DESIGN AND IMPLEMENTATION LIGHTWEIGHT ENGINE FOR MULTIMEDIA ENCRYPTION

REATREY PICH

A THESIS REPORT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF ENGINEERING IN COMPUTING IN ENGINEERING SYSTEMS
INTERNATIONAL COLLEGE
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
ACADEMIC YEAR 2017
KMITL-2017-IC-M-11-05

DESIGN AND IMPLEMENTATION LIGHTWEIGHT ENGINE FOR MULTIMEDIA ENCRYPTION

REATREY PICH

A THESIS REPORT SUBMITTED IN PARTIAL RULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF ENGINEERING IN COMPUTING IN ENGINEERING SYSTEMS
INTERNATIONAL COLLEGE
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
ACADEMIC YEAR 2017
KMITL-2018-IC-M-00X-00X

Thesis – Academic Year 2017

MASTER OF ENGINEERING IN COMPUTING IN ENGINEERING SYSTEMS

International College

King Mongkut's Institute of Technology Ladkrabang

Title: DESIGN AND IMPLEMENTATION LIGHTWEIGHT ENGINE FOR MULTIMEDIA ENCRYPTION

Authors:

1. Mr. Reatrey Pich Student ID 59610026

Approved for submission

.....

(Assistant Professor Dr. Jaruwit Prabnasak)

Advisor

Date ...../...../.....

THESIS TITLE	Design and Implementation Lightweight Engine For Multimedia Encryption
STUDENT NAME	Mr. Reatrey PICH
STUDENT ID	59610026
DEGREE	Master of Engineering
PROGRAME	Computing in Engineering Systems (International Program)
ADVISOR	Asst. Prof. Dr. Jaruwit Prabnasak
CO-ADVISOR	Asst. Prof. Dr. Sorawat Chivapreecha

Abstract

Security of multimedia data during the transmission is one of the main concern of vulnerable connection. In order to protect the data, cryptography has been employed by many techniques to hide the real information. Chaotic cryptography using chaos in digital filter with a new design of structure inside is proposed. It consists of two important parts, one is the key generator and other is crypto-engine. In this method, the unstable characteristic made by key generator's output selection to perform as a coefficient input to the system. It's composed by 16 characters password input (128 bits) and other two initialed coefficients then operates inside a new scheme of the second order IIR filters with the criteria finalization to get the proper desired output. The main engine of crypto-system, encryptor is also constructed by the second order IIR filter while the decryptor is by the second order FIR filter. In the whole system the non-linear behavior occurs because of the overflow function. Unstable and non-linear behavior produce the chaos in the system. As consequence, the output of both parts, software simulation and hardware conduction contain of key and plaintext sensitivity with strong confirmation of key space analysis and also get the high accuracy of security analysis.

The experimental results show that the proposed system can stand as a lightweight engine for multimedia encryption with the high security confirmation and high performance in order to secure the data throughout the transmission.

Acknowledgments

This work would have been impossible, if there is no the treasured contributions and support from the following people.

First and foremost, I would like to express all my gratitude and thank to both my advisor and co-advisor Dr. Jaruwit Prabnasak of International College and Asst. Prof. Dr. Sorawat Chivapreecha of Department of Telecommunication Engineering, Faculty of Engineering at King Mongkut's Institute of Technology Ladkrabang for their valued supervision, encouragement and suggestion to win all the problems and obstacles since the first day of my project until the last day of my study here. Additionally, I also would like to thank all lecturers and staff of KMITL who have provided the proper knowledge and services to fulfill my research and work with their worth contributions and time.

Furthermore, I also need to show my gratitude to AUN Seed Net scholarship and staff for providing the big opportunity for me to conduct my master degree here with an appropriate financial support and help for this whole two years.

Finally, is for my family and friends for their power of love and taking care to rich my motivation through these years. Because of these people above, my best achievement has brighten my educational life.

Bangkok, July 2018

Reatrey PICH

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation to the research

With recent high technology, the innovation and development of multimedia and information communication, data is connected in the terms of large infrastructure of network. Mainly use of information transferring, it becomes the main concern because of its values and privacy, especially in the commercial or security domain.

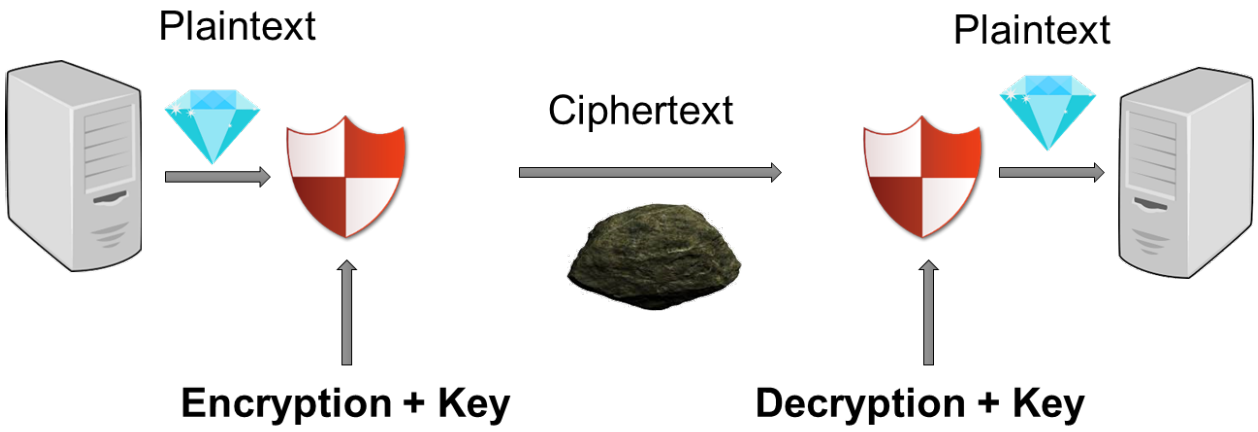


Figure 1.1: The process of data transmission with cryptography purpose

In order to conduct those needs during data processing before the transmission or distribution, there are many techniques composed by different algorithms which have been widely used such as Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES),

International Data Encryption Standard (IDEA) and Chaotic Cryptography in Digital Filter. In the base of digital multimedia data, chaotic cryptography in digital filter is the best direct solution to mask the data to be secure while other standard cryptography algorithms face with the obstacle of high redundancy point and high correlation data such as digital image. Therefore, the characteristic of chaotic cryptography in digital filter which is built to be the nonlinear dynamical systems with the unstable status stands as the recent strong attention in researching field of security of the world of digital data. Because it's widely used second order digital filter form with an adder overflow nonlinearity which can produce the high cipher text quantity of security and less of complexity because of using least number of multipliers and adders. However, there are still some weakness to fix up and improve in order to reach the best and optimal solution one. With other motivation for hardware conduction, there are a lot of services which are needed to be secured such as in niche markets smart card conduction to keep the privacy and security for customers before there card access to reach the servers. On the other hand, in terms of small system there is no room for software execution so external embedded cryptography is extremely needed because chip is not embedded any core to disturb the process. In the case of large volumes of secure data which is intended to process as the pay TV or SSL accelerator and technique to hiding the resource, cryptography hardware functions essentially to run that performance. In some conditions, if the software is emerged with cryptography system, the information of the key and the process will be able to be stolen in cache data in some ways. So high security algorithm with both advantages in software and hardware is a potential solution need for recent technology.

1.2 Objectives of the research

In this research work, the aim is to design and implement lightweight engine for multimedia data encryption. Step by step, the tasks have been divided as three main scopes differently. The first one is to orient the chaotic key generator to achieve the sensitive crypto-system with the high security confirm to the cipher text. For the second work, we focus on the investigation of the different structure of proposed system and its comparison the standard algorithm output. By the way, this work we have found some notification points of given architecture. And the last is the real product in local conduction in order to produce the real time system processing.

The whole goals of the work is shown as below:

Figure 1.2: The scope of researching project

1.3 System overview

In this thesis work, there are two proposed architectures different. Firstly is the single form of chaotic cryptography in digital filter and other one is the triple form. Both structures are composed by the second order digital filters and there are two parts in the main system. One is key generator and other is crypto engine. For the triple form it is just the multiplication three times single form and it is used Infinite Impulse Response (IIR) Filter to construct key and encrypt engine for the decryption process it is just the inverse process of IIR filter is Finite Impulse Response (FIR) filter. The system is constructed with one key generator and one IIR filter as encrypt engine. Key generator is made with three times of IIR filter to produce two coefficients for the main engine and its functionality of output is to make the system to be unstable. For the triple form of the proposed

architecture is three times of the single form but for the key generator we still keep the same input of 16 characters known as 128 bits to be the key input from the user and it produces six coefficients different for the encryption engine. In this case for crypto engine is also made by three times of IIR filter with different coefficients and one filter's output is the input for the new one. However it is composed by three times of key generator but the main structure inside the key generator is still kept the same for all the cases. Inside this structure, it is also cooperated with the initialed values of other two coefficients and other two of initialed input value.

The whole process is shown in the figure below:

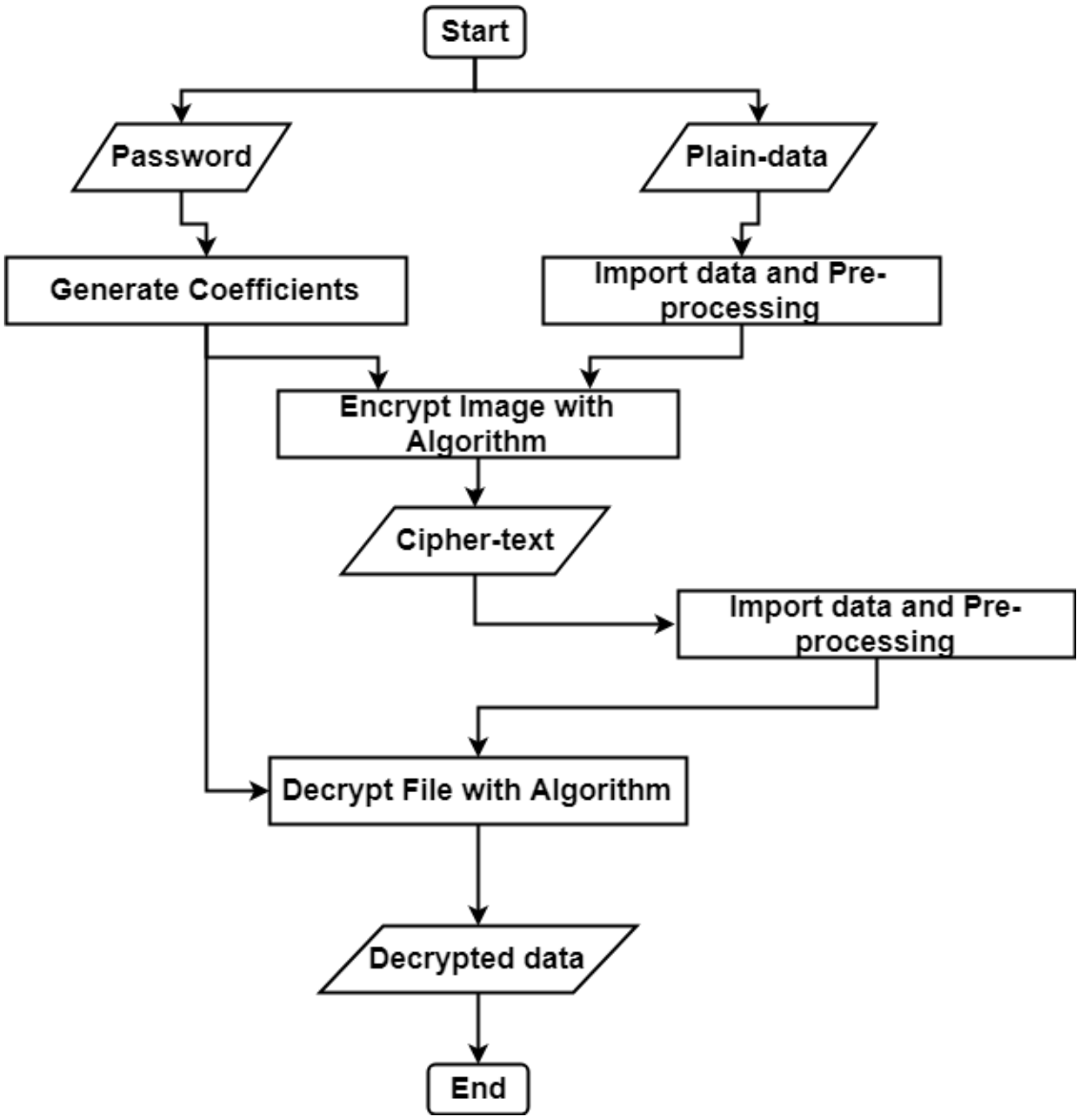


Figure 1.3: System overview

1.4 The organization of the thesis

The organization of this thesis is ordered as below:

- CHAPTER 1 : INTRODUCTION

In this chapter we provide the information about the motivation and the problematic to let use to do the project. And it also shows about the scope and system overview of the researching project step by step and respectively.

- CHAPTER 2 : LITERATURE REVIEW

The background information and also the points of existing solutions which encourage us to conduct this work and also some criteria of those work too.

- CHAPTER 3 : PROPOSED METHODOLOGY

Thirdly is about the proposed method that we used to conduct in our research. In addition it also gives the details of each point of proposed structures to let us know more specifically and how it works.

- CHAPTER 4 : RESULTS AND EVALUATION

In the results section, we are going to provide the outcome of our work with the cryptography and cryptanalysis. Each section we will give the evaluation to the answer and results that we got.

- CHAPTER 5 : CONCLUSION AND DISCUSSION

Lastly is the conclusion. In this section we will wrap us all we have done both the achievements and the weakness of the system. The next one is about the future work that will be the last point of this section.

Finally is the biography of the author and the publication information and papers.

Chapter 2

Literature Review

This chapter is denoted about the literature review about the related work in the same purpose but using the same and different methodology to conduct the system. It illustrates to confirm about some weakness of the existing solution and the design technique from other method to merge with this proposed solution.

2.1 Research background

Basing on the information security, the science of cryptology functions as the main solution to hide the originated information properties and techniques in order to keep its secrecy and privacy. That science points out the security technology for data crypto-processing characteristics such as cryptography and cryptanalysis. Both of them are the study of creating and solving the problems including encryption and decryption.

Figure 2.1: Cryptology diagram

1. **Cryptography**: is the methods, algorithms or the technique for hiding the information and against the unauthorized access. Focus on the cryptographic algorithms to multimedia data like encryption and decryption, it shares the key together in order to synchronize the process. The system which is conducted with symmetric-key techniques or algorithms work out by sharing the public key to each other such as Data Encryption Standard (DES), 3DES or AES while the asymmetric one use the private key for processing respectively like Elliptic Curve Cryptography (ECC) and Rivest, Sharmir and Adleman (RSA). Talking about the cryptographic protocol is also used the private key to run its performance. On the other hand, for primitives security terms is the process of random number generator.

2. **Cryptanalysis**: is the part of selected method analysis. It works directly to the secret information without accessing to the corresponding secrets. To assure the cypher text is qualified enough to stand hiding its own properties, the mathematics operations have been used to justify it. And it is also given the attention all some standard value to evaluate the output depend on the data type that is processed.

For the selected methods or algorithm which are used to work as symmetric or asymmetric system, all of them conduct with the key so the table below is some of the recommended key length for the

level security inside the key analysis.

Level of Security	AES/DES	ECC	RSA
Short-term security	64 bit	128 bit	700 bit
Middle-term security	80 bit	160 bit	1024 bit
Long-term security	128 bit	256 bit	4096 bit

Table 2.1: Key Length suggestion

2.2 Related studies

Cryptography is one of techniques of security concern in data transmission. It covers various aspects such as security, compression efficiency, encryption efficiency and format compliance. There are many data encryption algorithms which have been widely used like DES, 3DES, AES or IDEA. However, each other these algorithm still provide non-appropriate results if we focus on both security confirmation and high performance. Likely for DES which is known as a 64 bits block cipher, it works with 64 bits of data per time. In fact, the provided key is 64 bits but for the real operation inside it is used only 56 bits. This solution can provide an acceptable for cypher text but it work out not the suitable key length. To solve this weakness the new innovation of DES to be 3DES were approved to solve that but the performance is still the main concern because of high complexity.

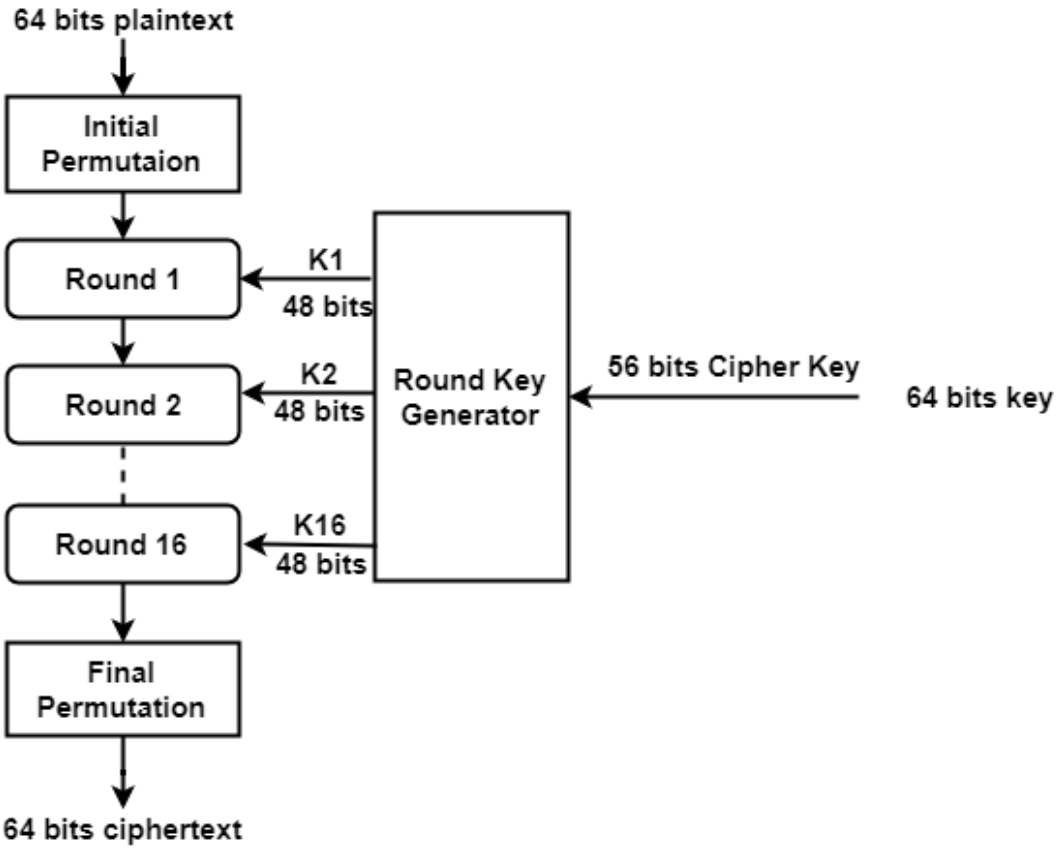


Figure 2.2: Diagram of DES Algorithm

For the structure of 3DES is the combination of three time of single DES by using the key bundle in order to generate K1, K2 and K3.

$$Ciphertext = E_{k3}D_{k2}(E_{k1}(plaintext)$$

Because of DES works until 16 rounds so inside 3DES, it has to perform 3 time of DES. Security can be confirmed strictly that it gives high impact but for the performance is still poor. To balance those things, AES was implemented to follow the same structure from DES but it has been increased the size of the key in order to get the better result both security confirmation and performance. But in the point of multimedia data is different from text because multimedia data has high redundancy, so AES produced non appropriate cipher-image [1].

