PES University, Bangalore

(Established under Karnataka Act No. 16 of 2013)

APRIL 2022: IN SEMESTER ASSESSMENT (ISA) B.TECH. IV SEMESTER

UE20MA251- LINEAR ALGEBRA

Project / Seminar

Session: Jan-May 2022

Branch : Computer Science and Engineering

Semester & Section : Semester IV Section H

Sl No.	Name of the Student	SRN	Marks Allotted (Out of 10)
1.	Sutejas K	PES1UG20CS451	
2.	Sushanth M Nair	PES1UG20CS450	
3.	Sriram R	PES1UG20CS435	
4.	Swapnil S Nair	PES1UG20CS452	

Name of the Course Instructor :**Prof. Jyothi R.**

Signature of the Course Instructor

(with Date) : ______________________________

A New Chaotic Encryption Scheme Based on Enigma Machine

A report by Sriram Radhakrishna (PES1UG20CS435)

Table of Contents

1. Title page
2. Table of contents
3. Abstract
4. Working of enigma
5. Literature review of the novel method
6. Linear algebra techniques used
7. Results
8. Reference

About the Paper

Title:
A New Chaotic Encryption Scheme Based on Enigma Machine

Authors:
Zhi-liang ZHU, Chao BU, Hui LI, Hai YU

Publisher:
IEEE Xplore

Copyright Date:
2011

Abstract

In this paper, we have proposed a novel encryption scheme with chaotic process based on Enigma. The encryption scheme takes the advantage of the approximate non-linear mechanism of original Enigma, with the chaos controlling the encryption process. It has strengthened the randomness of plaintext replacement and improved the security of the encryption scheme. The results of encrypting images and letters proved that the novel encryption scheme shows good performances in the analysis of key sensitivity related coefficient between adjacent pixels and differential cryptanalysis

Working of Enigma

Summary

Enigma is a portable electro-mechanical device; its internal structure is shown in the Fig. 1[6-7]. In order to describe its encryption principle, we take only six letters as the schematic diagram of the internal structure.

By the Fig. 1, Enigma is consists of keyboard, rotors and monitor. Each rotor has different corresponding relation between right and left, and can rotate counterclockwise. Three rotors' initial position should be set up as a key before encrypting, and then the plaintext is imported from keyboard and replaced through three rotors.

At last, the monitor displays corresponding ciphertext. The first rotor rotates a letter's position after one plaintext having been encrypted. After a cycle the first rotor has rotated, there is a gear that turns the second rotor counterclockwise a letter's position, and one after another. The Fig. 1(b) shows the case of three rotors. The design of Enigma makes the process of encoding and decoding simple. But the encryption process of Enigma is not a simple replacement of letters. The same letter lies in the different location in plaintext can be replaced by a different letter. And the same letter lies in the different location in ciphertext can represent different letters in the plaintext. All these features make the frequency analysis useless.

The design of reflector in Fig. 1 makes decryption process very convenient. In the case of known the key, through the same route structure, ciphertext can be decrypted into plaintext by the reflector.

Diagrams

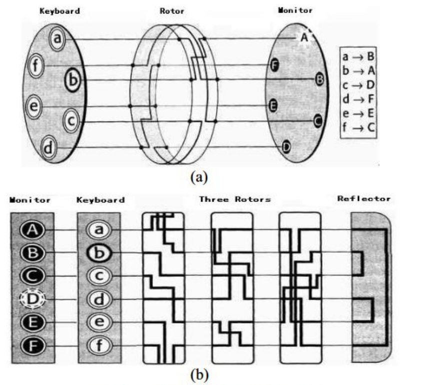
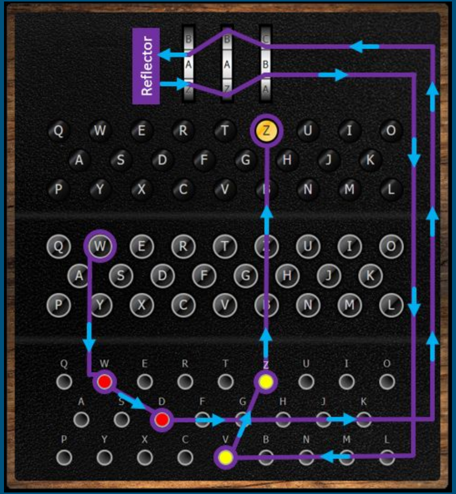


Figure 1. Structure sketch map of Enigma

(a)-The structure of rotor; (b)-The internal structure of Enigma



Literature Review of the Novel Encryption Method

Design

The original Enigma has the cyclical problem. The problem can be solved by increasing the number of rotor; however, it will reduce efficiency and increase costs. So the security can not be improved by this way. The novel encryption scheme is modeled on the structure of the Earth's latitude and longitude. Considering expanding the circle by using the chaotic mapping, the rotor will be chosen when each plaintext is encrypted, and the original position of the chosen rotor is determined by the correlation of the former plaintext. In this way, the cyclical characteristic is difficult to appear even in a very plaintext.

If each character in the plaintext is one integer between 1 and M, and the longitude (a complete circle) is as the rotor. Suppose there are six longitudes which locate at the degree 1=0°, 2 =30°, 3=60°, 4=90°, 5=120°, 6=150°. Each longitude is divided into M points which are points of intersection with latitude. All these points are the integers between 1 and M and distribute randomly on the longitude, so the points' values on the same latitude but different longitude are different.

