Advanced Hybrid image Encryption for Defense and Medical Security

Guide

Dr.J.SIVASANKARI

Assistant professor-II , ECE

Velammal college of Engineering and Technology

Presented by

SURYAPRAKASH K - 913121106109

AJAI V - 913121106006

KISHORE S - 913121106303

Pre-Final Year ECE

9131 - Velammal College of Engineering & Technology (Autonomous)

Introduction

We have proposed an efficient and secure method of image encryption. This image encryption method is new , where the plain image is scrambled with respect to pixel position using confusion phase and diffusion phase modifies the intensity of the individual pixel values .

Objective

- To generate the key using SHA-3 algorithm for the given image

- To design the fibonacci-Lucas transform in order to change the pixel position

- To change the individual pixel intensity using tribonacci transform

Literature Survey

S.No.	Title of the paper	Author & Date	Methodology	Findings
1	An Efficient and Secure Method of Plaintext-Based Image Encryption sing Fibonacci and Tribonacci Transformations	Chinmay maiti, Bibhas chandra dhara, Saiyed umer, Vijayan asari 16 May 2023	Plaintext based image encryption using Fibonacci and Tribonacci transforms	Proposed the method for Grey scale image encryption
2	2D logistic-sine-coupling map for image encryption	Z. Hua, F. Jin, B. Xu, and H. Huang Aug 2018	a new two-dimensional chaotic map (2D-CCLS)applied in a chaotic image encryption algorithm to scramble, rotate and diffuse the pixels of the image	This algorithm has good performance such as large key space, strong anti-noise attack capability, strong key sensitivity and high security.

Literature Survey

S.No.	Title of the paper	Author & Date	Methodology	Findings
3.	Arnold transform based image scrambling Method	L. Min, L. Ting, H. Yu-Jie 04 may 2020	Arnold transform is used to change the pixel position of the original image to obtain the initial scrambled image then performs a bitwise exclusive-or operation on each pixel	This algorithm improves the scrambling effect
4	Image encryption with a new Fibonacci Transform	C. Maiti B. C. Dhara 10 jan 2018	Fourier transform with the property of fourier series to obtain scrambled image	This method is simple and fast and gives robust performance against different attacks

Literature Survey

S.No	Title of the paper	Author & Date	Methodology	Findings
5	Image encryption using modified Rubik's cube algorithm	R. K. Sinha et al 11 july 2019	The original image is scrambled using two secret keys, which is generated using logistic function and shift register method Then with XOR operator, rows and columns of the scrambled image are again mixed using various means	It is observed that the proposed scheme can resist exhaustive attack, statistical attack and differential attack.

Literature Survey

S.No	Title of the paper	Author & Date	Methodology	Findings
6	Medical image encryption using fractional discrete cosine transform with chaotic function	S. Kumar, B. Panna, R. K. Jha 9 oct 2009	XOR is first operated between the original image and logistic map. Then the chaotic image is transformed with Discrete fractional cosine transform two times using different keys successively by rows and by columns.	The transmission of the encrypted image with DFrCT and chaos is faster than with fractional Fourier transform (DFrFT) and chaos