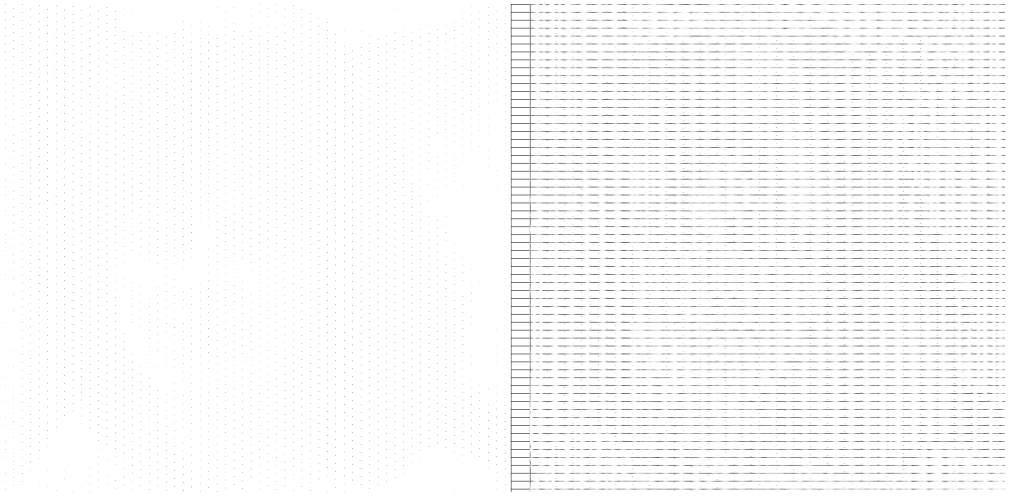


Figure 2.3: Multimedia Encryption of AES

Mainly the same problem [2] has stated DES using Logistic map can make the cipher text to be the stochastic noise to against the attack and can improve DES but inside the process it runs with high complexity because of the round keys randomization factor. Moreover, the technique of making only different 3 rounds of the key accompanied by the chaotic properties also produce the high security of encrypted image but the complexity of converting cypher image to by Elliptic Curve is still getting high [3].

On the other technique, chaos in digital filter is also the best solution and currently getting attention from the researchers in cryptology. It produces the nonlinear behavior and unstable system to make the cipher-image possess security by matching with overflow nonlinearity function [4]. But some concerns still exist such as some solution still give high complexity as same as compare to DES solutions. Otherwise, it is famous as the good password system in case of using the parameters and initial values as key [5]. Unlikely, in the work of [6] the results can improve the security and performance still stays in the considerable condition. It provided the best solution to key sensitivity to the system but the architecture of the system provided the high complexity structure with it XOR operation and other combination process. Because of those factor and lacking point above make the cryptography is given concentration by many research in different domains. In addition, because of the result of chaotic in digital filter gives the suitable notification of the results, it is also one the main resource and solution for keeping work to release the real hardware design in order to make as exactly running system.

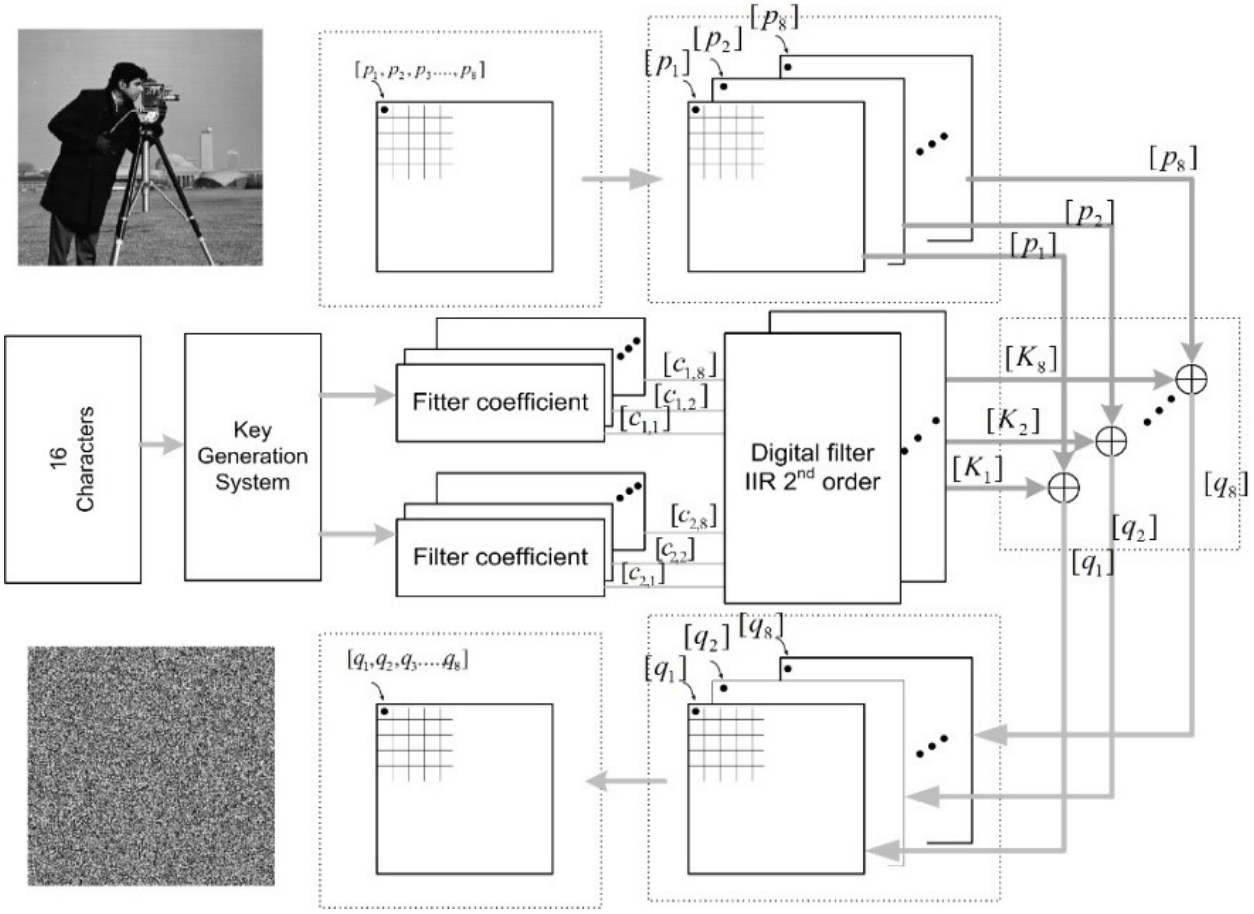


Figure 2.4: Architecture of previous chaotic cryptography in digital filter of laboratory

Chapter 3

Proposed Methodology

This chapter is introduced about the general knowledge to the background information about the method in use. It is also shown about the structure of each techniques inside this proposed solution from the key generator until the main system of cryptography.

3.1 Digital filter

Inside the domain of Digital Signal Processing (DSP), digital filter has stood as an important part that can make DSP to be famous and getting attraction in the researching fields. Because of its purposes which is aimed to work out with the signal to purchase two main goals accordingly such as Separation of Signal and Signal Restoration, digital filter has involved itself in to many sectors efficiently, cryptography is one of included uses.

1. **Separation of Signal**: Generally, in digital signal processing, there are always the problems of contamination with the interference, noise or with the other signal which is being processed in the same time or the same frequency domain flow so they must have been split from each other to get only the needed or important one.

2. **Signal Restoration**: In some ways or work, the goal is contrast to the mention above. Some signals have to be combined or filtered when they had been distorted in some way, especially when the poor equipment has been used for work processing like poor camera and multimedia editor.

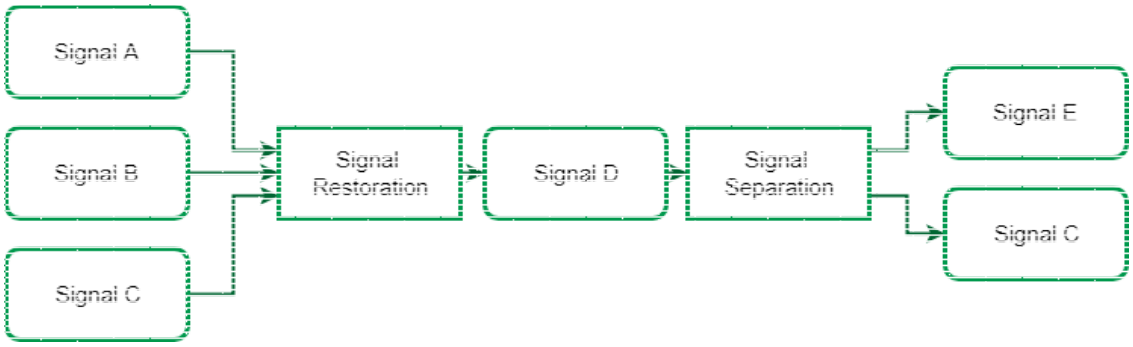


Figure 3.1: The introduction to signal combination and separation

To design digital filter, there are some strategies have been noticed such as Filter Kernel and Recursion. In each manner, the process to build it up has been made for different purposes and different structures.

- **Filter Kernel**: Normally in the filter usually contains an impulse response, a step response and a frequency response. In every responses exists of the whole information about the filter. Actually, when one of them is specified the other two must be fixed and can be found by directed calculation from the specified one. Therefore, when we make the combination or convolving of the input signal with digital filter's impulse response to create other third signal, this way is the straightforward solution to implement a digital filter which is called **Filter Kernel**.

- **Recursion**: is the other technique that is used to implement digital filter by using the convolution. And the formal definition of convolution is written as **Convolution Sum**. When we need the output of signal $y[]$ whose i is the position of signal point compare to the input one $x[]$ and we have $h[]$ is the M point signal running from 0 to $M-1$ that we can call it as impulse response. The equation to represent this process has been defined as below:

$$\mathbf{y[i]} = \sum_{j=0}^{M-1} h[j]x[i-j] \tag{3.1}$$

In the distributed system y is output signal, x is the input signal and h is system's impulse response.

Beside of using impulse response which is the filter kernel, we can use the recursive filter which is composed by a set of recursive coefficients. Inside this research work the proposed structure and

methods have been worked out with recursive filter when some amplitude eventually drop below the round-off noise of the system and ignore some of sampling so it is call Infinite Impulse Response Filter (IIR filter) in the place of key generator and encryption engine and also constructed by the convolution as the second order structure. Otherwise, the inverse process of this work has been used to be the decryption engine which filter named as Finite Impulse Response filter (FIR filter).

3.2 Proposed architecture

The scope of this project has been covered by three main architectures different. Firstly is the key generator which is aimed to use to produce the coefficients for the cryptography engine. The input of key generator has been given by the user and the length of key is 16 characters equals to 128 bits. Because of using the domain of digital filter and with non-linear behavior for the system, inside software simulation the value of each characters has been scaled into the domain of $[-1, 1)$. And it is composed by other fixed coefficients to construct IIR filter. The structure has been shown in the figure below:

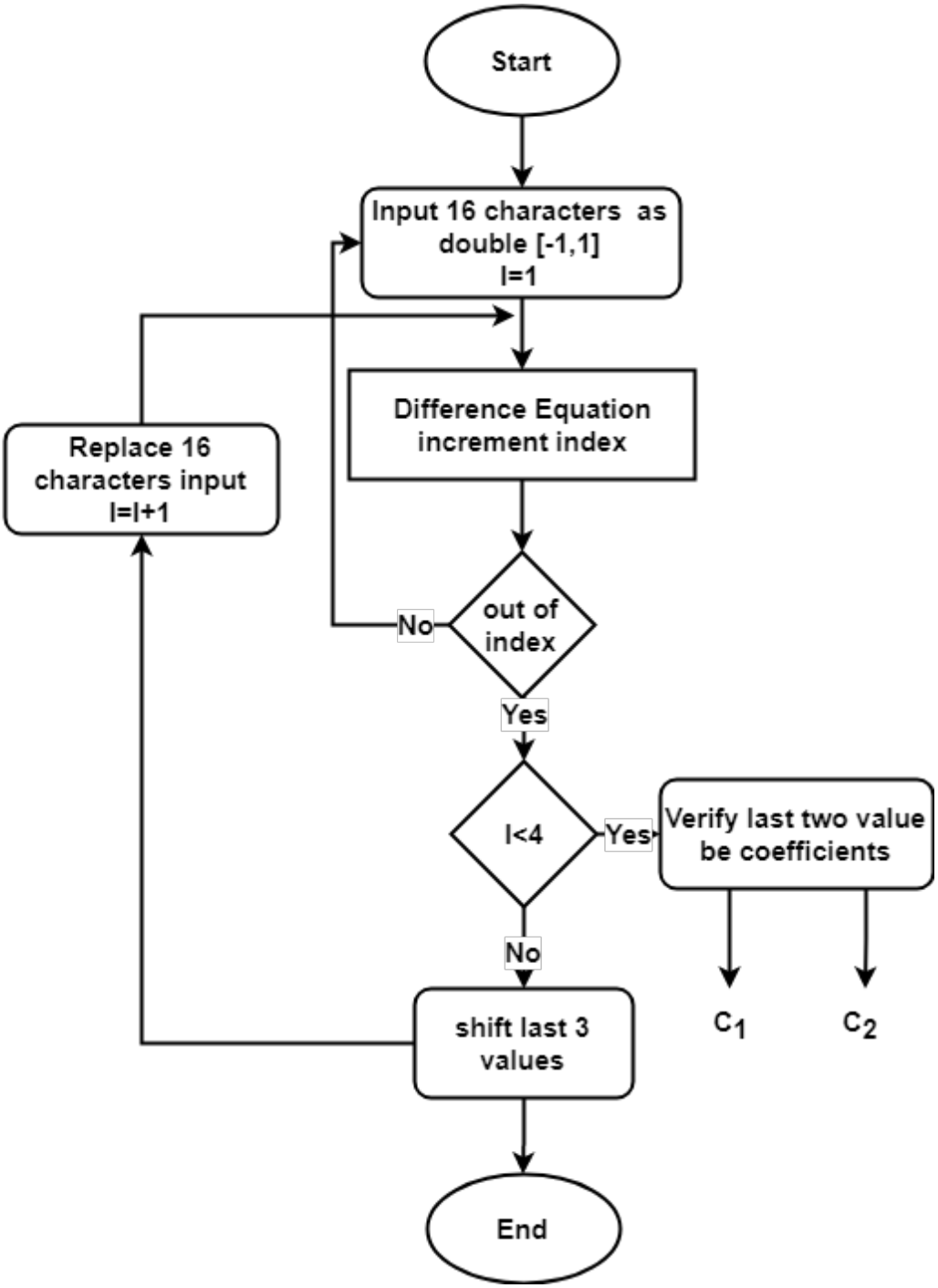


Figure 3.2: Diagram of key generator processing

The difference equation is the mathematic formula of IIR in the second order structure. The technique proposed in the work is to get the key sensitivity and efficiency for the whole system. There are many functions which is the sub element to reach the goal.

1. **Shifting function**: within this proposed structure, three IIR filters have been used to conduct the process, so to make change from one filter's output to be input for other filter we have make 3 values shifting. When the 16 output is gotten from the first filter the last three values have been scaled position to be the first three values.

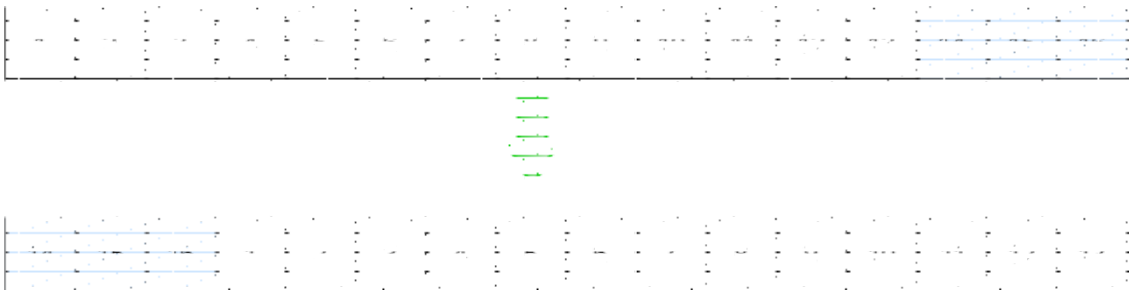


Figure 3.3: Shifting function technique

2. **Verification function**: the condition inside the system, not only focus on the output we also think of the initialed values in the system. In order to make sure that the proposed architecture produces chaos and suitable for the system the selected initialed values has been considered to follow the rules which mentioned in Figure 3.3. For the output we have to consider some conditions such as non-zero output and also respect the condition of unstable system and overflow function.

The other main proposed structure is the whole system architecture. Inside this research work the proposed main architectures are separated into two outline different. Each structure performs the security confirmation information and the performance separately. On the other hand, the work flow of each architecture also show in the different way too but the basic concept of the work is the same.

3.2.1 Single form of chaotic cryptography using chaos in digital filter

For this proposed structure is one of the main and also the selected achievement of this researching work. As have been mentioned above the architecture of the system exists of two main parts different: one is key generator which the work flow have been described in the first section of the proposed architecture. Key generator functions at the coefficients provider to the main system to

construct the operation inside. For the main system is built up with one of Infinite Impulse Response Filter in the second order. Inside the process the coefficient which aims to make the system to be unstable system have been verified in key generator. When we input the multimedia data as the input to the system we consist of some process before we use it with the main operator.

1. **Preprocessing Technique**: the process of this position, it depends on which type of data that we will use. Inside this project we worked out with three type different one is text encryption and other two are audio and image for the video file it is just the combination of audio and multi frame of image. All the case, the main concept is the same we have to convert all the data to be in the domain of $[-1, 1)$ and input as one dimensional array input. Then it is set to the main encryption process or decryption process as its purpose of the process.

2. **Encryption**: inside the encryption engine it is composed by two mains thing too. First one is IIR filter mathematic operation to operate the encryption process and another one is Overflow function which aims to convert and manage all the data to be in the limited domain. Each point of the data in the operation have relationship to the previous point of its position so it is the dynamic notification inside the cryptography processing.

