# Image Cryptography using Nearest Prime Pixels

**[1]Mrs. Ayesha Razia Anha [2] Dr. T. Bhaskara Reddy**
[1]Research Scholar, Department of Computer Science & Technology
[2]Professor, Research Scholar, Department of Computer Science & Technology
raziaanha@gmail.com, bhaskarareddy.sku@gmail.com

-----ABSTRACT-----

**Protecting the data in a safe and secure way which does not impede the access of an authorized authority is an immensely difficult and very interesting research problem. image cryptography is a special type of encryption technique to obscure image-based secret information which can be decrypted by Human Visual System. Communication is the process of transmitting information from source to destination. The exchanging information should not be stolen by unauthorized parties like hackers while sending or receiving via channel. To avoid this stealing of the information visual cryptography techniques are used. This paper proposes a novel method for key generation by using nearest prime pixels. Further 2's complement and logical operations are performed to generate decrypted image. The final decrypted image is generated by representing pixels in matrix form and data is retrieved in column wise.**

Keywords—**Image Cryptography; Nearest prime pixels; 2's complement; XOR operation;**

Date of Submission: Sep 12, 2016 Date of Acceptance: Sep 30, 2016

## I. INTRODUCTION

Image cryptography [1]is a cryptographic technique where visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the human visual system without aid of computers. Cryptography is used to constrain the potential sender and/or receivers of a message. Cryptography is based on secrets called keys. The sender can encode its message so that it can only decode with suitable key.

Image is sensed by human. Pixel is the smallest unit constructing a digital image. Cipher is the algorithm that is used to transform plaintext into cipher text, this method is called encryption or enciphers, in other words, it's a mechanism of converting readable and understandable data into "meaningless" data, and it is represented as follows:

$$C = E_{(k)}(P) \qquad (1)$$

Where E(k) is the encryption algorithm using key k,C is a cipher text and P is a plain text. Symmetric and asymmetric are two types of encryption algorithm.

The opposite of cipher mechanism is called decipher that is the algorithm which recovers the cipher text, this is called decryption, in other words, it's a mechanism of converting "meaningless" data into readable data, and it is represented as follows:

$$P = D_{(k^{-1})}(C) \qquad (2)$$

Where D (k-1) is the decryption algorithm using key k.

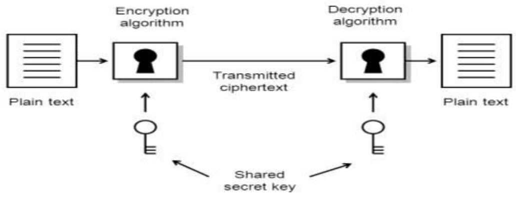


**Fig 1.** Conventional Encryption Model

Security services:

Here are some of the services that are provided by the security.

- Confidentiality(privacy)
- Authentication(who created or sent the data)
- Data integrity(has not been altered)
- Non-repudiation(the order is final)
- Access control(prevent misuse of resources)
- Availability (permanence, non-erasure).

If we are protecting confidential information then cryptography is provide high level of privacy of individuals and group.

In image cryptography scheme an image is divided into n number of shares such that minimum k number of shares is sufficient to reconstruct the image. The division is done by Random Number generator. There are a number of cryptographic primitives-basic building blocks, such as block ciphers, stream ciphers and hash functions. Cryptography has been used for millennia to safeguard military and diplomatic communications. Data encryption standard adopted by the National institute of standards is the most commonly used symmetric encryption algorithm. Black-box transformations are some of the transformations that are hidden in the algorithm.

## II. HISTORY

Image cryptography was originally invented and pioneered by Moni Naor and Adi Shamir in 1994 at the Eurocrypt conference. Image cryptography is "a new type of cryptographic scheme, which can be decode concealed images without any cryptographic computation". As the name suggests, image cryptography is related to images. Naor and Shamir's initial implementation assumes that the image or message is a collection of black and white pixels, each pixel is handled individually and it should be noted that the white pixel represents the transparent colour. Image cryptography mechanism is very secure and very easily implemented. This is another advantage of image cryptography over the other popular conditionally secure cryptographic schemes. An electronic secret can be shared directly, alternatively the secrets can be printed out onto transparencies and superimposed, revealing the secret. The piece of secret is known as share. The secret can only be reconstructed when a sufficient number of shares are combined together. While these shares are separate, no information about the secret can be accessed. That is, the shares are completely useless while they are separated. There are many types algorithms which will included in image cryptography with different concepts and techniques to enhance the security.

