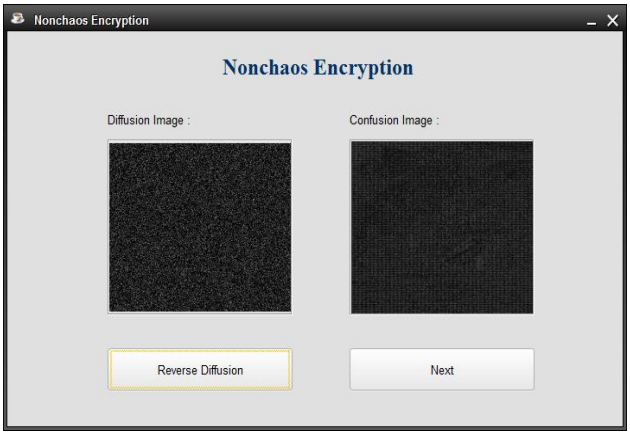


Fig 7. Reverse Confusion


Fig 8. Original Image

## V. CONCLUSION AND FUTURE WORK

The XOR cipher is an important instrument for encrypting an image. If an image is encrypted using the XOR cipher, then the randomness of the pixels of the original image increases. If randomness is greater, we can assume that the picture is safer. By studying the histogram, horizontal and vertical correlation, it can be inferred that the randomness increases in their ciphered images after scrambling various images, indicating that the ciphered images are more reliable that decryption is not possible. So, we may infer that the protection of a picture is improved by this procedure.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 9, September 2020

DOI 10.17148/IARJSET.2020.7904

Future work focuses on the technique of S-box substitution to allow an empirical study of the distinct image encryption. The S-box is referred to as a two-dimensional substitution table where multiplicative inverse and affine transformation is applied.

## REFERENCES

[1]. Shyamalendu Kandar, Dhaibat Chaudhuri, Apurbaa Bhattacharjee, Bibhas Chandra Dhara "Image encryption using sequence generated by cyclic group", 2019 Journal of Information Security and Applications", pp: 117-129.
[2]. Deepak Kumar Singh, Dr. Kuldeep Tomar "A Robust Color Image Encryption Algorithm in Dual Domain using Chaotic Map", 2018 International Conference on Inventive Communication and Computational Technologies, pp: 931-935.
[3]. Sakshi Dhall, Saibal K. Pal, Kapil Sharma "A chaos-based probabilistic block cipher for image encryption", 2018 Journal of King Saud University – Computer and Information Sciences, pp:1-11.
[4]. Tatsuya Chuman, Warit Sirichotedumrong and Hitoshi Kiya "Encryption-then-Compression Systems using Grayscale-based Image Encryption for JPEG Images", 2018 IEEE Transactions on Information Forensics and Security, pp;1-11.
[5]. Avinash Ray, Anjali Potnis, Prashant Dwivedy, Shahbaz Soofi, Uday Bhade "Comparative Study of AES, RSA, Genetic, Affine Transform with XOR Operation, And Watermarking for Image Encryption", October 2017 International conference on Recent Innovations is Signal Processing and Embedded Systems, pp: 27-29.
[6]. Long Bao, Shuang Yi and Yicong Zhou "Combination of sharing matrix and image encryption for lossless (k, n)-secret image sharing", 2017 IEEE Transactions on Image Processing, pp: 1-14.
[7]. Peiya Li and Kwok-Tung Lo **"**A Content-Adaptive Joint Image Compression and Encryption Scheme", 2017 IEEE Transactions on Multimedia, pp: 1-13.
[8]. Sagar Mal Nitharwal, Harsh Kumar Verma "A Boolean-based multi-secret image sharing scheme using bit-reversal", 2017 International Conference on Intelligent Communication and Computational Techniques, pp:114-118.
[9]. Wen Chen "Optical Multiple-Image Encryption Using Three-Dimensional Space", 2016 IEEE Photonics Journal.