After that the last process is convert all the data into its original structure and format for the vision overview. The detail has been shown in the figure below:

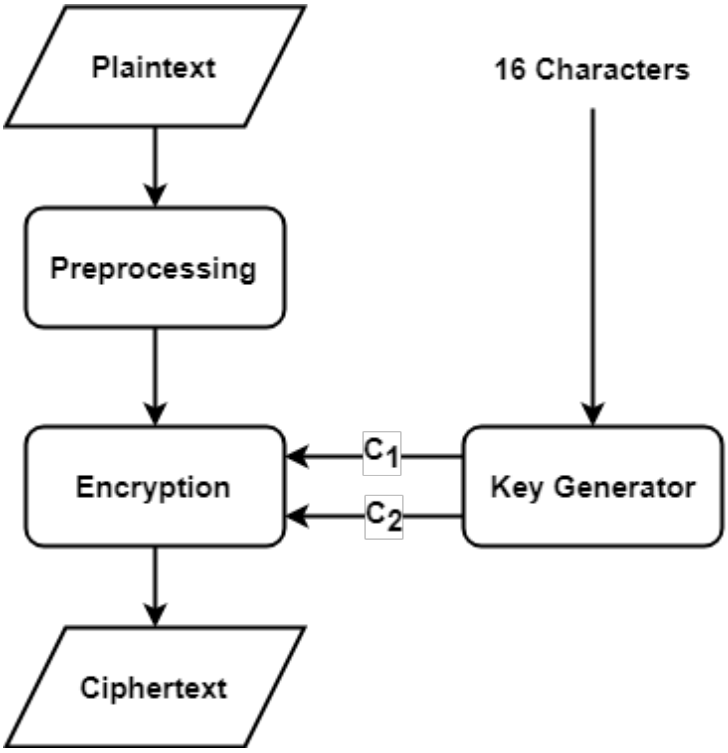


Figure 3.4: Diagram of single structure

On the other hand is inside the encryption engine also contains of the other initialed values in order to operate to make change to the first point of the data. For this case if the initialed value has been set to be 0 the first point of the data will keep as the original for image and audio is not the main problem because the data contains of big connection of its intensity value but for text file it has to show that its original first alphabet or character.

3.2.2 Triple form of chaotic cryptography using chaos in digital filter

However, it is not the main goal of this research work but it is also the main notification point in order to consider and analyze the system too. And the process is also complicate if we compare to the first proposed structure. Its structure is the combination of three times of single form. The concept inside is still kept the same as the first proposed one.

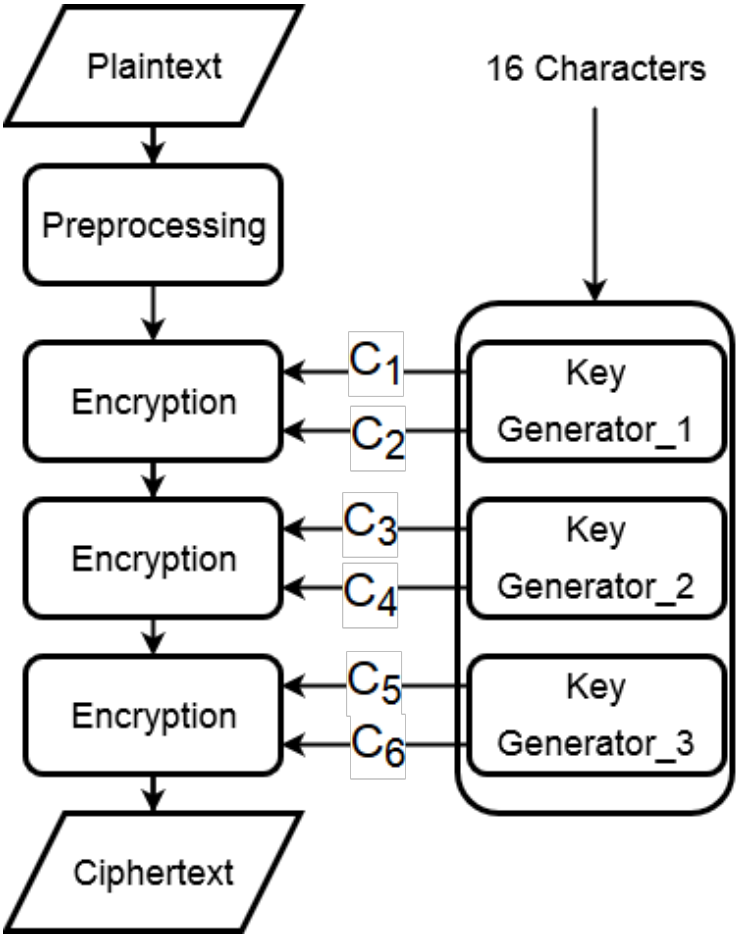


Figure 3.5: Diagram of triple structure

Although, it is the three combination but we still have only input password but the difference of each key generator is the initialed values inside. All coefficients can't be 0 and it follows the rules of stability the same as before. The detail is shown in the block diagram below:

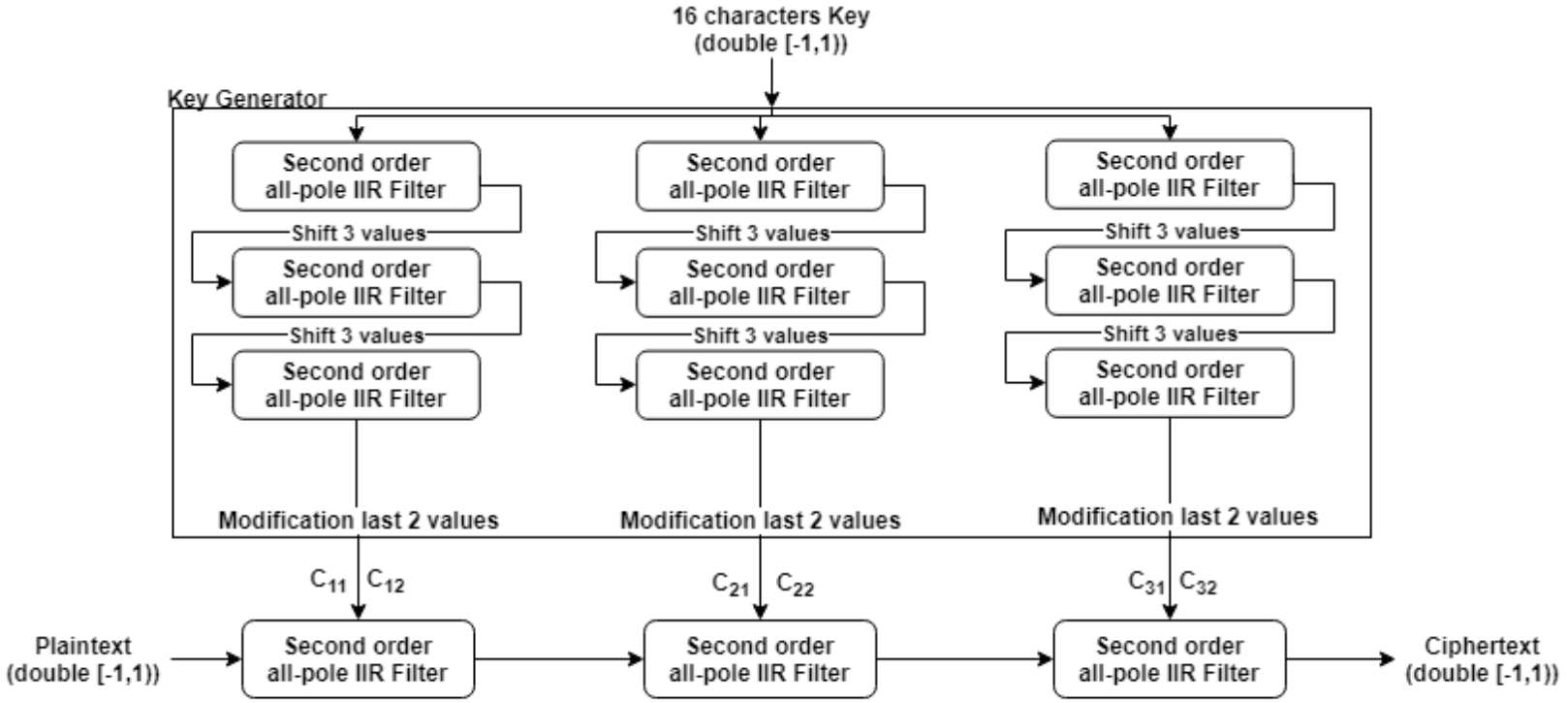


Figure 3.6: detail of triple form work flow

We have to use 12 IIR filters for encryption engine system totally. But if we focus on the decryption engine we have to use 9 filters in key generator and 3 FIR filters in the main engine. For main engine it follows the concept from the key generator. It means that the output from the first engine to be the input for the next engine but in this case we do not use the shift function. Each output become the input as originally value. The proposed structure provides high complexity than the first one but security confirm is better. It still consists of one more weak one is the black color become white color in the decryption process in some position. Second order digital filter and chaotic characteristics.

Digital filter which is built up by the recursive structure accompanied by the convolution summation mathematic equation is known as the widely used technique for Digital Signal Processing Term. The condition of equation which is aimed to produce dynamic system especially in cryptography domain. Such as in [7], chaotic cryptography is known as a dynamic system that's followed by the mathematical equation such as in Cat map and Baker map which are used for the confusion portion. Otherwise, digital filter has been used in the unstable system and non-linear system instead of chaos-based algorithm by cooperating with the overflow function in order to make the chaos [8]. It is also mentions that the second order of digital filter is the common used and so effective to the system implemented. Chaos in digital filter, IIR filter functions as an encryptor while FIR is its inverse to work as deycryptor. The authors has also mentioned that in the digital domain for secure communications, QC-properties are used to characterize a chaotic non autonomous digital filter. Each properties has been confirm with the assumption of the experimental results and if other researcher can confirm other thing than this the paper suggestion to contrast the idea.

Having mentioned above that the second order digital filter is the widely used to make the operation in cryptography functionality. This work is also made the new concept of architecture design of digital filter both in the part of key generator and crypto-engine.

For the key generator and encryption engine have been implemented with IIR filters and the characteristic of the filter has been shown in the figure below:

Figure 3.7: IIR Filter in second order structure

The operation of this figure is replaced by the mathematic operation which is known as the convolution summation in the seconder other follow by characteristic of chaos which is the main definition of this research. In the formula, the value of a_1 and a_2 have been replaced respectively by C_1 and C_2 and $b_1 = 1$. The figure above is not yet emerge the overflow function with which is in the last position to be output.

$$\mathbf{y(n)} = x(n) + C_1 y(n-1) + C_2 y(n-2) \tag{3.2}$$

$$\mathbf{H(z)} = \frac{y(z)}{x(z)} = \frac{1}{1 - C_1 z^{-1} - C_2 z^{-2}} \tag{3.3}$$

$$\mathbf{f(x)} = [(x+1) mod 2] - 1 \tag{3.4}$$

$$\mathbf{y(n)} = f\{x(n) + C_1 y(n-1) + C_2 y(n-2)\} \tag{3.5}$$

The first equation is the formula of second order IIR filter which $y(n)$ is the output of the system while $x(n)$ is the input as the multimedia data. For $H(z)$ is the transform function for this digital filter. In order to make our system to have non-linear behavior the overflow function $f(x)$ with modulo operation to number 2 has been used. The last equation the whole equation when we combine together.

To build the decryption engine, FIR filter has been used and the process of this filter is the inverse process of IIR filter only. For the structure is also constructed in the seconder order as IIR

filter. If we focus on the mathematic formula is also the contrast form IIR formula. But the overflow function structure and the condition of the coefficients still be kept to be the same all cases. Beside the single form, the triple form is also used the same structure to connect the filter continuously as in encryption we used IIR filters and in the decryption we just replaced them by FIR filters.

The architecture of this filter has been formed as the detail in the figure below:

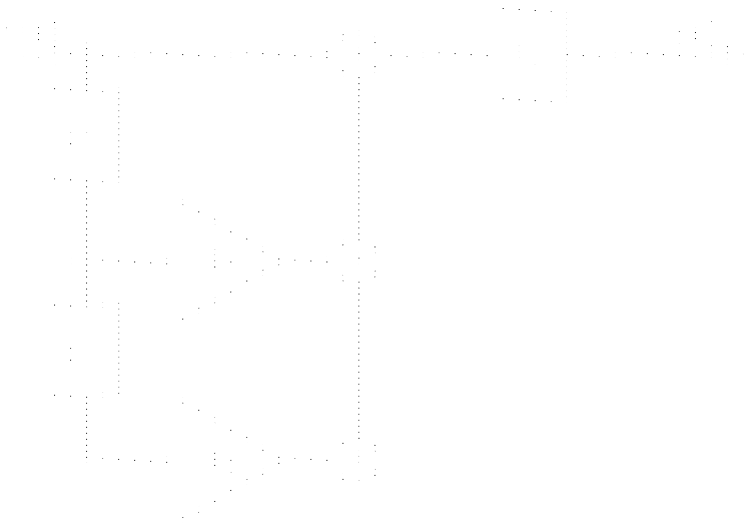


Figure 3.8: FIR Filter in second order structure

For the mathematic operation is also not really different from the IIR filter it is something the same with overflow function and the inverse form of the previous equation and the figure is merge with overflow function already:

$$\mathfrak{Z}(\mathbf{n}) = y(n) - C_1 y(n-1) - C_2 y(n-2) \tag{3.6}$$

$$\mathbf{H}(\mathbf{z}) = \frac{\mathfrak{Z}(z)}{y(z)} = 1 - C_1 z^{-1} - C_2 z^{-2} \tag{3.7}$$

$$\mathbf{f}(\mathbf{x}) = [(\mathfrak{Z} + 1) mod 2] - 1 \tag{3.8}$$

$$\mathfrak{Z}(n) = f\{y(n) - C_1 y(n-1) - C_2 y(n-2)\} \tag{3.9}$$

As in IIR and FIR equations we have to initial the values of the first two inputs in order to make change to the encryption process for the first element of input data and also to get back the original data. The selected initialed value, we can't choose whatever we want. [9] The author has mentioned

about the characteristic of the fractal geometry of self-similarity of the trajectory which is the property to combine with the coefficients to make the system to be unstable system. So the suitable one we got as the first two inputs are $y(-1) = -0.6135$ and $y(-2) = 0.6135$. Otherwise, our system will become the stable system which can't get to the chaotic characteristic and our system can produce the appropriate results with the perspective of cryptography and cryptanalysis. On the other hand, the unstable system of second order digital filter is defined by the characteristic of the coefficients to the stable triangle if they are staying both inside the triangle it means that our system is the stable system. In contrast if one of the coefficients or both stay outside the stable triangle region, it points out that the system is unstable. [10] The authors have confirmed that in order to make certain that our system is unstable system and generate chaotic output, the coefficient must be at least one is outside the stable triangle or be larger than unity.

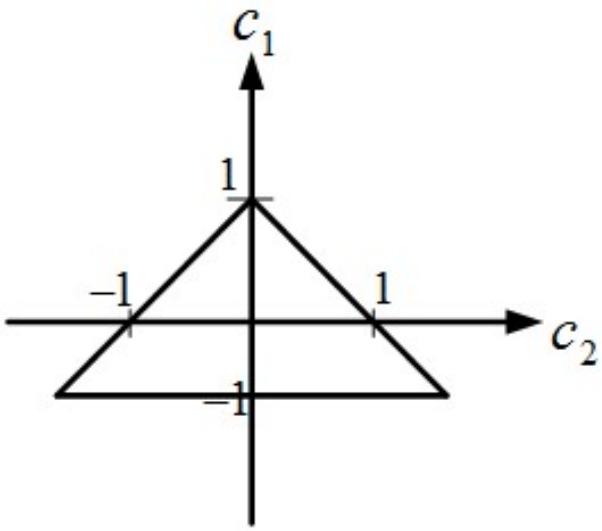


Figure 3.9: Stable triangle

To verify that the coefficients are outside the stable triangle, the mathematic operation of the unit circle has been used to analysis. And for this condition there no coefficient be 0 all must be the value.

$$\mathbf{P} = (-b \pm \sqrt{b^2 - 4ac})/2a \tag{3.10}$$

Where it is the formula of the root of second degree of the equation. But inside the system, we

have the transform function as below:

$$\mathbf{H}(\mathbf{z}) = \frac{y(z)}{x(z)} = \frac{1}{1 - C_1 z^{-1} - C_2 z^{-2}} \tag{3.11}$$

Therefore:

$$\mathbf{P_1} = (C_1 + \sqrt{C_1^2 - 4C_2})/2 \tag{3.12}$$

$$\mathbf{P_2} = (C_1 - \sqrt{C_1^2 - 4C_2})/2 \tag{3.13}$$

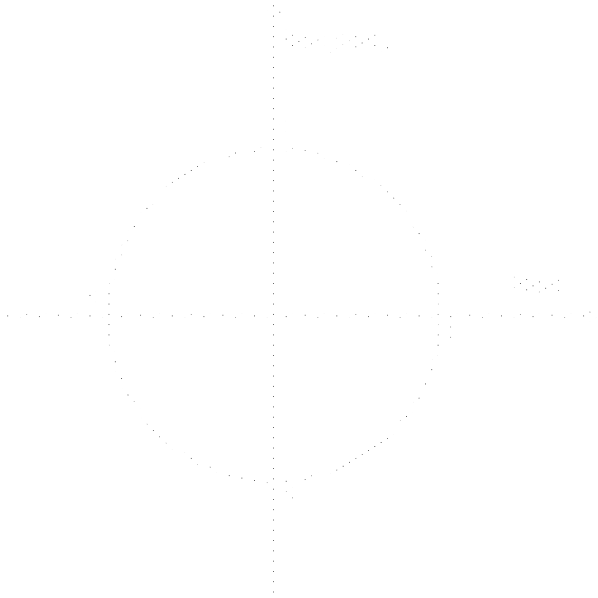


Figure 3.10: The unit circle

In this case we need to have the verification of the value of P_1 and P_2, if P_1 and P_2 both have to stay outside the unit circle it means that the generated coefficients can be used inside the system. But if they are less than one or inside the unit circle, we have to make change to the coefficients in order to get the right one. In this case we just use the technique of making the division C_2 by 10 and then we can use that coefficients after this case have been made.

For the case of software simulation, because inside the mathematic operation of digital filter, we have the multiplication of coefficients to the output data $y(n)$ and the value is the type of double in the domain of $[1, 1)$ so when we decrypt it back we will lose some small information. To solve this problem we have to use the value of coefficients as the integer value. To do that the technique

inside we have used the Floor and Round function inside matlab to get coefficients as integer value. Therefore, when we have verification process we added the Floor and Round function inside.

The other case to produce chaos in our system is non-linear behavior. To get that, the overflow function and its characteristic is very information to make our system be more satisfaction and dynamic in chaos manner. So the overflow function has made the data input and the relation of one point to the other point like the figure below:

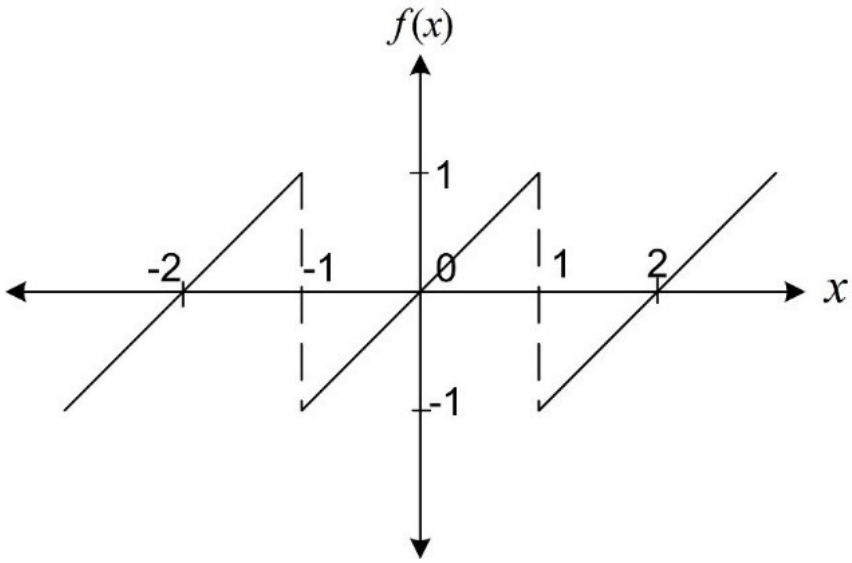


Figure 3.11: Overflow function characteristic

The both characteristics above can make our system to be chaotic cryptography in the term of digital filter and the techniques that we used inside the system can make our system to be more efficient and proficiency to the real world to again cryptanalysis.