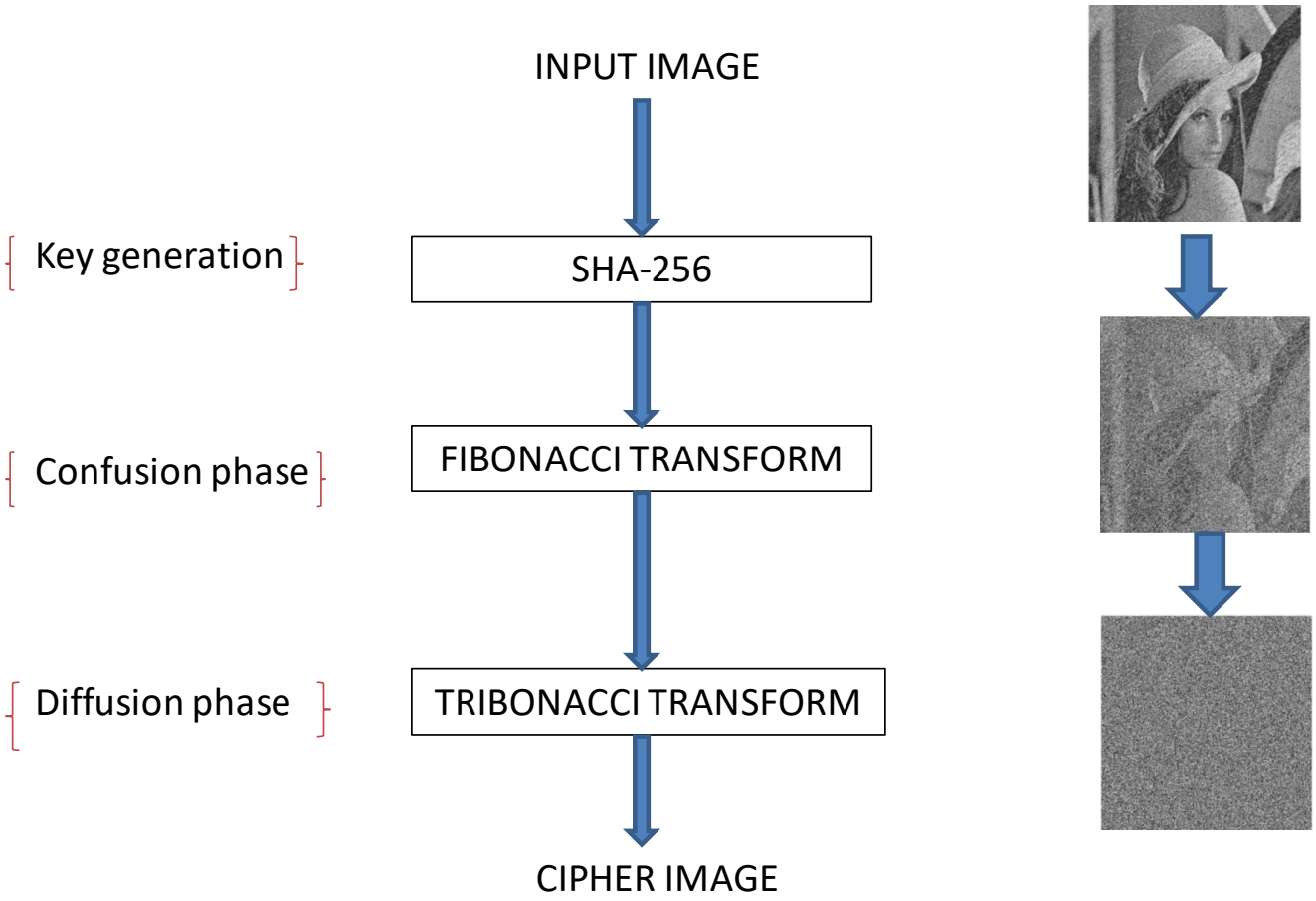
Literature Survey

S.No	Title of the paper	Author & Date	Methodology	Findings
7	XOR-based progressively secret image sharing	C.-S. Lin C. Chen Y, c. Chen,	The Progressive secret sharing produces a set of shared images in noisy-like form, while Friendly Secret Sharing generates shared images into more-visually-friendly appearance	This proposed method offers a lossless ability in the recovery result of secret image.