Visualization and formulae

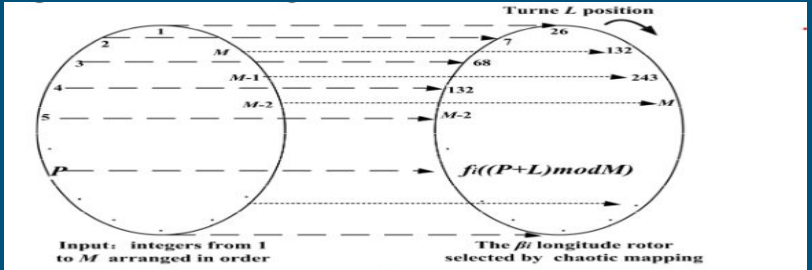

Turne L position
1
2
M
3
M-1
4
M-2
5
P
26
7
132
68
243
132
M
M-2
fi((P+L)modM)
Input: integers from 1 to M arranged in order
The βi longitude rotor selected by chaotic mapping

Figure 3. Encryption process of one character of plaintext

$$a_{n+1} = \mu \times a_n \times (1 - a_n) \qquad 0 < a < 1, n = 1, 2 \ldots \text{ (1)}$$

Where μ is the branch parameter, the system goes into chaotic status when 3.5699456…≤μ≤4.The more μ close to 4, the better randomness.

$$L_i = (a_1 \oplus a_2 \oplus \cdots a_{i-1}) \bmod M$$

$$\beta = \begin{cases} \beta_1; & 0 \le a_i < 1/6 \\ \beta_2; & 1/6 \le a_i < 2/6 \\ \beta_3; & 2/6 \le a_i < 3/6 \\ \beta_4; & 3/6 \le a_i < 4/6 \\ \beta_5; & 4/6 \le a_i < 5/6 \\ \beta_6; & 5/6 \le a_i \le 1 \end{cases}$$

$$c = f_i((Plaintext + l) \bmod M)$$

Linear Algebra Techniques Used

- Matrix translation
- Scaling
- Transformation to a spherical system

Results

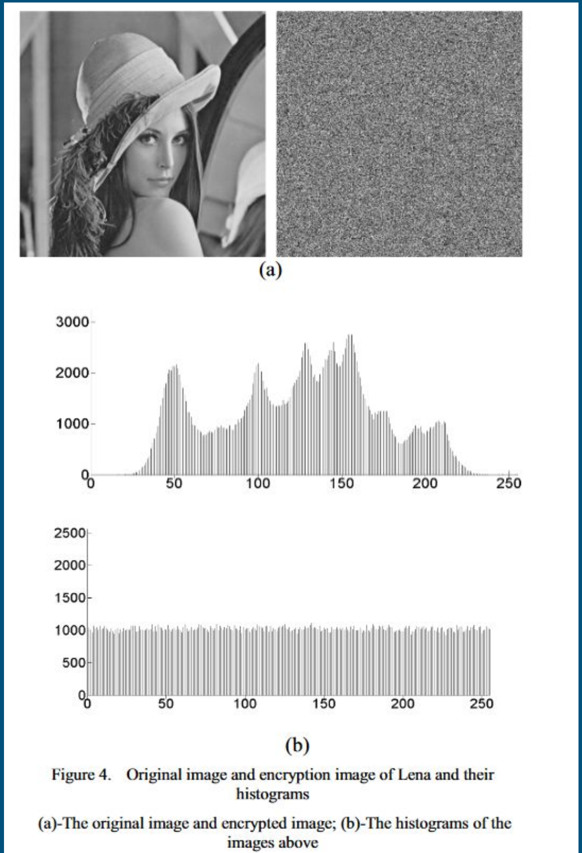
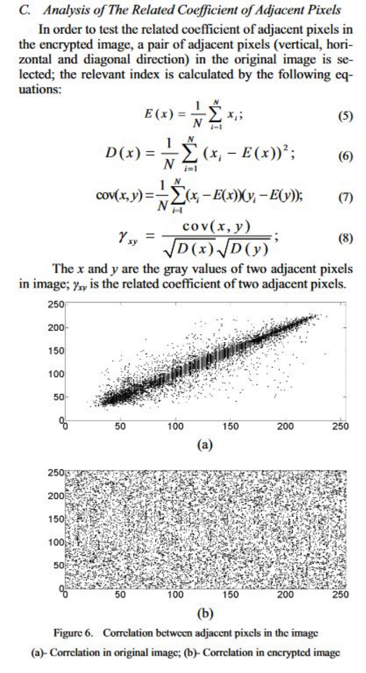


Figure 4. Original image and encryption image of Lena and their histograms

(a)-The original image and encrypted image; (b)-The histograms of the images above



C. Analysis of The Related Coefficient of Adjacent Pixels

In order to test the related coefficient of adjacent pixels in the encrypted image, a pair of adjacent pixels (vertical, horizontal and diagonal direction) in the original image is selected; the relevant index is calculated by the following equations:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i; \tag{5}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2; \tag{6}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)); \tag{7}$$

$$\gamma_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}; \tag{8}$$

The x and y are the gray values of two adjacent pixels in image; γ_{xy} is the related coefficient of two adjacent pixels.

Figure 6. Correlation between adjacent pixels in the image

(a)- Correlation in original image; (b)- Correlation in encrypted image

1. The end result at face value is a grainy, unrecognizable image. This indicates that the demo was successful.

2. Below the result is a plot relating the index of any given pixel on the image v/s their saturation values (only saturation was considered here due to the black and white nature of the image).

   We can observe that the variations in saturation have been normalized into a form with no apparent patterns, validating the working of the novel method

3. The final excerpt is a verification of the randomization of the saturation values using the correlation coefficient method. The plots indicate the saturation values of any two adjacent pairs of pixels

References

★★★★☆

This implementation exceptionally interesting read. You can find the paper and it’s included references at :

https://zero.sci-hub.se/3228/0cd82c32a20e0e5ad9d60cda31c59f04/zhu2011.pdf?download=true