3.3 Proposed hardware design

The final work of this project is to implement the real hardware for the proposed system. For the conduction of the work, we have used Raspberry Pi to be the controller of the work by joining execution of Python.

1. **Hardware description**:The first one is Raspberry Pi Module B is the third generation of Raspberry Pi product and it also the board that can be used with many applications and with

many functions especially it is matched with wireless LAN and Bluetooth which is the best solution of power connected design. Inside the project it is used to implement key generator and also occupied with input and output operation. Technology that we used is Python co-operated with OpenCV to conduct with data input as image. On the other hand is the part of crypto-engine. In this project we used binary operation coded in python to design the crypto-engine as encryptor and decryptor. The techniques of the work have been made to get some of the specific term or problems solving that occurs such as technique to replace the overflow function to the operation and also can reduce the error rate of the output data compared to the original one. The description below is the specifications of the product of this experimental setup:

Components	Specification
System-On-Chip(SoC)	Broadcom BCM2837
Central Processing Unit(CPU)	2 x ARM-A53, 1.2GHz
Graphics Processing Unit(GPU)	Broadcom VideoCore IV
Random-access memory(RAM)	1GB LPDDR2(900MHz)
Network	10100 Ethernet, 2.4GHz 802.11n wireless
Bluetooth	BluetoothSD
GPIO	40-pin header,populated
Ports	HDMI 3.5mm analogue audio-video jack, 2 x USP 2.0 Ethernet Camera serial Interface(CSI), Display Serial Interface(DSI)

Table 3.1: The specification of Raspberry Pi

Anyways inside the project we use only some specific components which is affect to our project such as operation unit and some ports like camera port because it is connected to its plug in camera of raspberry pi and all the output is monitored by the its screen. About the memory card is made of 16 GBs to operate with operating system and running the application

of proposed system.

2. **Hardware design**: Key generator in side Raspberry Pi, data operation and preparation station provides have been made as normal conduction of IIR filter in second order with the multiplication and addition of double number to get the appropriate results with the unstable condition verification and the output is the binary 8 bits number in order to work out with the main engine. The architectures below are the design of the proposed solution both IIR and FIR shown respectively:

Figure 3.12: IIR Filter in hardware design

Each structures of hardware design is made by working out with binary operation and the technique that we used we can cover the overflow function. Inside encrypt engine, the process is made up by using XOR, AND and OR operations. The 8 bits encryptor has been built like show in Figure above.
Step to design:

- Difference equation in use
  $\mathbf{y(n)} = x(n) + C_1 y(n-1) + C_2 y(n-2)$
- Determine the initialed value $y(1) = 0.6135$, $y(2) = -0.6135$

- Determine the input format as double inside the domain of $[-1, 1)$. Therefore, it can be represented by x.xxx xxxx
- For Coefficients from key generator is formed as 8 bits and concatenate with other 2 bits so it is formed as xxx.xxx xxxx

As the input has been used with 10 bits values so for the output we have to reduce or truncate 2 bits out to get as 8 bits as input data [6].

For the multiplication process the results this operation contains of 20 bits so we capture only the effective 10 bits to make the next operation.

Only the last 10 bits are selected to do next operation

$$111000...1 + 01010...0 = 10\mathbf{100...1}$$

Only the last 8 bits are capture to be the results.

As it has been used the multiplication of formula of 10 bits time by 10 bits so the results will get 20 bits but it is used only 10 bits. So the region which is used is M_1 (19:10) and same case with M_2. The captured bits are the effective block that can make change the data and can cover the plaint data back.

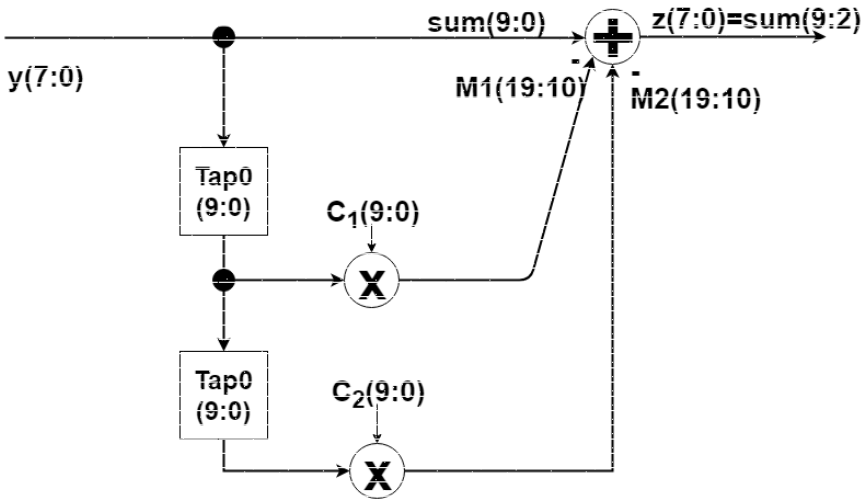


Figure 3.13: FIR Filter in hardware design

The inverse process of encryption by IIR 2nd order filter is operated by FIR 2nd order filter. For the condition and operation with input and output is the same as the encryption process. To reach that operation, 2's complement technique in order to make the inverse process of the IIR.
Step to design:

- Difference equation in use

  $\mathbf{\mathfrak{Z}(n)} = y(n) - C_1 y(n-1) - C_2 y(n-2)$

- Determine the initialed value $y(1) = 0.6135$, $y(2) = -0.6135$

- Determine the input format as double inside the domain of $[-1, 1)$. Therefore, it can be represented by x.xxx xxxx
- For Coefficients from key generator is formed as 8 bits and concatenate with other 2 bits so it is formed as xxx.xxx xxxx

The output of the decryptor is the plaintext of 8 bits value for each intensity. The same case of IIR filter, the multiplication operation will produce the 20 bits output from the system so the usable value is truncate into 10 bits by getting only M_1(19:10) and M_2(19:10). To return into the real value y equals to summation of those bits. And last 8 bits will be selected to be the results.

Chapter 4

Results and Discussion

This chapter introduces the results of two proposed structures to illustrate the different between both of them. and it is also included the result of hardware conduction of this system too. The results is divided into two parts different one is the cryptography which is focus on overall overview to the output and the other one is cryptanalysis.

4.1 Introduction to data input and initialed values

In this research work, the information about achievements of exploration about new architecture of chaotic cryptography which can produce high security confirmation and best performance and consists of key generator which that have efficient key sensitivity to the system has been confirm by analysis to the input and out of four multimedia data such as text, audio, image (both grayscale and color image) and video.

Text file:the string with redundant alphabet have been made to be the input of the system to make sure that our dynamic system can produce different appearance to the same input but different position in the file. The text has been used to keep the security because of nowadays the world internet applications are opened widely to get access from everywhere and the authentication is one of important security protection and in order to have double security in file text, qualified cryptography has been indorsed in this research experimentation [11].

Audio file: inside data transmission, not only the text the file as audio also need to be privacy for some terms of voice conversation in the public connection such as Internet. The small size of audio

file has been set to be the input because the best small size audio cryptography is the main concept and suitable criteria for the big size file in next step [12]. In this testing set up the whole audio has been operated for encryption and decryption not only partial technique to reach an important part. It causes the problem of complexity to work out only the important position of the file because it spent much time to find and fix up the data when we need original data back [13]. For this chaotic cryptography, the whole data has been conducted because our proposed solution can work fast with all those files.

Image file: Image is one of the data which contains high redundant intensity value among multimedia after the video file. To confirm all image categories such as grayscale (one color channel) and color image (RGB, three color channels), all of them have been used to make the experimentation. And it is also the main data for this thesis too to analyze all security confirmation.

Video file:The process of video file is the same of image processing operation. In the experimentation, the application works frame by frame and it consists difference only in the preprocessing technique.

Initialed Values: there are two main parts of initialization, firstly is the coefficients for key generator. And for the triple form consists of three key generator so there are 6 coefficients were set respectively$(C_1, C_2), (C_3, C_4), (C_5, C_6)$ such as $(2, -3), (4, -3) and (-3, 2)$. On the other hand, the single form only take a pair of coefficients to make up the system. Secondly is the initialed inputs $f(1) = 0.6135, f(2) = -0.6135$ in order to make the change to the first value of file. All the initialed condition has been confirmed about unstable condition to the stable triangle.

4.2 Experimental setup

In this experiment, there are two main set up different such as software simulation and hardware conduction. In software simulation all multimedia data have been taken to make as input. Such as below:

Text: **"This chaotic cryptography produces high security confirmation and best performance by standing as dynamic system, however it has high redundant data input such aaaabbbb"** consists of aaaabbbb which is the notification point to show the quality of system not line substitution cipher primitive or polyalphabetic cipher primitive which depends on the static operation

according to each opposition of the password.

Audio: The testing audio consists of 736 KB size and the length is 4 seconds. It is the small file and if it can confirm high security, large size also work well too.

Image: as has been mention, the gray scale and color images has been used to make experiment and there are four images for this work:

Figure 4.1: Gray scale and Color Baboon Image

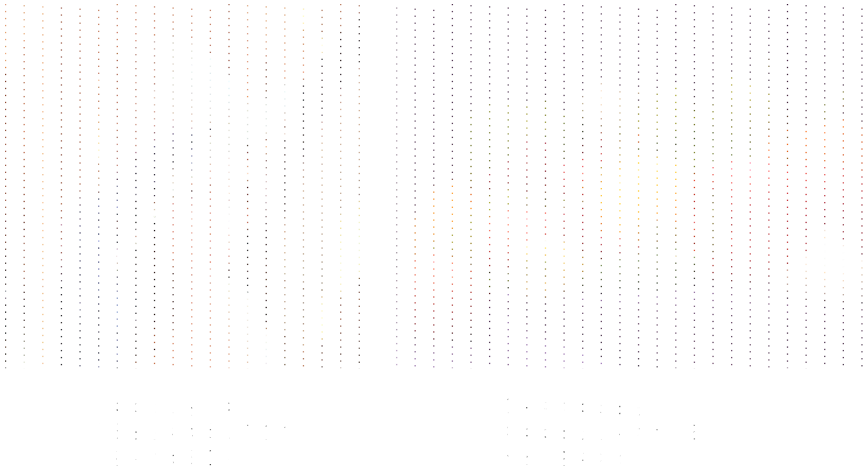


Figure 4.2: Color Lenna and Pepper Image

Video: consists of 9.6595 second duration with $width = 1280$ pixels, $height = 720$ pixels, video format RGB24,$framerate = 29.97$ and number of $frames = 289$ frames. All the kinds

of these multimedia data has been conducted with different security information exclamation. And in key generator has been set with the input of 16 character equals to 128 bits and for the triple for also the same password.

4.3 General analysis and results of cryptography

In terms of cryptography characteristics, there are some of critical points that have been shown and analysis to confirm that the proposed system is strong enough to stand in the real situation. The results of the tables below have firmed that all the properties of the system are in the standard proportion. For the single and triple structure have produced the appropriate output as the same vision overview.

Algorithms	**Key length (Char, bits)**	**Key Space**	**Time To Brute Force**
DES	7, 56	7.2×10^{16}	13 years 91 days
Proposed System	**16, 128**	$\mathbf{4.4 \times 10^{38}}$	$\mathbf{4.4 \times 10^{31}}$**years**
3DES	21, 168	3.7×10^{50}	3.4×10^{41} years
AES-192	24, 192	6.2×10^{57}	2.9×10^{47} years

Table 4.1: Key Length Analysis

According to the duration and the space of the key, our proposed system can work comfortably to the outside world. Another one is about the key sensitivity (ks) to each categories of multimedia data, in case video is considered the same as image processing. The information below shown to ensure about the key sensitivity to the system. The calculation of the value is made by the

mathematic operation below:

$$\textbf{ks} = \frac{100\%}{2 * f\_length}\left(\sum_{i=1}^{f\_length} X_1(i) + \sum_{i=1}^{f\_length} X_2(i) \right) \tag{4.1}$$

Where $X_1(i)$ and $X_2(i)$ are the value defined by

If $Cipher_file(i) == Cipher_filek(i)$ Then

$X_k(i) = 0$

Else

$X_k(i) = 1$

End

$Cipher_file(i)$ and $Cipher_filek(i)$ are the encrypted file with only one bit different of the key by increasing and decreasing one bit to the current key and operate it with the same input file. The results of key sensitivity with three different file respectively shown in the table below:

Password	**Key sensitivity ($ks(\%)$)for text encryption**	
	Single Structure	**Triple Structure**
CHAOTICCRYPTOAPB	100	100
ILOVETELECOMMUCH	100	100
1234567890987654	100	100
1234567891098763	100	100
!@#$%^&*()_+%$#R	100	100
G3$Hf43!$@$09@88	100	100

Table 4.2: Key sensitivity on Text encryption

Password	Key sensitivity ($ks(\%)$)for audio encryption	
	Single Structure	Triple Structure
CHAOTICCRYPTOAPB	100	100
ILOVETELECOMMUCH	100	100
1234567890987654	100	100
1234567891098763	100	99.7242
!@#$%^&*()_+%$#R	100	100
G3$Hf43!$@$09@88	100	100

Table 4.3: Key sensitivity on Audio encryption

Password	Key sensitivity ($ks(\%)$)for gray scale image encryption	
	Single Structure	Triple Structure
CHAOTICCRYPTOAPB	100	100
ILOVETELECOMMUCH	100	100
1234567890987654	100	100
1234567891098763	100	99.3881
!@#$%^&*()_+%$#R	100	100
G3$Hf43!$@$09@88	100	100

Table 4.4: Key sensitivity on gray scale image encryption

Password	Key sensitivity ($ks(\%)$)for color image encryption					
	Single Structure			Triple Structure		
	Lenna	Baboon	Pepper	Lenna	Baboon	Pepper
CHAOTICCRYPTOAPB	100	100	100	100	100	100
ILOVETELECOMMUCH	100	100	100	100	100	100
1234567890987654	100	100	100	100	100	100
1234567891098763	100	100	100	100	100	100
!@#$%^&*()_+%$#R	100	100	100	100	100	100
G3$Hf43!$@$09@88	100	100	100	100	100	100

Table 4.5: Key sensitivity on on color image encryption

The first reactions to the files is the overview of its original status. So it is important to transform the cipher file in cryptography system to the other view that no one can recognize what it is. The other options is its pattern, however it is transformed some of weak algorithm still keep the scratch of file to let attacked can come up with those points to get the original file.

Figure 4.3: Text encryption results

The notification of the highlighted alphabets pointed that the proposed solution stands as dynamic system. The same characters in plain text and the vision in cipher text is different. For the key sensitivity to text encryption if we change only one bit of the key, it still can't get any information from the original text. Not only is the high redundancy data, the file text also confirmed with key too when the similar input has been made. In this system is efficiently conducting in this coming point.

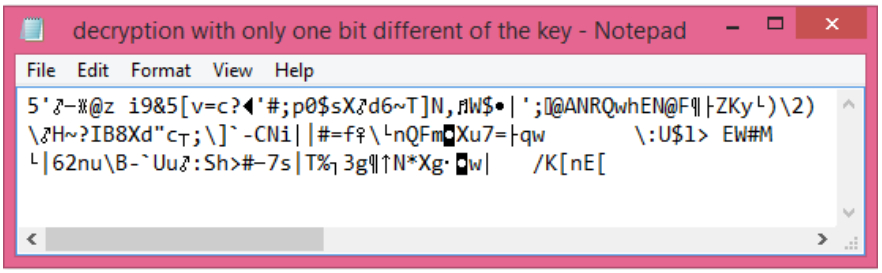


Figure 4.4: Text encryption with one bit different of the key

For the type of audio file which is in the other kind of view. It needs to be mess sound that the middle person cannot listen and know what is talked about. To show up the confirmation, the information of histogram, has been figured out with the same condition to the file text.

Figure 4.5: Original audio file and encryption results

Figure 4.6: Decrypted audio file with right and one bit different key

Working with image processing file, however it has high redundancy positions, this proposed system still can conduct efficiently and in the cipher images the patterns of the file are messy and can't recognize what it is. And for the point the same values, in the decrypted file it didn't keep with the same scratch of the shape of the image. The figures below are the results of the gray scale image and it can survive the weakness of AES.

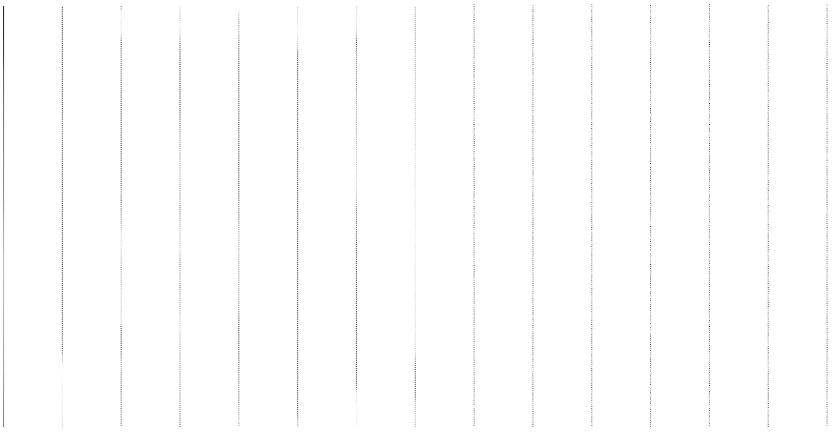


Figure 4.7: Gray scale image encryption result

When the experiment is aimed to set as the previous kind of multimedia data the results come up with the same expectation. The image still keep the same proportion to the cipher image when we tried to use the similar key to decrypt the file back. The results below shows about its outcome.

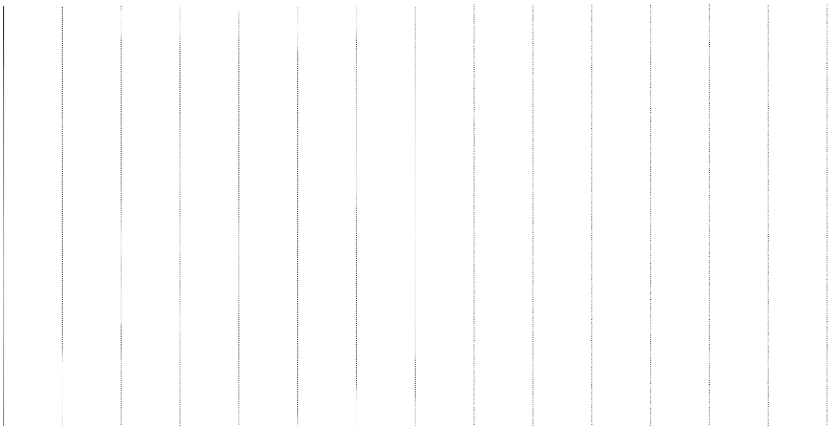


Figure 4.8: Gray scale image decryption results with right and wrong key

The histogram also can confirm the mess of cipher image and the results of the system when we try to test with the key sensitivity.

Figure 4.9: Histogram of plain image and cipher image

Figure 4.10: Histogram of decrypted images with right and wrong key

In terms of color images, the appearance of the cipher images show up as the gray scale image with point of messy. But it exists of the combination the three colors to form up those messes. In the experiment, the three file of the color images gave the same expectation result such as the figures below. It is the results of Pepper.jpg image and other two are the same results.