Literature Survey

S.No	Title of the paper	Author & Date	Methodology	Findings
8	Image encryption using permutation generated by modified Regula–Falsi method	A. Paul, S. Kandar, B.C.Dhara 21 jan 2022	The permutation is defined by the modified Regula-Falsi method and image encryption is achieved by pixel value substitution and iterative addition with the cyclic shift.	As the result of this proposed method, fully noisy images are obtained. It is immune against different attacks

Existing Methodology



Drawbacks of existing methodology

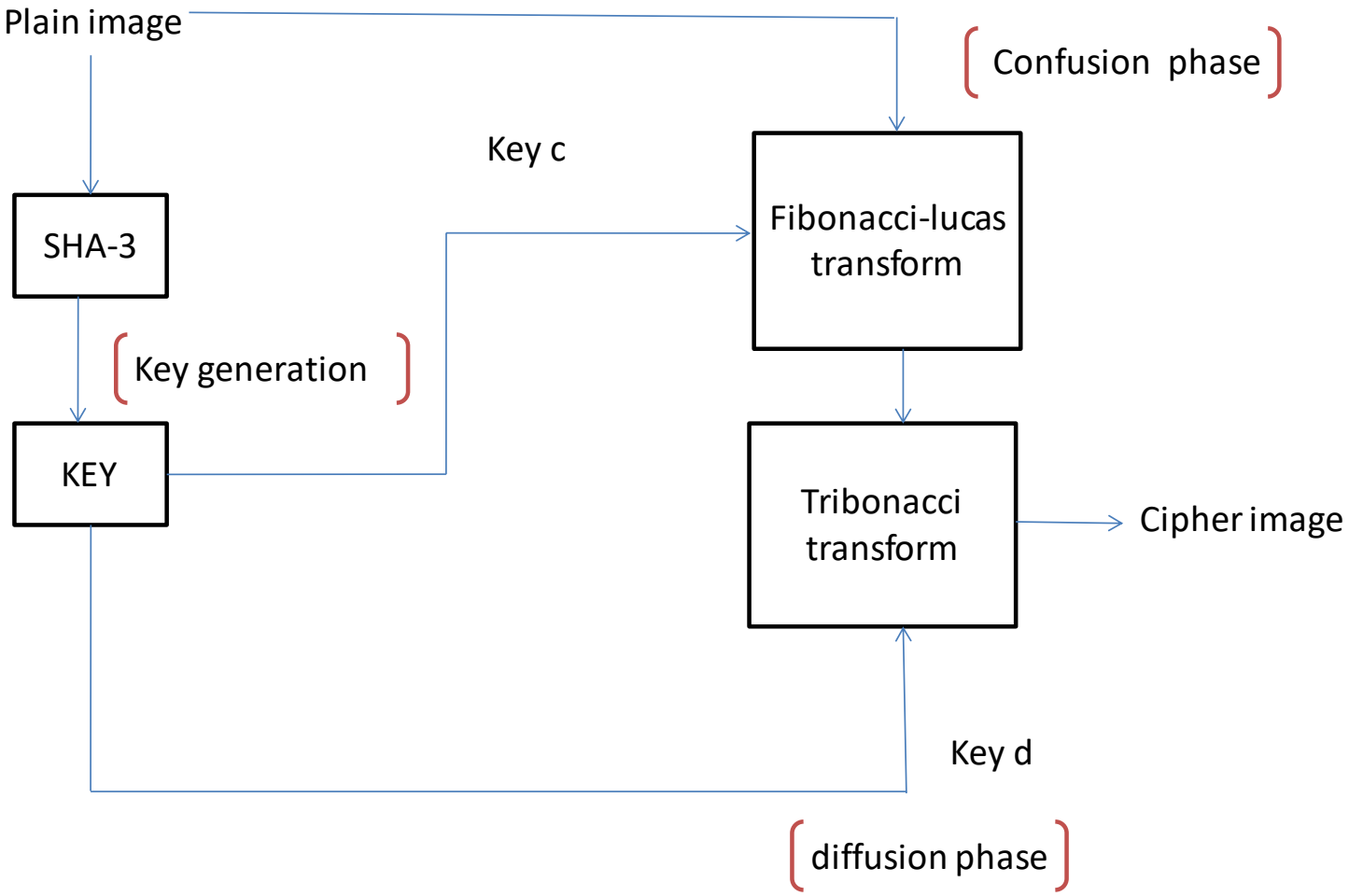
Drawbacks of SHA-256

- Low key space (no of possible keys) – brute force attack
- concerns about the length extension attack
- Fixed length upto 256 bits(Block size)
- Fixed output size
- Not specifically designed for resistance to quantum attacks