## III. PROPOSED WORK

The proposed work generates a 8-bit random sequence for key generation. Key[2] is obtained by performing subtraction between digital values and its nearest prime pixel values. Several stages are involved in encryption and decryption.

### *A. Key Generation*

The Each pixel of image converted into pixels. Further find nearest prime of it. For key generation find the difference between nearest prime pixel and for each pixel of image. Consider the difference value as key, it is continued for each and every pixel of image.

**Key generation algorithm steps**:-

Step1: Initially, the given image is converted into its equivalent digital pixels.
Step2: Find nearest prime pixels for each pixel of image.
Step3: The key values are obtained from finding difference between pixel values and nearest prime pixel values.
Step4: Perform 2's complement for generated pixels.

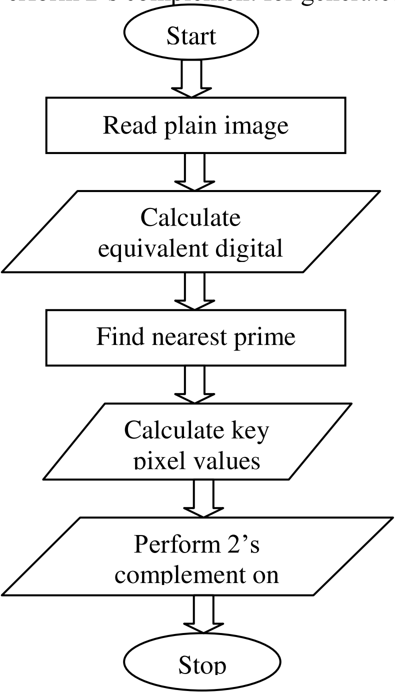

Start
Read plain image
Calculate equivalent digital
Find nearest prime
Calculate key pixel values
Perform 2's complement on
Stop

**Fig 2.** Flow chart showing key generation process

Example for key generation:

Sample pixel values are :
78 69 84 87 79 82 75 83 69 67 85 82 73 84 89
Nearest prime pixel values are:
79 71 89 89 83 83 79 89 71 71 89 83 79 89 97

Key values are:
1 2 5 2 4 1 4 6 2 4 4 1 6 5 8

**Table 1.** Key generation process

| Key Value | Binary code | 2's complement |
|---|---|---|
| 1 | 00000001 | 11111111 |
| 2 | 00000010 | 11111110 |
| 5 | 00000101 | 11111011 |
| 2 | 00000010 | 11111110 |
| 4 | 00000100 | 11111100 |
| 1 | 00000001 | 11111111 |
| 4 | 00000100 | 11111100 |
| 6 | 00000110 | 11111010 |
| 2 | 00000010 | 11111110 |
| 4 | 00000100 | 11111100 |
| 4 | 00000100 | 11111100 |
| 1 | 00000001 | 11111111 |
| 6 | 00000110 | 11111010 |
| 5 | 00000101 | 11111011 |
| 8 | 00001000 | 11111000 |

### *B. Encryption [4]algorithm*

Round1: perform XOR operation between nearest prime pixel and key.
Round2: reverse the result of round1.
Round3: store it in matrix form (column wise).
Round4: retrieve pixels from rows of each n*4 matrix. Find equivalent pixel values and considered to be as final decrypted image.

Round 1:

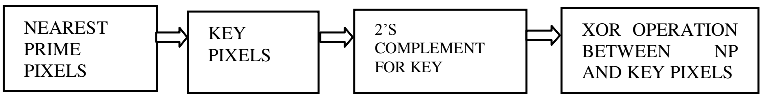


**Fig 3.** Steps involved in round 1

Round 2:

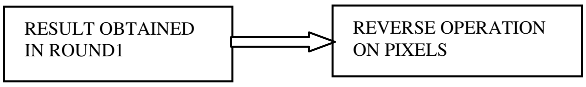


**Fig 4.** Steps involved in round 2

Round 3:

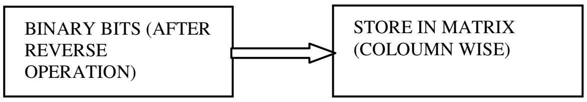

BINARY BITS (AFTER REVERSE OPERATION)
STORE IN MATRIX (COLOUMN WISE)

**Fig 5.** Steps involved in round 3

Round 4:

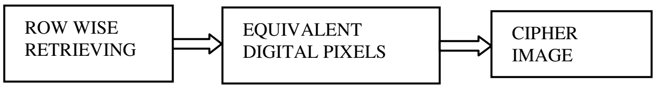


**Fig 6.** Steps involved in round 4

### *C. Decryption algorithm*

Round 1: Rearrange the decrypted image information in the form of matrix by finding their binary equivalents.
Round 2: Retrieve row wise binary pixels and reverse them.
Round 3: Reversed pixels are XOR with key to find nearest prime pixel values.
Round 4: Find the original image by subtracting with key value from nearest prime pixel value.
Round 1:

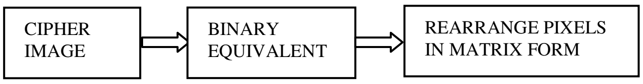


**Fig 7.** Steps involved in round 1

Round 2:

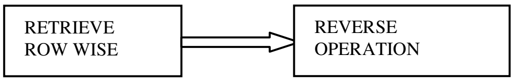


**Fig 8.** Steps involved in round 2

Round 3:

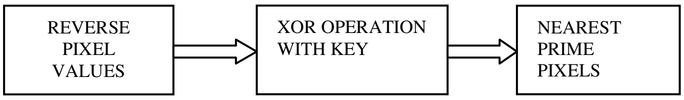


**Fig 9.** Steps involved in round 3

Round 4:

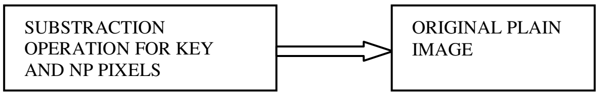
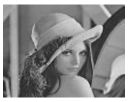
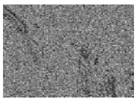


**Fig 10.** Steps involved in round 4

## RESULTS



a) Plain Image



b) Cipher Image

c) Decrypted Image

## IV.ADVANTAGES

- Nearest prime pixels technique is used for the key generation.
- Mixed column and row wise retrieval process is extended for image pixels which is one of the advantages added in this paper.
- It is applicable for images.

## CONCLUSION

Image cryptography [5,6] is playing vital role in current trends. This paper focusing on novel key generation using nearest prime pixels. Further different complementary and logical functions are used to improve the secrecy. Finally cipher image is generated with column wise retrieving. This work may be extended with genetic operators and genetic algorithms.

## REFERENCES

[1] S. Kiran, R. Pradeep Kumar Reddy, "Multi-Stage Encryption using Seeded SDES" International Journal of Advanced Networking and Applications Volume: 07 Issue: 02 Pages: 2694-2699 (2015) ISSN: 0975- 0290.

[2] B.Bazith Mohammed, "automatic key generation Of Caesar cipher", international journal of Engineering trends and technology (IJETT), vol.6, no.6, pp.337-339, dec.2013.

[3] S.G.Srikantaswamy and Dr.H.D.phaneendra,"A Cipher design using the combined effect of arithmetic And logic operations with substitutions and Transposition techniques", International Journal of Computer Applications (0975-8887), vol.29, no.8, pp.34-36.

[4] A. Sinha and K. Singh, "Image encrypt ion by using fractional Fourier transform and Jigsaw transform in image bit planes", Source: optical engineering, spie-int society optical engineering, vol. 44, no. 5, (2005), pp. 15-18.

[5] N. Taneja, B. Raman and I. Gupta, "Combinational domain encryption for still visual data", Journal of Multimedia Tools and Applications, DOI 10.1007/s11042-011-0775-4, (2011).

[6] A. Gautam, M. Panwar and P. R. Gupta, "A New Image Encryption Approach Using Block Based Transformation Algorithm", International Journal Of Advanced Engineering Sciences and Technologies, IJAEST, (2011).