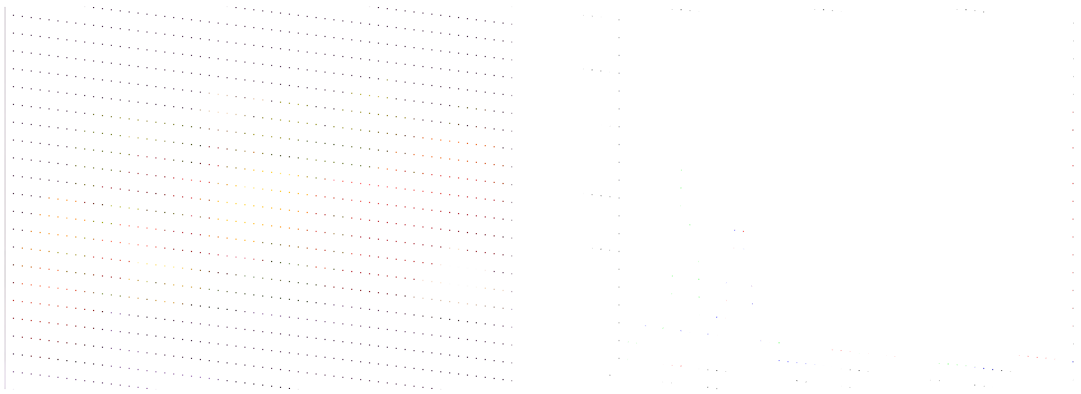


Figure 4.11: The original color image and its histogram

Figure 4.12: The encrypted image and its histogram

To decrypt back the file, the results has been made to be seen as the original file but if we compare the intensity value it occurs 0.03 % of error in the whole comparison. But in case taking only 10 digits of the double number of intensity the error rate is 0%. But in the operation of hardware that we will work out with binary structure so it doesn't cause any problem of error because we worked out with 8 bits operation of intensity value. In case of different one bit of the key has been used the results still come up with nothing different to the results gray scale image.

Figure 4.13: The decrypted image with the wrong key and its histogram

For the video encryption results has been made up and the results shown as the sequences of the images and each images has to be separated into three channels differently and for the results from decryption process is gotten the same as color image decryption. It is different only it is the combination of sequence of images. In this work we were working on only non-audio video:

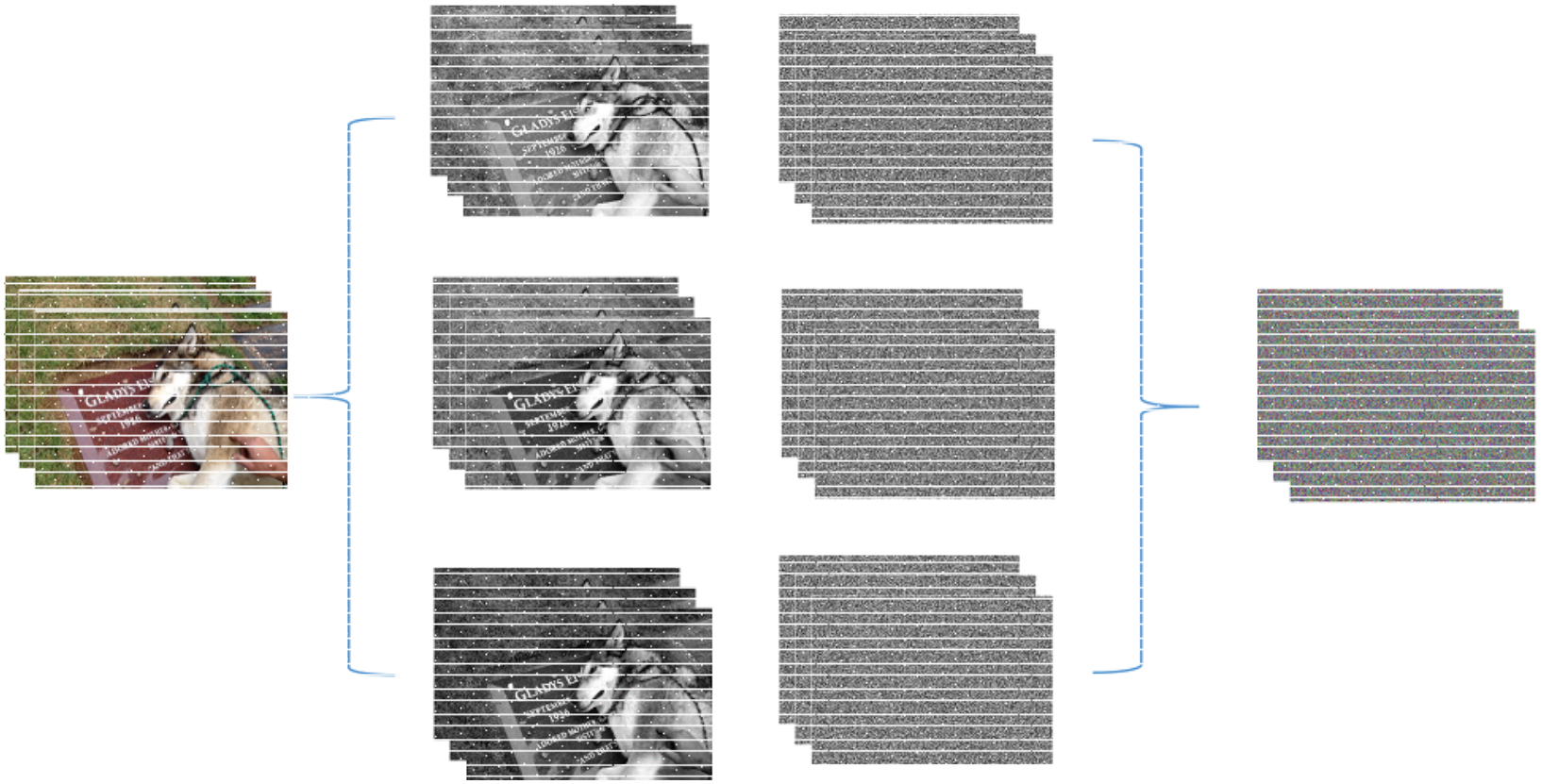


Figure 4.14: The results of video encryption

4.4 Results of cryptanalysis

Several cryptanalysis criteria to evaluate the security confirmation of the proposed system. Those results have made sure that this system can get through with all standard analysis properties which all encryption methods have to have.

Information Entropy ($H(s)$):The notification of the increasing rate of entropy much as much possible is the best solution for against the entropy analysis. The high value of reliable pseudo-random number which the original point can appear in the cipher file can make those information to be mumbled. The maximum value of high value of entropy is 8 to be the most murmur for the cipher file based on mathematic theory operation [14]. The system information entropy results of each type of data were calculated by the equation below and the results shown consequently after that.

$$\mathbf{H(s)} = \sum_{i=1}^{2^n-1} P(S_i)\log_2 \frac{1}{P(S_i)} \tag{4.2}$$

Where $P(s_i)$ is the probability of the value inside the whole file.

Information Entropy Status	**Multimedia data type**			
	Text	**Audio**	**Image**	
			Gray scale	**Color**
Plain_file_Entropy	4.1725	3.4201	7.2742	7.3812
Cipher_file_Entropy	6.8952	4.9605	7.9682	7.9710
Increasing_rate	2.7227	1.5404	0.6940	0.5898

Table 4.6: Entropy analysis of single proposed structure

Information Entropy Status	Multimedia data type			
	Text	Audio	Image	
			Gray scale	Color
Plain_file_Entropy	4.1725	3.4201	7.2742	7.3812
Cipher_file_Entropy	6.7939	4.9865	7.9978	7.9982
Increasing_rate	2.6214	1.5664	0.7236	0.6170

Table 4.7: Entropy analysis of triple proposed structure

Furthermore, the next criteria about information privacy is the relationship between the original input and output from the encryption process. It is commonly called **Correlation coefficient**. In the case that the plain file and cipher file are closed to each other correlation coefficient equals to 1 it means that our cryptography system is not suitable for keeping data security. The results shown that the corresponding system is qualified enough to make the hidden information is pretty far different from the original input.

Structure	Multimedia data type			
	Text	Audio	Image	
			Gray scale	Color
Single Structure	-0.0300	0.0029	0.0003	-0.0004
Triple Structure	-0.1237	0.0013	-0.0002	0.0007

Table 4.8: Correlation of original file and cipher file

In case of image operation, there are three direction that it must be considered. There are Horizontal, Vertical and Diagonal correlation that the system need to guarantee the relation of each direction within each other. The value of each direction must keep the same criteria as the relationship like file text and audio, otherwise, it is considered as inappropriate system.

Correlation Direction	System Structure and Multimedia data			
	Single Structure		Triple Structure	
	Gray scale	Color	Gray scale	Color
Horizontal	0.0011	-0.0027	0.0033	0.0003
Vertical	0.0010	0.0011	-0.0011	0.0036
Diagonal	0.0010	-0.0010	-0.0004	0.0016

Table 4.9: Correlation of all directions of cipher image

For the appearance of each direction of correlation of the image, the gray scale and color image also shown as the same view. On the other hand, both structures of the proposed solutions provide the same vision too.

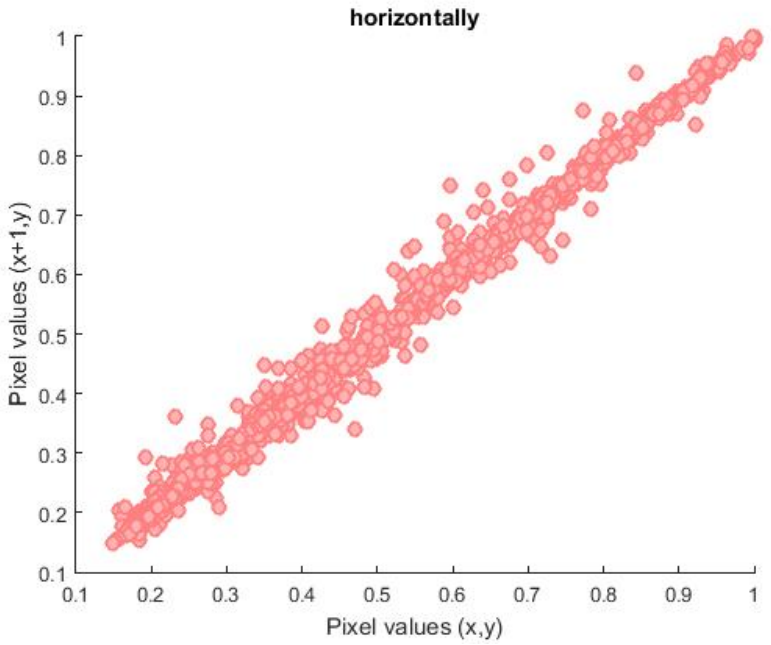


Figure 4.15: Original image correlation in horizontal direction

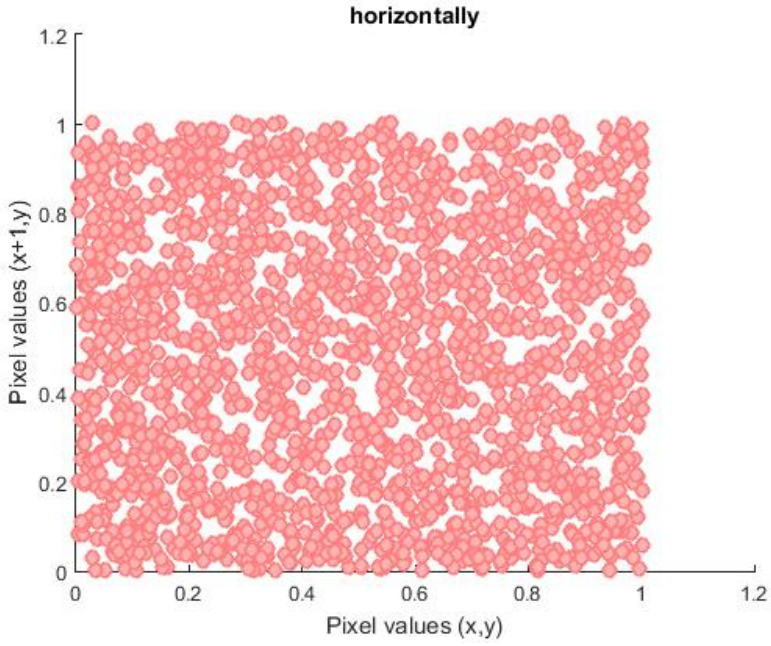


Figure 4.16: Cipher image correlation in horizontal direction

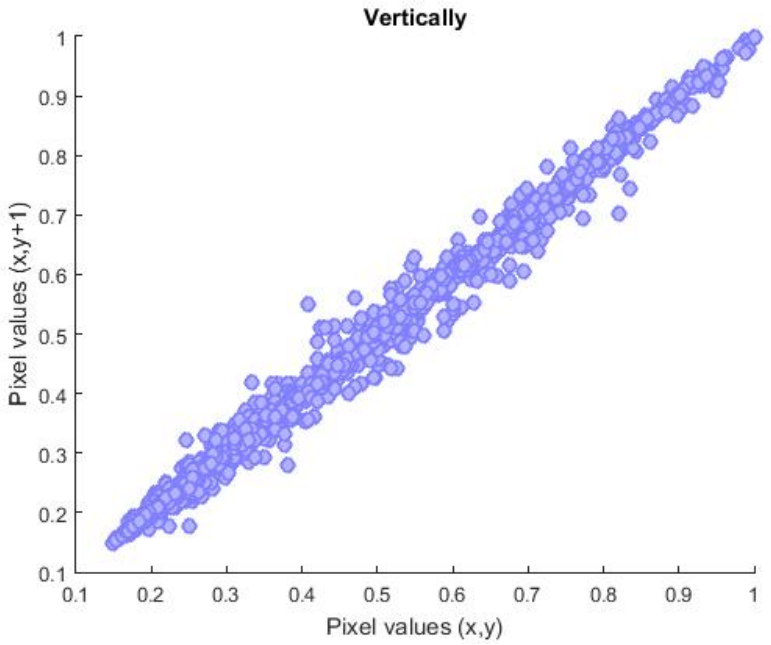


Figure 4.17: Original image correlation in vertical direction

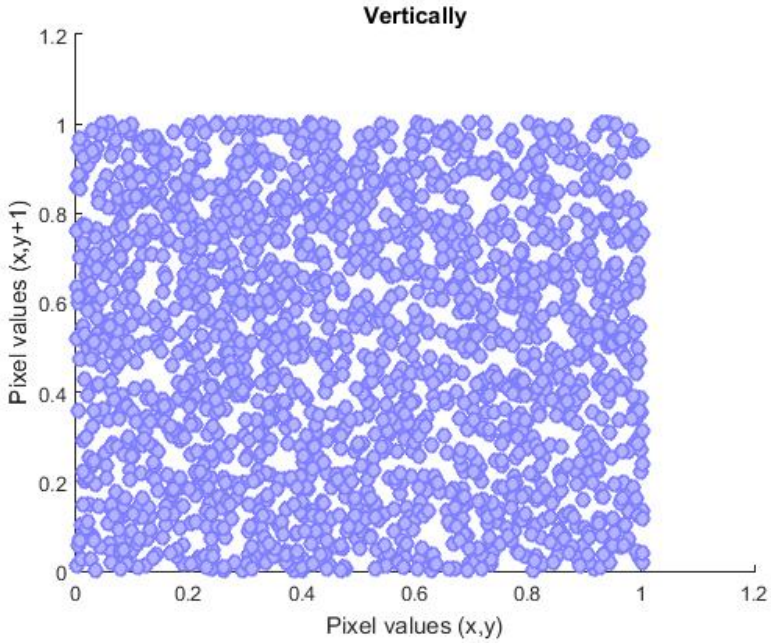


Figure 4.18: Cipher image correlation in vertical direction

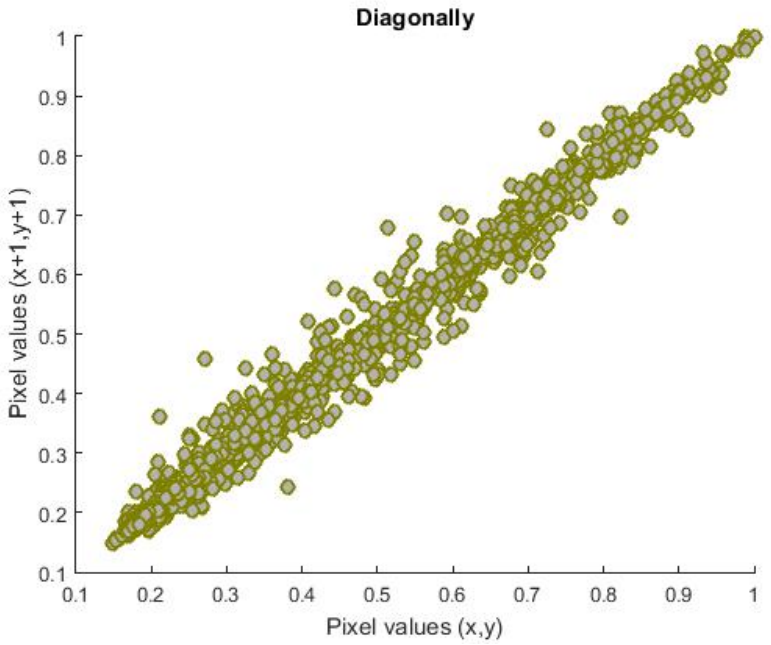


Figure 4.19: Original image correlation in diagonal direction

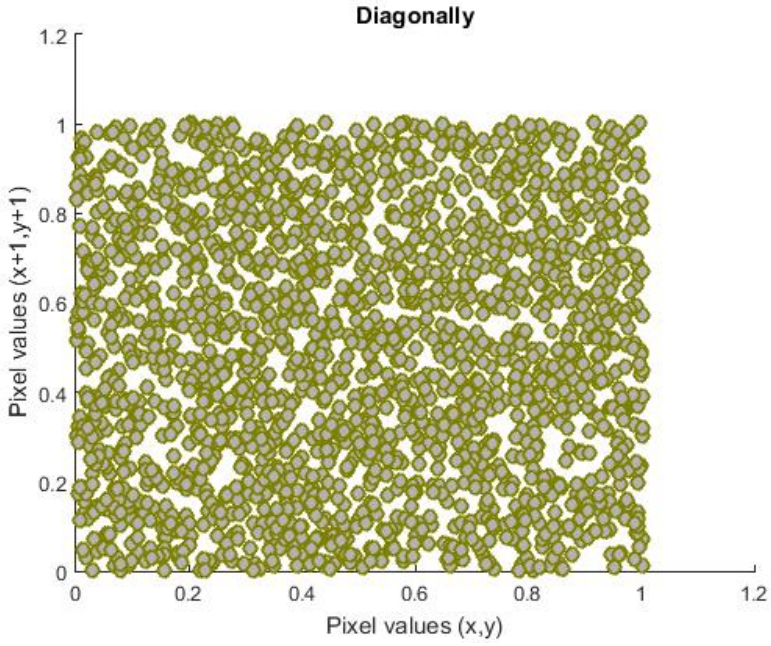


Figure 4.20: Cipher image correlation in diagonal direction

In image processing, there are other value that it has to be confirmed in order to test the plain file sensitivity inside the system. To against the differential attack in cipher file resistance, **the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI)** are commonly

analyzed. The mathematic equation to get values and the results shown respectively in the following table.

$$\textbf{NPCR} = \frac{100\%}{\text{Im}g\_size}(\sum_{i=1}^{n}\sum_{j=1}^{m} X(i,j)) \tag{4.3}$$

$$\textbf{UACI} = \frac{100\%}{\text{Im}g\_size}(\sum_{i=1}^{n}\sum_{j=1}^{m} \frac{|C_1(i,j) - C_2(i,j)|}{Intensity\_level}) \tag{4.4}$$

A bipolar array $X(i,j)$ is defined depends on the values of C_1 and C_2 which are the values of cipher image before and after we changed one pixel in plain image.