Drawbacks of Fibonacci transform

- Lack of Robustness - straightforward and predictable structure
- simplicity may not provide as much confusion as more complex transformations
- Lack of randomness

Proposed Methodology



Advantage of proposed methodology

Advantages of SHA-3 algorithm

- Large key space - variable upto 1024 bits (military applications)
- High resistance due to sponge construction
- Variable output lengths
- Simple padding scheme
- Performance - Balanced between security and speed

Advantages of Fibonacci-lucas transform

- High randomness
- Strong key distribution
- Combines Fibonacci and Lucas numbers
- adds complexity by incorporating both the Fibonacci and Lucas sequences.

STEP 1 : KEY GENERATION (SHA – 3)

Input: Img the plain image
Output: Keys {key_c, key_d} and key image key_img

Step 1. key_c(1: 128) = 0, key_d(1: 128) = 0

Step 2. key(1:256)= SHA3(Img)

Step 3. For i= 1 to 128

a. key_c(i) = key(i)

b. key_d(i) = key(128 + i)

Step 4. Return {key_c, key_d,}

STEP 2 –CONFUSION PHASE

Input : Plain image Img , confusion key key_c
Output : Confused image Img_conf

Step 1. Compute r' and c'

Img_conf(r', c') = fib_luc(Img(r, c),key_c)

Step 2. Return Img_conf

STEP 3 – DIFFUSION PHASE

Input : confused image img_conf , key image key_img , diffusion key key_d
Output : cipher image img_enc

Step 1 : k=mod(key_d , key_img)

Step 2 : img_enc = tri_trans(img_conf,k)

Return img_enc

Key Generation

Input image

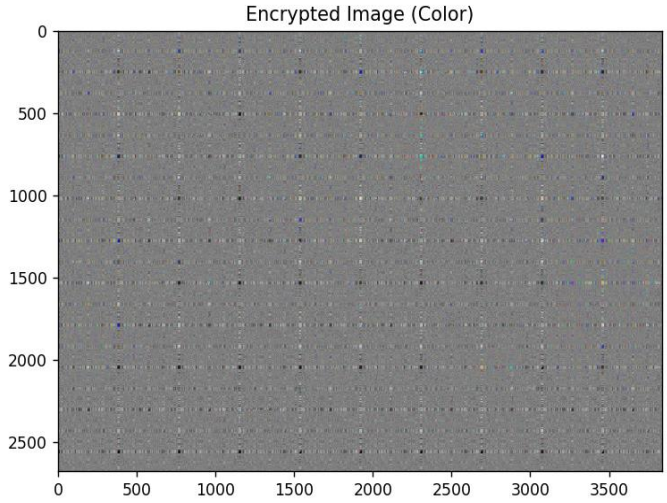
Key

IDLE Shell 3.12.1

File Edit Shell Debug Options Window Help

```
Python 3.12.1 (tags/v3.12.1:2305ca5, Dec  7 2023, 22:03:25) [MSC v.1937 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
========== RESTART: C:/Users/ajaif/final 3.py ==========
Enter the path of the color image: C:\Users\ajaif\OneDrive\Documents\thomas shelby.jpg
Generated Key: [1723922955, 3648364795, 1036889380, 3325281617]
```