If $C_1(i,j) == C_2(i,j)$ Then

$X(i) = 0$

Else

$X(i) = 1$

End

Plain file sensitivity	**System Structure and Multimedia data**			
	Single Structure		**Triple Structure**	
	Gray scale	**Color**	**Gray scale**	**Color**
NPCR	100%	99.65%	100%	100%
UACI	33.39%	33.30%	33.43%	33.31%

Table 4.10: NPCR and UACI of the image file

The last value is about **Peak Signal-to-Noise Ratio (PSNR)**. The analyzing value is due to the mean square difference between the encrypted image and decrypted image. The original value of PSNR of two images if they are similar is around 30 db to 50 db. For the encryption file if it is less as much as possible, it means that the encrypted file is high security confirmation information. The mathematic equation represented this point is shown as the following.

$$\textbf{PSNR} = 10\log_{10}(\frac{\text{int}ensity\_level^2}{MSE}) \tag{4.5}$$

$$\textbf{MSE} = \frac{1}{img\_size}(\sum_{i=1}^{n}\sum_{j=1}^{m}(img_1(i,j) - img_2(i,j))^2) \tag{4.6}$$

Where $img_1(i,j)$ is the decrypted image and $img_2(i,j)$ is the encrypted image of the system.

Plain file sensitivity	**System Structure and Multimedia data**			
	Single Structure		**Triple Structure**	
	Gray scale	**Color**	**Gray scale**	**Color**
PNSR(db)	8.3149	7.6026	7.7755	7.6033

Table 4.11: Results of PNSR analysis

The proposed structure, both provided with high security confirmation, while DES consists with weak key conduction and 3DES is made to ensure with the key but the performance is slow because of three times compare to DES [15]. However the length of the key can solve the problem from some attack, it still faces with meet-in-the-middle attack. The security comparison is shown as below [16]:

Parameters	**Proposed structure**	**Data Encryption Standard**
	(Average)	**(Average)**
PNCR	100	99.6643
PSNR(db)	8.166	7.6057
UACI	33.34	51.2491

Table 4.12: Comparison results with DES

4.5 Results of hardware implementation of single form structure

As in hardware, the system runs in binary operation (8 bits), the input and the output from the decryption process, it exists with no error between both of them. Not like in software simulation, the error occurs with the last 10th digits of each intensity value. The result also can provide the same as software's output in all terms, security analysis and sensitivity. The results below shown as the overview output from the system:

Original		**Encryption**		**Decryption**	
(Decimal)	**(Binary)**	**(Decimal)**	**(Binary)**	**(Decimal)**	**(Binary)**
254	11111110	225	11100001	254	11111110
42	00101010	183	10110111	42	00101010
213	11010101	76	01001100	213	11010101
74	01001010	32	00100000	74	01001010
98	01100010	234	11101010	98	01100010
125	01111101	83	01010011	125	01111101
164	10100100	221	11011101	164	10100100
121	01111001	198	11000110	121	01111001
3	00000011	179	10110011	3	00000011
244	11110100	85	01010101	244	11110100

Table 4.13: Hardware implementation results

Figure 4.21: Hardware image encryption results

Chapter 5

Conclusions and Recommendations

Inside this section is to conclude to the overall of the results and performance of the proposed system. and also provide some suggestions to the future work for completing the whole efficient system to secure the data in current needs.

5.1 Conclusions

In this research work, the chaotic crypto-system consists of two main parts different, one is key generator and other one the crypto-engine for encryption and decryption process.

For key generator, the architecture is composed by three IIR filter in order to generate the output which is the coefficients for the main engine. It has to get input as 16 characters equals to 128 bits and the second order digital filter consists of two initialed coefficients and other two initialed value to make change the first input data if those two are zero the first index of data will keep the same. The output named as coefficients are verified to be outside the stable triangle in order to make our system to unstable system. But for the output from first filter until the last filter has been made change by swift last three value of the output to the front to be input for the next filter.

Other one is crypto-engine, the encryptor is constructed by one IIR filter for the single form and three IIR filters for the triple form. The system get the coefficient from the key generator and operated with two initialed value to work out with the input data. The combination of that two signal input and system produced the output which is the cypher file that contain high security and accuracy. And for the inversing process which is decryptor is constructed by FIR filter and the

number of the filter is depending on the form of the system whether it is single form or triple form. The proposed solution is able to work out with all kind of data and give the appropriated results. The single form is the suggested one because it consisted high security and performance compared to the triple form.

5.2 Recommendations

The next work is we would like to but the complete system which consists of the compressor and decompresser to merge into this system in order to speed up the process and this encryption technique to make it to be the best cryptography system ever.

Figure 5.1: The complete system of lightweight cryptography

For the compression and decompression is suggested to use effective method such as Wavelet transform that can denoise an compress the data after that we input the new data into our proposed system.

Inside the process of hardware implementation, there are two processes which can be executed in parallel because those two block of operations are independent to each other.

Therefore, to enlarge the performance of the proposed system the parallel running is the best way to process structure. On other hand, because it works out with frame by frame so for the video

processing can be paralleled to number of the frame according to the processing unit in use of the product.

References

[1] S. Lian, Multimedia Content Encryption: Techniques and Application, CRC, 2008.

[2] M-S. Liu, Y. Zhang, J. li, "Research on Improving Security of DES by Chaotic Mapping" IEEE, Proceedings of the 8th International Conference on Machine learning and Cybernetics, Baoding, pp. 12-15, Jul 2009. K. Elissa. *http: 10.1109ICMLC.2009.5212554*

[3] B.J. Saha, Arun, K.K. Kabi and C. "A Robust Digital Watermarking algorithm using DES and ECC in DCT Domain for Color Images" 2014 international Conference on Circuit, Power and Computing Technologies [ICCPCT]. *http: 10.1109ICCPCT.2014.7054975*

[4] L. O. Chua and T. Lin, "Chaos in digital Filters", in IEEE Trans. Circuits System., vol. 35, no. 6, pp. 648-658, June 1998. *http: 10.110931.1802*

[5] H. H. Abdlrudha and Q. Nasir, "Low Complexity High Security Image Encryption Based on Nested PWLCM Chaotic Map" in 6th International Conference for Internet Technology and Secured Transactions (ICITST), Abu Dhabi, United Arab Emirates,2011. *http:ieeexplore.ieee.orgstampstamp.jsp?tp=&arnumber=6148381*

[6] N. Ronnaronglit, S. Chivapreecha and T. Sato, "An Improved Digital Image Encryption Using Chaos in Digital Filter", 2015 International Symposium on Multimedia and Communication Technology, 23-25, 2015.

[7] M. George and A. Ioannis, "Cryptography with chaos", in Proceeding 5th Chaotic Modeling and simulation International Confference, Athens Greece, 2012. *http:www.cmsim.org/images/1_CHAOS2012_Proceedings_Papers_MP.pdf*

[8] D. R. Frey, “Chaotic Digital Encoding”, in IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, Volume: 40, Issue: 10, Oct 1993. *http: 10.1109/82.246168*

[9] R. Chanathip, D. Xaysamone,K. Khamphong, P. Nounchan and C. Sorawat, “Chaotic Encoder-Decoder on FPGA for Crypto System” in Signal and Information Processing Association Annual Summit and Conference (APSIPA), Siem Reap, Cambodia, 2014 Asia-Pacific.*https: 10.1109/APSIPA.2014.7041740*

[10] P. Reatrey, C. Sorawat and P. Jaruwit, “A New Key Generator for Data Encryption Using Chaos in Digital Filter” in Control and System Graduate Research Colloquium (ICSGRC), 2017 IEEE 8th, Shah Alam, Malaysia , 4-5 August 2017. *https: 10.1109/ICSGRC.2017.8070574*

[11] A. Ahmad and B. Hawashin, “A Secure Network Communication Protocol Based on Text to Barcode Encryption Algorithm” in International Journal of Advanced Computer Science and Applications, Vol. 6 No. 12, 64-70, 2015. *https:pdfs.semanticscholar.org61cdec74b32600d6d9876928bd1919460dcb3c97.pdf*

[12] P. Pitale, A. Pateria, P. Sings and N. Golchha, “Audio based Secure Encryption and Decryption”, in International Journal of Computer Application (0975-8887): Application of Computers and Electronics for the Welfare of Rural Masses(ACEWRM),2015. *https:pdfs.semanticscholar.orgc72fe27ab00ce5d61253c66658fb380794fd5af8.pdf*

[13] R. A. Gandhi and A. M. Gosai, “A Study on Current Scenario of Audio Encryption”, in international Journal of Computer Applications (0975-8887), Vol 116-No.7,2015. *https:pdfs.semanticscholar.org3121176b09970d82d7f38f9e1b8ea6b3c8946b6d.pdf*

[14] C. Shannon, “Communication theory of secrecy systems”, Bell system Technical Journal 28:656-715,1949. *https:10.1002j.15387305.1949.tb00928.x*

[15] M. Ebrahim, S. Khan and U. B. Khalid, “Symmetric Algorithm Survey: A Comparative Analysis”, International Journal of Computer Applications (0975-8887) Volume 61-No. 20, January 2013. *http:arXiv:1405.0398*

[16] S. Soni, H. Agrawal and M. Sharma, " Analysis and Comparison between AES and DES Cryptographic Algorithm", IJEIT 2017. *http:www.ijeit.comvol%202Issue%206IJEIT1412201212_64.pdf*

AUTHOR BIOGRAPHY

Author : Mr. Reatrey PICH

Degree : Master of Engineering

Date of Graduation :

Date of Birth : 24^{th} February 1993

Place of Birth : Banteaymeanchey, Cambodia

Undergraduate and Graduate Education:

Master of Engineering in Computing in Engineering Systems,
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand, 2018

Bachelor degree in Information and Communication Engineering,
Institute of Technology of Cambodia, Phnom Penh, Cambodia, 2016

Major: Computing in Engineering Systems

Presentations and Publications:

- Paper's name : **"A New Key Generator for Data Encryption Using Chaos in Digital Filter"** 04-05, August, 2017, ICSGRC 2017, Grand Blue Wave Hotel, Shah Alam, Malaysia
- Paper's name : **"A Single, Triple Chaotic Cryptography Using Chaos in Digital Filter and Its Own Comparison to DES and Triple DES"** 07-10, January, 2018, IWAIT 2018, Chiang Mai, Thailand

A New Key Generator for Data Encryption Using Chaos in Digital Filter

Reatrey Pich
International College
King Mongkut's Institute of Technology
Ladkrabang, Bangkok 10520, Thailand
Email: reatrey.pich@gmail.com
/59610026@kmitl.ac.th

Sorawat Chivapreecha
Department of Telecommunication
Engineering, Faculty of Engineering
King Mongkut's Institute of Technology
Ladkrabang, Bangkok 10520, Thailand
Email: sorawat@telecom.kmitl.ac.th

Jaruwit Prabnasak
International College
King Mongkut's Institute of Technology
Ladkrabang, Bangkok 10520, Thailand
Email: kpjaruwi@kmitl.ac.th

***Abstract*—The presented work of this paper is to propose the implementation of chaotic crypto-system with the new key generator using chaos in digital filter for data encryption and decryption. The chaos in digital filter of the second order system is produced by the coefficients which are initialed in the key generator to produce other new coefficients. Private key system using the initial coefficients value condition and dynamic input as password of 16 characters is to generate the coefficients for crypto-system. In addition, we have tension specifically to propose the solution of data security in lightweight cryptography based on external and internal key in which conducts with the appropriate key sensitivity plus high performance. The chaos in digital filter has functioned as the main major in the system. The experimental results illustrate that the proposed data encryption with new key generator system is the high sensitive system with accuracy key test 99% and can make data more secure with high performance.**

Keywords—cryptography; chaos; chaotic encryption; digital filter; key generator

I. INTRODUCTION

With recent high technology, the innovation of multimedia and information communication, data is connected in terms of large public infrastructure of network. In order to conduct security and privacy during data processing before the transmission or distribution, there are many techniques composed by different algorithms which have been used such as DES, 3DES, AES and chaotic encryption. In addition to the point of chaotic cryptography using directly in multimedia, N. Ronnaronglit et al., [1] mentioned that the result of experiment can improve the security, performance when compared with other algorithms like DES or AES. Furthermore, H. Abdlrudha and Q. Nasir [2] reported that the chaotic system has become the good password system in case using the parameters and initial value as a key. Therefore, the key has stood as the main point in the system especially in the symmetric key encryption algorithm. K. N. Prasetyo et al., [3] have shown that this kind of algorithms quality depends on the secrecy of the key. However, some parts of algorithm of existing chaotic algorithm and non-chaotic algorithm still provide the high complexity in term of key generating in order to reach the proper key which is the main causes of security issue.

The objective of this research work is to orient the chaotic key generator to achieve the sensitive crypto-system. New key generator has been designed by containing the connection of three infinite impulse response (IIR) filters and it is responsible to produce the appropriate coefficients in order to perform the cryptography processing.

This paper is organized as the follow: Section II briefly introduction to the chaos in digital filer and its application for data encryption. Section III shows the proposed key generator, the validation and effectiveness of the proposed system are given in the section IV. Finally, the conclusion will be described in the section V.

II. CHAOS IN DIGITAL FILTER

M. George and A. Ioannis [4], chaotic cryptography is known as a dynamic system that is followed by the mathematical equation such as in Cat map and Baker map which are used for the confusion portion. Otherwise, digital filter has been used under the conditions of unstable and non-linear system instead of chaos-based algorithm by cooperating with the overflow nonlinearity function in order to make the chaos as proposed by [5-6]. Chaos in digital filter, IIR filter functions as an encryptor while FIR is its inverse to work as decryptor.

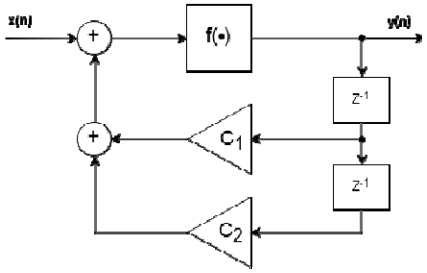


Fig. 1. The second order IIR digital filter structure.

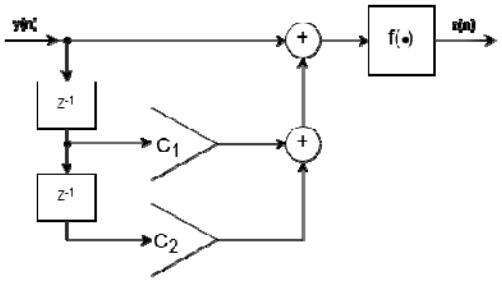


Fig. 2. The second order FIR digital filter structure.

For representing Fig.1 into the system, mathematical equation which is formed as the difference equation shown in (1) is used to cover the operation of IIR filter. The transfer function and overflow function are also shown consequently as (2) and (3). Having put the overflow function into main equation of the system, the difference equation can be formed as (4).

$$y(n) = x(n) + C_1 y(n-1) + C_2 y(n-2) \quad (1)$$

$$H(z) = \frac{y(z)}{x(z)} = \frac{1}{(1 - C_1 z^{-1} - C_2 z^{-2})} \quad (2)$$

$$f(x) = [(x+1) \bmod 2] - 1 \quad (3)$$

$$y(n) = f\{x(n) + C_1 y(n-1) + C_2 y(n-2)\} \quad (4)$$

In order to perform the decryption process the structure of FIR filter in Fig. 2 has been made as the inverse from of IIR filter in Fig.1, the equation has been shown in (5). And in order to reach the same output as plaintext overflow function (3) is still used in the operation but different location in the system. In this case transfer function has been form as (6). Same as IIR filter case, the difference equation can be the other form when it is included the overflow function like (7).

$$z(n) = y(n) - C_1 y(n-1) - C_2 y(n-2) \quad (5)$$

$$H(z) = \frac{z(z)}{y(z)} = 1 - C_1 z^{-1} - C_2 z^{-2} \quad (6)$$

$$z(n) = f\{y(n) - C_1 y(n-1) - C_2 y(n-2)\} \quad (7)$$

Both cases in the encryptor and decryptor as the whole system we need the overflow function for making input and output to work in the nonlinear system. The characteristic of overflow nonlinearity function has been shown in Fig. 3.

K. Kutzer et al., [7] has confirmed that in order to make certain that our system is unstable system and generate chaotic output, the coefficient must be at least one is outside the stability triangle or be larger than unity as shown in Fig. 4.

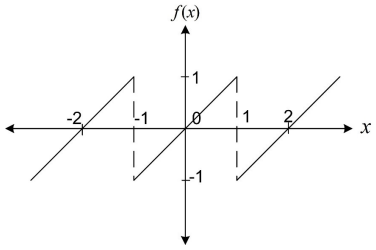


Fig. 3. The characteristic of overflow function.

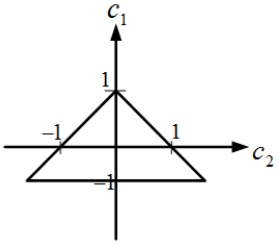


Fig. 4. The stability triangle.

III. The Proposed Key Generator System

The whole crypto-system is consisted of two main parts. One is private key generator and other one is operating system which is known as encryptor and decryptor. The private key generator functions to make the coefficients C_1 and C_2 from the input of password 16 characters and other coefficients as the initial value. Password 16 characters is alphanumeric represented by P1P2P3...P16, then it has been normalized to be input of the system with the condition of [-1, 1).

The proposed system of private key generator contains of three IIR filters the same or it is possible to say that one IIR filter looping three times in case of software simulation/implementation. The output of the first filter must be the input of second filter and then the second output will be the input of the third filter. All output must be shifted three value first before becomes the input to the other filter. On the other hand, the coefficients produced can't make system more sensitive. Otherwise, output which is chosen to be the coefficients of the encryption system is the last two indexes with the verification to the stability triangle. Only coefficients that can make secrecy in the nonlinear system so both C_1 and C_2 must at least one outside the triangle. The process of key generator has been shown in the Fig. 5 and the process how it works in the sense of software simulation/implementation is shown in Fig. 6.

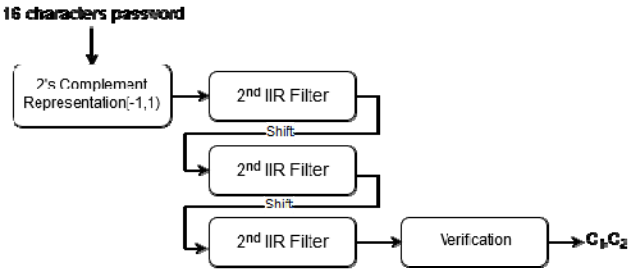


Fig. 5. The block diagram of new key generator.

As the output of key generator consist of 16 values so C_1 and C_2 will take from the last values of output 15^{th} and 16^{th} consequently, in the reason of related connection from the first value to the last one. In order to use C_1 and C_2, both of them must respect the rule of stable triangle of non-linear system.

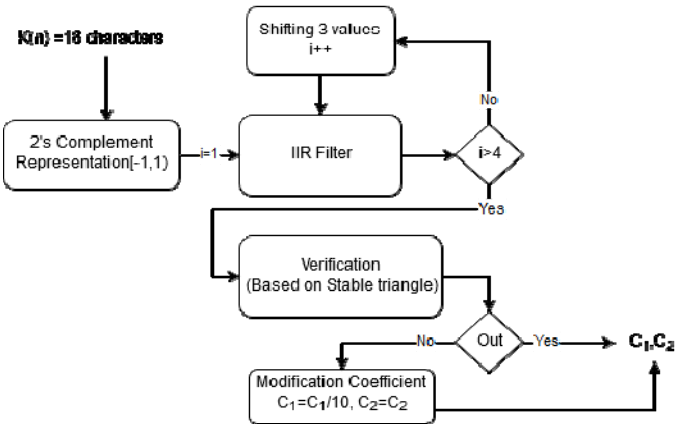


Fig. 6. The workflow of new key generator.

The whole structure that can be used for simulation has been shown in Fig. 7. For the 2's complement representation is not different from key generator that is used to be the technique to convert original input to be the suitable input in the system. As it is known that the input in chaotic system implemented by digital filter must be in range of [-1, 1).

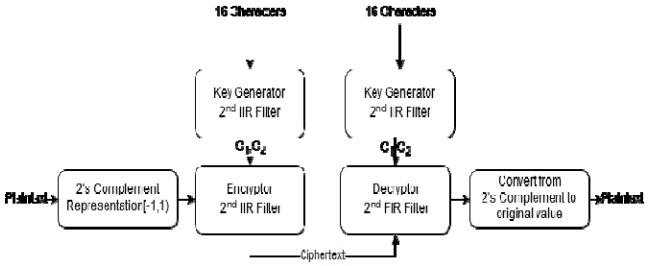


Fig. 7. The whole structure of crypto-system.

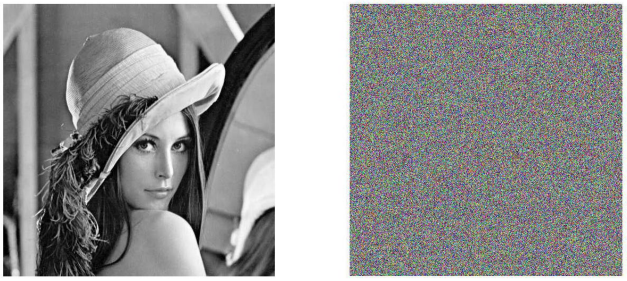
IV. THE EXPERIMENTAL RESULTS

The functionality of the proposed system can work on all multimedia data such as text, audio, image and video. Otherwise, in this paper has shown the experiment on the gray scale digital image. To operate in the system, the input has to be converted to 1 dimensional array and rearrange again to get the original output. The results of experiment have been simulated in MATLAB. The input of encryptor shown in Fig. 8 (a) and its output is in Fig. 8 (b). When using the same private key in both encryptor and decryptor, the result has been shown in Fig.9 (b) and Fig.9 (a) is the output of decryptor when using the different password of 16 characters.

A. Key Space, Key Sensitivity and Plaintext Sensitivity

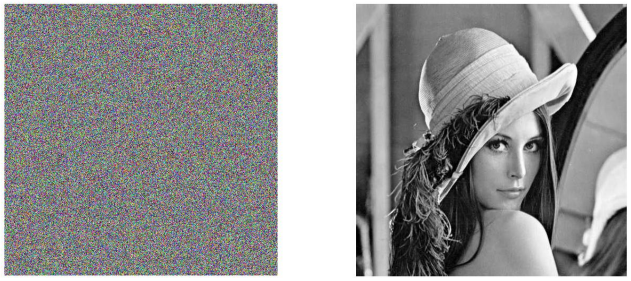
There are many algorithms for crypto analysis. Among of them, brute force has been known widely one. In the system private-key as password input contains 16 characters represented 8 bits for each, so totally there is a private-key space of 128 bits to be used. In this condition, it is greater enough if we compare to Blowfish-32 or 56 bits DES. According to brute force calculator, the processing speed it uses is 160,806k per second [8]. Therefore 128 bits private-key space is qualified enough for our crypto-system to prevent the brute force attack. The time for brute force use to operate in each key space has been shown in Table I.

In order to measure the key sensitivity, the crypto-system must be sensitive with the small change of input private-key. For example in encryptor, we use this private-key "ILOVETELECOMMUCH" to be the input password then we make a small change to it like "ILOVETELECOMMUCI" to use in the decryptor. With the difference of the small change, the decryption can't extract any information to the same or similar to the plain-image.



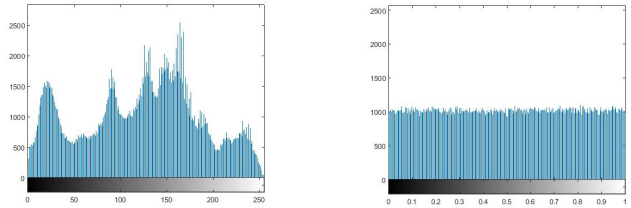
(a) Original image (b) Encrypted image

Fig. 8. Image before and after encryption.



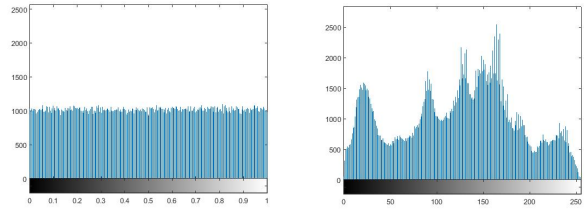
(a) Decrypted image with wrong key (b) Decrypted image with right key

Fig. 9. Decryption with different and same key.



(a) Histogram of original image (b) Histogram of encrypted image

Fig. 10. Histogram of image before and after encryption.



(a) Histogram with wrong key (b) Histogram with right key

Fig. 11. Histogram of decryption with different and same key.

TABLE I. KEY SPACE ANALYSIS

Key Length (bits, Char)	Algorithm	Key Space	Time To Brute Fore
32, 4	Blowfish-32	4.3×10^{9}	8 minus 7secs
57, 7	DES	7.2×10^{16}	13 years 91 days
112, 14	-	5.2×10^{33}	4.9×10^{27} years
128, 16	AES-128, Proposed system	4.4×10^{38}	4.4×10^{31} years
168, 21	3-DES	3.7×10^{50}	3.4×10^{41} years
192, 24	AES-192	6.2×10^{57}	2.9×10^{47} years
256, 32	AES-256 Blowfish-256	5.8×10^{64}	1.9×10^{63} years

To denote the key sensitivity the equation in (8) will be used. If the system is sensitive the *Ks* must greater than 50% as many as better.

$$Ks = \frac{100\%}{2MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} K_1(i,j) + \sum_{i=1}^{M}\sum_{j=1}^{N} K_2(i,j)\right) \quad (8)$$

where $K_1(i,j)$ and $K_2(i,j)$ are defined by

$$K_k(i,j) = \begin{cases} 0 & \text{if } F(i,j) = F_k(i,j) \\ 1 & \text{if } F(i,j) \neq F_k(i,j) \end{cases} \quad (9)$$

M and N are the width length and high length of the plain-image, K is the private-key, F(i,j) is the ciphertext image while $F_1(i,j)$ is the cipher-image with the condition of increasing private-key one bit and $F_2(i,j)$ is the cipher-image with the condition of decreasing private-key one bit. The results of key testing have been show in Table II.

TABLE II. KEY SENSITIVITY ANALYSIS

Private-Key	*Ks* (%)
ILOVETELECOMMUCH	99.9998
1234567891098763	100
G3$Hf43!$@$09@88	100

In order to measure the plaintext sensitivity, Y.W. Joseph et al., [9] reported that the Number of Pixel Change Rate of cipher-image (NPCR) and Unified Average Changing Intensity (UACI) have been used to be the standard testing. NPCR is used while one pixel of plain-image is changed and UACI is to measure the average intensity of difference between the plain-images. The formulas of NPCR and UACI have been shown respectively in (10) and (11).

$$NPCR = \frac{100\%}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)\right) \quad (10)$$

$$UACI = \frac{100\%}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|P_1(i,j) - P_2(i,j)|}{L-1}\right) \quad (11)$$

A bipolar array D(i,j) is defined by

$$D(i,j) = \begin{cases} 0 & \text{if } P_1(i,j) = P_2(i,j) \\ 1 & \text{if } P_1(i,j) \neq P_2(i,j) \end{cases} \quad (12)$$

where $P1$ *and* $P2$ are the cipher-image before and after one pixel changed in a plain-image, L is the intensity level random. Inside the Table III is the results of experiment of two cipher images P_1 and P_2 which are corresponding to the plain-images that have only one pixel different.

B. Peak Signal-to-Noise Ratio

The objective to evaluate the method of crypto-system, the peak signal to noise ratio (PSNR) is the most commonly used index in cryptography. It is the ratio of the mean square difference of the component of two images. So to reach the value of PSNR, first we have to calculate the Mean Square Error (MSE) between the hidden image and the cover image. Its formula has been shown in (13).

$$MSE = \frac{1}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} (C(i,j) - H(i,j))^2\right) \quad (13)$$

$C(i,j)$ and $H(i,j)$ respectively represent the cover image and hidden image. The value of PSNR is expressed as a decibel value. For our digital image encryption that value must be less than 30 dB. The formula to calculate has been show in (14).

$$PSNR = 10\log_{10}\left(\frac{L^2}{MSE}\right) \quad (14)$$

where L is the maximum possible value of pixel. The results of the system evaluation with PSNR were put in Table III.

C. Information Entropy

In 1949 in masterpiece of C. Shannon [10], information entropy theory which is the mathematical theory of data

communication has been found. In order to be negligible and be secure to against an entropy analysis, the value of entropy must ideal to 8. In our proposed system, the result of entropy has been shown in Table III by followed the formula of (15).

$$H(s) = \sum_{i=1}^{2^M - 1} P(S_i) \log_2 \frac{1}{P(S_i)} \qquad (15)$$

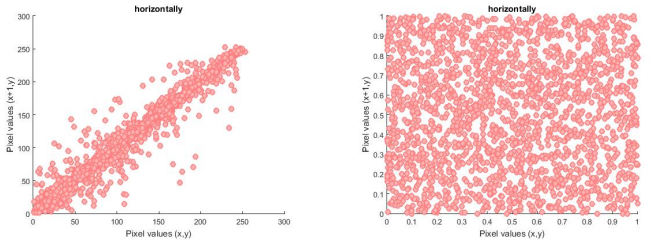
where M is the total number of pixel of the image.

TABLE III. SECURITY PERFORMANCE

Image	NPCR (%)	UACI (%)	PSNR (db)	Entropy H(s)
Lenna	100	33.293232	8.340112	7.997743
Baboon	100	33.394519	9.560207	7.997718
Pepper	100	33.364977	8.241336	7.997765

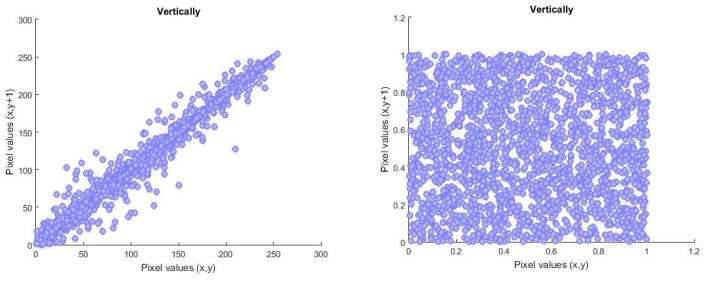
D. Correlation Coefficient

As our system also works with image data, so we have to think of high redundancy of each pixel inside image. It is highly correlated to adjacent pixel in horizontal, vertical and diagonal direction. The result of cipher-image must be low correlation between the adjacent pixels like in Fig. 12, Fig. 13 and Fig. 14. The results of the system corresponding to those three directions have been shown in Table IV with the confirmation security guaranty.



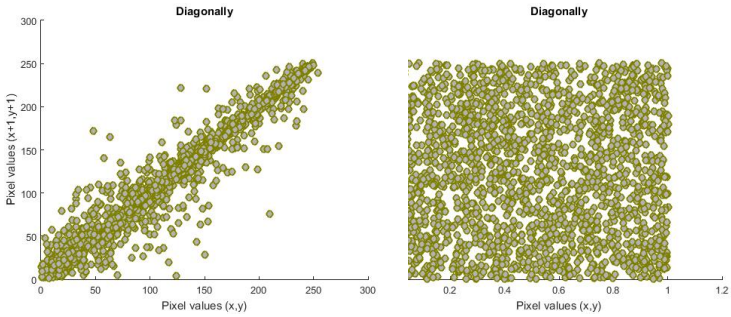
(a) Original horizontal correlation (b) Encrypted horizontal correlation

Fig. 12. Horizontal correlation before and after encryption.



(a) Original vertical correlation (b) Encrypted vertical correlation

Fig. 13. Vertical correlation before and after encryption.



(a) Original diagonal correlation (b) Encrypted diagonal correlation

Fig. 14. Diagonal correlation before and after encryption.

TABLE IV. CORRELATION COEFFICIENT

Image	Horizontal	Vertical	Diagonal
Lenna	-9.065261×10^{-4}	-2.245709×10^{-3}	-2.668720×10^{-3}
Baboon	-1.816787×10^{-3}	8.543164×10^{-4}	1.497774×10^{-3}
Pepper	-4.395587×10^{-4}	-7.833773×10^{-5}	-1.503614×10^{-3}

V. Conclusion

In this paper, a new technique of key generator to apply in cryptography using chaos in digital filter has been proposed. The 2nd order both IIR and FIR filter have been used to perform the process of the encryption and decryption. As consequence, the high key sensitivity produced by key generator to get security concern of the system coefficients, system key space and plaintext sensitivity satisfied the noted secure in the process of ciphertext transaction. It is confirmed efficiently to protect cryptanalysis such as the attacks by brute force, known-plaintext attack and select-plaintext attack.

Acknowledgment

The authors would like to thank AUN/Seed-net and International College of King Mongkut's Institute of Technology Ladkrabang Research Fund and the appropriate supply.

References

[1] N. Ronnaronglit, S. Chivapreecha and T. Sato, "An improved digital image encryption using chaos in digital filter," 2015 International Symposium on Multimedia and Communication Technology, 23-25, 2015.

[2] H. H. Abdlrudha and Q. Nasir, "Low complexity high security image encryption based on nested PWLCM chaotic map," 6th International Conference on Internet Technology and Security Transactions, 11-14, 2011.

[3] K. N. Prasetyo, Y. Purwanto and D. Darlis, "An implementation of data encryption for internet of things using Blowfish algorithm on FPGA," 2nd International Conference on Information and Communication Technology (ICoICT), 2014.

[4] M. George and A. Ioannis, "Cryptography with chaos," Proceeding 5th Chaotic Modeling and simulation International Conference, June 2012.

[5] L. O. Chua and T. Lin, "Chaos in digital filters," IEEE Trans. Circuits Systs., vol. 35, no. 6, pp. 648-658, June 1988.

[6] D. R. Frey, "Chaotic Digital Encoding": An Approach to Secure Communication, IEEE Transactions on Circuits and System -II: Analog and Digital Signal Processing, vol. 40, no. 10 October 1993.

[7] K. Kutzer, W. Schwarz and A. C. Davies, "Chaotic signals generated by digital filter overflow", IEEE International Symposium on Circuits and Systems, vol. 6, pp. 17-20, June 1994.

[8] Brute Force Calculator Open Security Research, sponsored by Foundstone http://calc.opensecurityresearch.com/.

[9] Y. W. Joseph, P. Noonan and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Department of Electrical and Computer Engineering Tufts University Medford, MA, USA.

[10] C. Shannon, "Communication theory of secrecy system", Bell system Technical Journal 28:656-715, 1949.

2017 8th IEEE Control and System Graduate Research Colloquium (ICSGRC 2017)

4-5 August 2017.

Grand Blue Wave Hotel, Shah Alam, Malaysia

ORGANIZED BY:

Organized by:

IEEE Malaysia Section Control Systems Chapter

SECRETARIAT:

Secretariat

UNIVERSITI TEKNOLOGI MARA

Advanced Signal Processing Research Group (ASPRG), Universiti Teknologi Mara Malaysia

PAST INDEXING

SCOPUS

IEEE Xplore Digital Library

ICSGRC2016
IEEExplore | Scopus

ICSGRC2015
IEEExplore | Scopus

ICSGRC2014
SCOPUS | IEEExplore

ICSGRC2013
SCOPUS | IEEExplore

ICSGRC2012
SCOPUS | IEEExplore

ICSGRC2011
SCOPUS | IEEExplore

ICSGRC2010
SCOPUS | IEEExplore

Like us on Facebook and Google+!

Home

The IEEE Control Systems Society Chapter Malaysia and the Faculty of Electrical Engineering, UiTM are pleased to announce the 2017 8th IEEE Control and System Graduate Research Colloquium (ICSGRC 2017), which will be held in the Grand Blue Wave Hotel, Shah Alam, Malaysia on 4-5 August 2017.

The colloquium will provide an excellent platform for knowledge exchange between postgraduates & researchers working in areas of listed below. In addition, it provides an opportunity for the participants from Malaysia and overseas to share research findings and establish network and collaborations. This event calls for local and international participation.

Authors are invited to submit original, unpublished papers on all aspects of control and system including but not limited to the following technical areas:

- **Control, Information and Systems Engineering**
- **System Identification and Modeling & Signal Processing**
- **Instrumentation and Automation**
- **Technological Advancements**
- **Power Systems**
- **Communication**
- **Electronics Engineering**
- **Computer Engineering**
- **Remote Sensing & Geomatic Engineering**
- **Other related areas.**

Important dates are listed below:
Submission of full papers deadline: ~~**31st May 2017**~~ **(extended to 2nd June 2017)**
Issuance of notification of acceptance: **16th June 2017**
Registration & camera-ready submission deadline: **30th June 2017**

Conference content will be submitted for inclusion into IEEEXplore as well as other Abstracting and Indexing (A&I) databases

Welcome to IWAIT2018

International Workshop on Advanced Image Technology 2018 (IWAIT 2018) will be held on January 7-9, 2018 in Chiang Mai, Thailand. IWAIT 2018 will provide an international forum for researchers and engineers who are interested in the field of advanced image technologies.

News

- **Manuscript for IEEE Xplore - February 22, 2018**

  Accepted paper will be published in IEEE Xplore after the conference. The IWAIT 2018 submission site will check the submitted files for compliance and will reject non-compliant files. Failure to comply will prevent proper publication or accreditation of your work. Before uploading a final manuscript, authors are requested to check whether the manuscript is Xplore-compliant using IEEE PDF eXpress. Please click here. (http://www.iwait2018.org/Accepted Paper.html)

Question about Manuscript for IEEE Xplore, please mail to secretary@iwait2018.org (mailto:secretary@iwait2018.org)

- **BEST PAPER AWARDS - January 25, 2018**

  IWAIT 2018 is pleased to announce the winners of the best paper awards from the set of papers submitted to the conference. Please Click here (http://www.iwait2018.org/Best Paper Award.html)

- **IWAIT 2018 Conference Pictures - January 18, 2018**

  We are pleased to announce that photos of the IWAIT 2018 Conference are online. Please Click here (http://www.iwait2018.org/Conference Pictures.html) to view the photos.