Encrypted and Decrypted image



Flow of Work

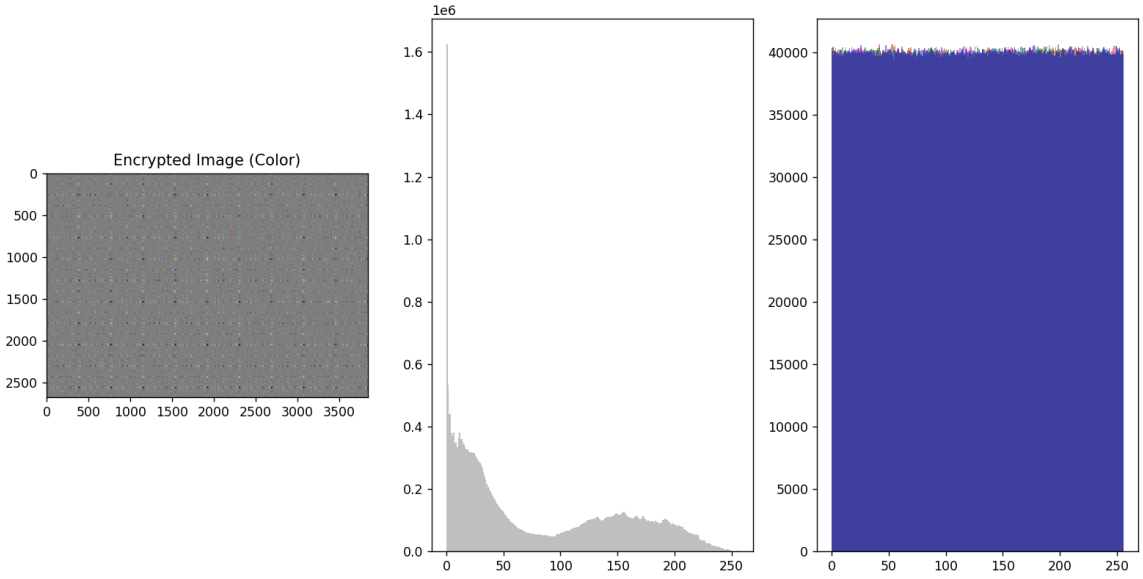
Encryption -

- Image from user
- Image to key generation
- Confusion phase – Fibonacci-lucas transform
- Diffusion phase - Tribonacci transform
- Cipher image (Encrypted image)

Decryption -

- Inverse of encryption

Histogram analysis



- histogram analysis involves examining and visualizing the distribution of pixel intensity values in the original and encrypted images
- Our proposed methodology showed excellent results for histogram analysis

Time analysis

Lena.bmp

```
>>>
====================== RESTART: C:\Users\ajaif\final 3.py ======================
Enter the path of the color image: C:\Users\ajaif\OneDrive\Documents\lena1.png.crdownload
Generated Key: [2372970498, 2835766870, 2358586091, 926782262]
Decrypted image saved as 'decrypted_image_color.png'
Average Execution Time: 0.6813 seconds
```

- Performed in intel i5 11400H
- 8 GB ram
- python

ALGORITHM	AVG TIME (sec)
Fibonacci-Lucas transformation	0.68
Arnold	2.6047
Fibonacci	2.2097
Poker Shuffle	0.79689

References

[1] Z. Hua, F. Jin, B. Xu, and H. Huang 2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map for Image Encryption January 2019 PP(99):1-1 IEEE access

[2] C. Maiti ,B. C. Dhara Conference: 2018 Fifth International Conference on Emerging Applications of Information Technology (EAIT) 10 jan 2018

[3] R. K. Sinha et al 'Advances in Computational Intelligence (pp.69-78)' 11 jul 2019

[4] S. Kumar, B. Panna, R. K. Jha 'Medical image encryption using fractional discrete cosine transform with chaotic function'international journal of information security 09 oct 2009

[5] C.-S. Lin C. Chen Y, c. Chen, 'XOR-based progressively secret image sharing ' IEEE Access (pp.66-76) 11 oct 2019

[6] A. Paul, S. Kandar, B.C.Dhara 'Image encryption using permutation generated by modified Regula–Falsi method ' IEEE transactions (pp-76-87) 21 jan 2022