- **Changed the place of banquet from Ballroom A and B to Chang Garden - January 5, 2018**

  On the evening of January 8 at 18:30 - 21:00 hrs., IWAIT 2018 is hosting an banquet for all conference participants. Please be announced that **the event will take place at the Chang Garden (Beer Garden).** Please click the link : Program at a Glance (http://www.iwait2018.org/program.html) for your information.

- **Updated Program at a Glance - December 27, 2017**

  We have updated the Tentative Conference Program of IWAIT 2018. Please click the link : Program at a Glance (http://www.iwait2018.org/program.html) for your information.

- **Poster Presentation Guidelines - December 26, 2017**

  We would like to announce that there are two poster sessions : Poster Session 1 and 2. The authors have two hours for poster presentation. Please see Program Conference for details of each session. Please follow the guidelines as described below:

  1. Ensure your poster is placed on the assigned poster board for the duration of your poster session.
  2. Stand at your poster during your assigned 120-minute presentation time.
  3. Please remove your poster from poster board after finishing your presentation.
  4. The authors should brief and introduce their own research around 1-2 minutes in the beginning of the poster session.

  Poster Board Size: The poster board surface area is 60 cm wide by 70 cm high. **Your poster size should be no bigger than 60x70 cm.**

- **Updated Program at a Glance - November 29, 2017**

A Single, Triple Chaotic Cryptography Using Chaos in Digital Filter and Its Own Comparison to DES and Triple DES

Reatrey Pich
International College
King Mongkut's Institute of Technology
Ladkrabang, Bangkok 10520, Thailand
Email: reatrey.pich@gmail.com
/59610026@kmitl.ac.th

Sorawat Chivapreecha
Department of Telecommunication
Engineering, Faculty of Engineering
King Mongkut's Institute of Technology
Ladkrabang, Bangkok 10520, Thailand
Email: sorawat@telecom.kmitl.ac.th

Jaruwit Prabnasak
International College
King Mongkut's Institute of Technology
Ladkrabang, Bangkok 10520, Thailand
Email: kpjaruwi@kmitl.ac.th

***Abstract*—The Data Encryption Standard (DES) of the multimedia cryptography possesses the weak point of key conducting that is why it reaches to the triple form of DES. However, the triple DES obtains the better characteristic to secure the protection of data to against the attacks, it still contains an extremely inappropriate performance (speed) and efficiency in doing so. This paper provides the effective performance and the results of a single and triple chaotic cryptography using chaos in digital filter, compare to DES and triple DES. This comparison has been made pair-to-pair of single structure respectively to the triple form. Finally the implementation aspects of a single chaotic cryptography using chaos in digital filter can stand efficiently as better performance speed with the small complexity algorithm, points out the resemblances to DES and triple DES with the similar security confirmation results without reaching to the triple form of the structure. Simulation has been conducted using Matlab simulation with the input of grayscale image.**

Keywords—Cryptography; DES; Triple DES ; Chaos in Digital Filter

I. INTRODUCTION

Cryptography is one of techniques of security concern in data transmission. It covers various aspects such as security, compression efficiency, encryption efficiency and format compliance. There are many data encryption algorithms which have been widely used like DES, triple DES, AES or IDEA, but in the point of multimedia data is different from text because multimedia data has high redundancy, so it produced non appropriate cipher-image [1]. For DES using Logistic map can make the cipher-image to be the stochastic noise to against the attacks, but it contains of high complexity because of round keys randomization [2]. The high security of encrypted image with three different round keys accompanied by chaotic properties have made cipher-image to be secure strongly too but it gave the same problem of complexity of making cipher image to be elliptic curve [3]. Same as Triple DES which makes the performance issues three time worse compare to its single form. Chaos in digital filter produces the nonlinear behavior and unstable system to make the cipher-image possess security by matching with overflow nonlinearity function [4].

II. CHAOTIC IN DIGITAL FILTER AND DES

A. Chaotic In Digital Filter

Chaotic cryptography is known as the dynamic system and using chaos in digital filter has produced the unstable system and nonlinear behavior to make the system is more profitable by involved with mathematic operation and overflow function [4-5]. During the process all-pole IIR filter function as encryption engine while its inverse form as all-pole FIR filter will work as decryptor. The detail of all-pole IIR filter is in the figure. 1 and equation (1-4).

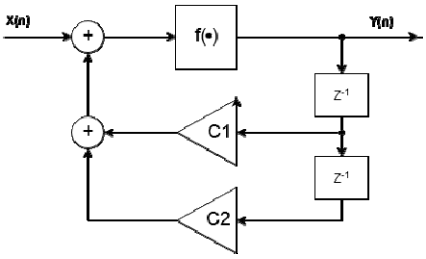


Fig. 1 All-pole IIR filter in second order

$$y(n) = x(n) + C_1 y(n-1) + C_2 y(n-2) \quad (1)$$

$$H(z) = \frac{y(z)}{x(z)} = \frac{1}{(1 - C_1 z^{-1} - C_2 z^{-2})} \quad (2)$$

$$f(x) = [(x+1) \bmod 2] - 1 \quad (3)$$

$$y(n) = f\{x(n) + C_1 y(n-1) + C_2 y(n-2)\} \quad (4)$$

In order to make sure that system is unstable and conducts with nonlinear behavior to produce the chaos inside the system, the coefficients are at least one is outside the stable triangle and system is worked through the overflow function [6].

978-1-5386-2615-3/18/$31.00 ©2018 IEEE

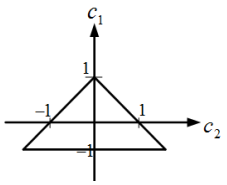


Fig. 2. The stable triangle.

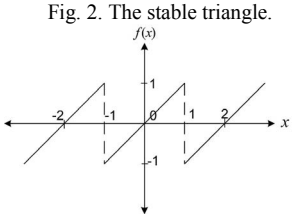


Fig. 3. The characteristic of overflow function.

B. *Data Encryption Standard (DES)*

DES is a 64 bits block cipher which work with 64 bits of data per time. It uses 64 bits key input, but only 56 bits of the key will be used inside the operation. In this technique it is used as iteration process that is known as Round. The whole process consist of 16 rounds. More detail is shown in figure. 4.

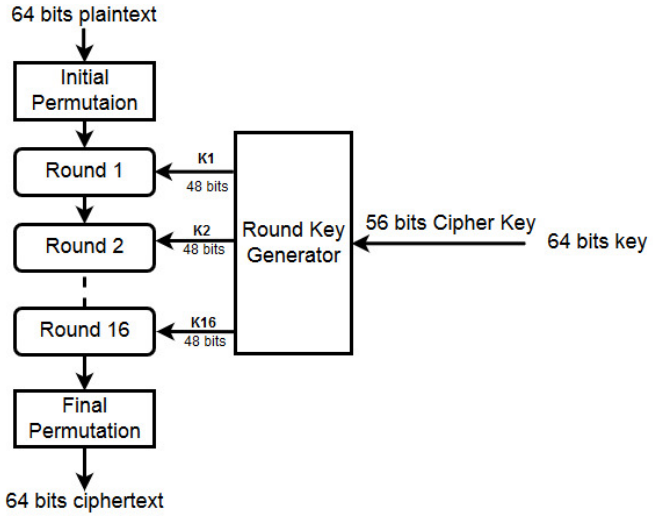


Fig. 4. Block diagram of Data Encryption Standard

For the structure of triple DES is the combination of three time of single DES by using the key bundle in order to generate K_1, K_2 and K_3. The detail of encryptor is show as below:

$$\text{Cipher-Image} = E_{K3}(D_{K2}(E_{K1}(\text{Plain-Image})))$$

For the decryptor is the inverse form of the encryptor only by exchanging the Encrypted process to Decrypted process and Decrypted process to Encrypted process.

III. The Proposed Structure

A. *Single form of Chaotic cryptography*

The proposed structure for data encryption using chaos in digital filter is composed by two main parts. First is the key generator which is made up with three all-pole IIR filters of input of 16 characters (128 bits). Second is the encryption engine which uses only one all-pole IIR filter to perform the process. The system provides the value as key sensitivity and high security confirmation [7]. The detail is shown in Fig. 5.

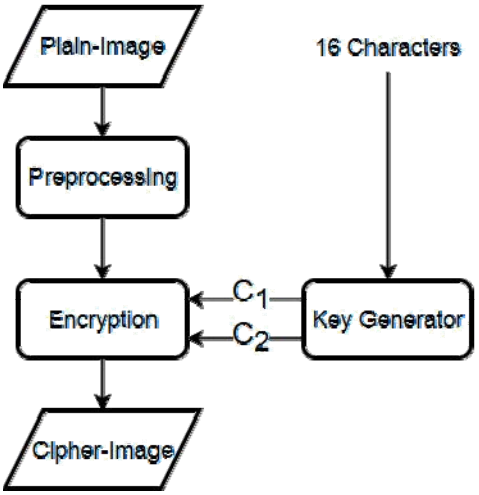


Fig. 5 The structure of single form of chaotic cryptography.

B. *Triple form of Chaotic cryptography*

For its triple form is made as the concept of triple DES and followed the structure of single chaotic cryptography. But for the coefficients of each filters of encryption engine are produced by different sub key generators which have different made up coefficients but the same input of 16 characters. The strong security over the single form is it has more initialed values than the single. The detail is in Fig. 6.

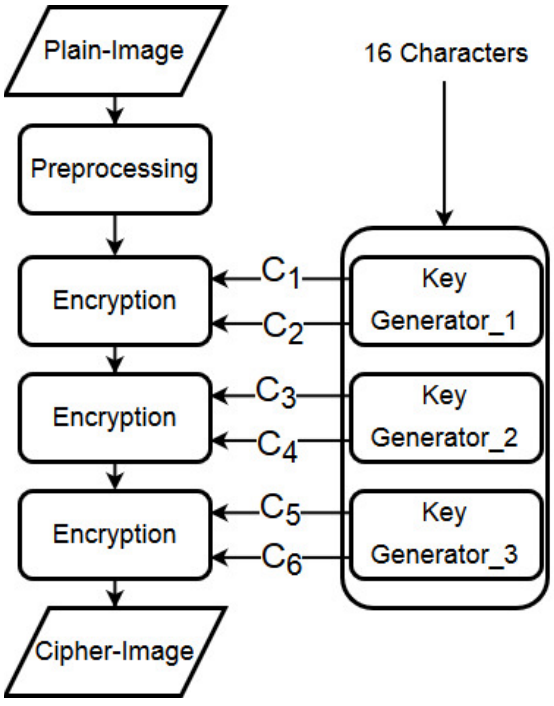


Fig. 6 The structure of triple form of chaotic cryptography.

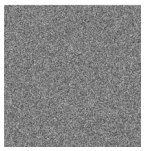
IV. THE EXPERIMENT

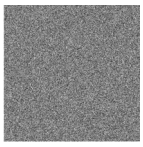
For the experiment, the input data are the gray scale image. Inside the paper, three images have been selected for testing the security and results analysis. Input and output of chaotic cryptography are shown respectively:

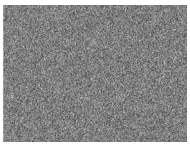
(a) Lenna image

(b) Baboon image

(c) Pepper image







(d) Lenna cipher-image (e) Baboon cipher-image (f) Pepper cipher-image

A. The proposed structure results

In order to confirm about the security and sensitivity inside the cipher-image to make sure our system is qualified enough to use, there are some main factors to be considered:

- Key Space, Key Sensitivity and Plaintext Sensitivity: the values that can confirm that our system can against the attacks such as brute force attack which is widely known. Moreover, to make sure our system is sensitive to the key, key sensitivity is the main factor to be considered.

TABLE I. KEY SPACE

Key Length (bits, Char)	Algorithm	Key Space	Time To Brute Fore
128 , 16	**Single form of proposed technique**	4.4 x 10^{38}	4.4 x 10^{31} years
57, 7	DES	7.2 x 10^{16}	13 years 91 days
128, 16	**Triple form of proposed technique**	4.4 x 10^{38}	4.4 x 10^{31} years
168, 21	Triple-DES	3.7 x 10^{50}	3.4 x 10^{41} years

To define key sensitivity the formula below is used:

$$Ks = \frac{100\%}{2MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} K_1(i,j) + \sum_{i=1}^{M}\sum_{j=1}^{N} K_2(i,j)\right) \quad (5)$$

where $K_1(i,j)$ and $K_2(i,j)$ are defined by

$$K_k(i,j) = \begin{cases} 0 & \text{if } F(i,j) = F_k(i,j) \\ 1 & \text{if } F(i,j) \neq F_k(i,j) \end{cases} \quad (6)$$

where F(i,j) and $F_k(i,j)$ are the cipher-images with different one bit of the key input.

TABLE II. KEY SENSITIVITY

Image	Key Sensitivity (Ks) %	
	Single form of proposed structure	***Triple form of proposed structure***
Lenna	99.9999	99.9998
Baboon	99.9998	99.9998
Pepper	99.9997	99.9997

To define Plaintext sensitivity, Number of Pixel Change rate of cipher-image (NPCR) and Unified average changing intensity (UACI) are used with below formula:

$$NPCR = \frac{100\%}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)\right) \quad (7)$$

$$UACI = \frac{100\%}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|P_1(i,j) - P_2(i,j)|}{L-1}\right) \quad (8)$$

A bipolar array D(i,j) is defined by

$$D(i,j) = \begin{cases} 0 & \text{if } P_1(i,j) = P_2(i,j) \\ 1 & \text{if } P_1(i,j) \neq P_2(i,j) \end{cases} \quad (9)$$

where P_1 and P_2 are the cipher-image before and after one pixel changed in a plain-image.

TABLE III. PLAINTEXT SENSITIVITY (NPCR, UACI)

Image	***Single form of proposed structure***		***Triple form of proposed structure***	
	NPCR	**UACI**	**NPCR**	**UACI**
Lenna	100	33.29	100	33.29
Baboon	100	33.39	100	33.43
Pepper	100	33.36	100	33.25

- Peak Signal-to-Noise Ratio (PSNR): It is the ratio of mean square difference between two images. To get the PSNR evaluation, it is necessary to calculate Mean Square Error (MSE).

$$MSE = \frac{1}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} (C(i,j) - H(i,j))^2\right) \quad (10)$$

C(i,j) and H(i,j) are the cover image and hidden image. And the formula of PSNR is defined as below:

$$PSNR = 10\log_{10}\left(\frac{L^2}{MSE}\right) \quad (11)$$

- Information Entropy (H(s)): The mathematic theory of data communication used to against entropy analysis and the best value is reaching to 8 [7]. The formula is shown as below:

$$H(s) = \sum_{i=1}^{2^M - 1} P(S_i)\log_2 \frac{1}{P(S_i)} \quad (12)$$

Where M is the number of pixel of cipher-image

TABLE IV. PEAK SIGNAL-TO-NOISE RATIO(PSNR) INFORMATION ENTROPY (H(S))

Image	*Single form of proposed structure*		*Triple form of proposed structure*	
	PSNR(db)	**H(s)**	**PSNR(db)**	**H(s)**
Lenna	6.6965	7.9980	6.6929	7.9979
Baboon	9.5602	7.9977	9.5612	7.9979
Pepper	8.2413	7.9977	8.2567	7.9977

- Correlation Coefficient: The value to find the correlation between plain-image and cipher-image. Good cryptography gives the low correlation.

TABLE V. CORRELATION COEFFICIENT (HORIZONTAL)

Image	**Horizontal**	
	Single form of proposed structure	***Triple form of proposed structure***
Lenna	-0.0027	0.0012
Baboon	-0.0018	-0.0017
Pepper	-4.3955×10^{-4}	5.2933×10^{-4}

TABLE VI. CORRELATION COEFFICIENT (VERTICAL)

Image	**Vertical**	
	Single form of proposed structure	***Triple form of proposed structure***
Lenna	-0.0022	0.0017
Baboon	8.5431×10^{-5}	4.1482×10^{-4}
Pepper	-7.8337×10^{-5}	-4.9636×10^{-4}

TABLE VII. CORRELATION COEFFICIENT (DIAGONAL)

Image	**Diagonal**	
	Single form of proposed structure	***Triple form of proposed structure***
Lenna	0.0030	1.0201×10^{-4}
Baboon	0.0014	0.0029
Pepper	-0.0015	-0.0055

B. Comparison and Discussion

The proposed structure, both provided with high security confirmation, while DES consists with weak key conduction and 3DES is made to ensure with the key but the performance is slow because of three times compare to DES [8]. However the length of the key can solve the problem from some attack, it still faces with meet-in-the-middle attack. The security comparison is shown as below [9]:

TABLE VIII. COMPARISON OF SECURITY CONFORMATION

Parameters	***Proposed structure (average)***	***Data Encryption Standard (average)***
PNCR	100	99.6643
PSNR(db)	8.166	7.6057
UACI	33.34	51.2491

But in terms of the complexity of both DES and 3-DES generally is made as O(m) that consist of 8 S-Box and many round of XOR Operation (16, 48) which is the main issue effects to the performance of the system. For the proposed structure, it works only with second order of convolution summation that can produce high performance conduction.

V. CONCLUSION

In this paper, we have presented the comparison results between the proposed structures of chaotic cryptography in digital filter with DES and Triple DES. Having computed the experiment, the security confirmation of each technique provided the similar exclamation while produced different performance of complexity running. A single form of chaotic cryptography in digital filter can obtain the best outstanding consideration among others.

ACKNOWLEDGMENT

The author would like to express gratefully attitude to AUN/Seed-net and thankful to International College of King Mongkut's Institute of Technology Ladkrabang for supporting the fund and material supply during my research process.

REFERENCES

[1] S. Lian, Multimedia Content Encryption: Techniques and Application, CRC, 2008.

[2] M-S. Liu, Y. Zhang, J. li, "Research on Improving Security of DES by Chaotic Mapping" IEEE, Proceedings of the 8th International Conference on Machine Learning and Cybernetics, Baoding, pp. 12-15, Jul 2009. K. Elissa, "Title of paper if known," unpublished.

[3] B.J. Saha, Arun, K.K. Kabi and C. "A Robust Digital Watermarking algorithm using DES and ECC in DCT Domain for Color Images" 2014 international Conference on Circuit, Power and Computing Technologies [ICCPCT].

[4] L. O. Chua and T. Lin, "Chaos in digital filters," IEEE Trans. Circuits Systs., vol. 35, no. 6, pp. 648-658, June 1988.

[5] M. George and A. Ioannis, "Cryptography with Chaos", Proceeding 5th Chaotic Modeling and simulation International Conference, June 2012.

[6] P. Reatrey, C. Sorawat and P. Jaruwit, "A New Key Generator for Data Encryption Using Chaos in Digital Filter", 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC 2017), 4-5 August 2017, Shah Aam, Malaysia

[7] C. Shannon, "Communication theory of secrecy system", Bell system Technical Journal 28:656-715, 1949.

[8] M. Ebrahim, S. Khan and U. B. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis", International Journal of Computer Applications (0975-8887) Volume 61-No. 20, January 2013

[9] S. Soni, H. Agrawal and M. Sharma, " Analysis and Comparison between AES and DES Cryptographic Algorithm", IJEIT 2017

AUTHOR BIOGRAPHY

Author : Mr. Reatrey PICH

Degree : Master of Engineering

Date of Graduation :

Date of Birth : 24^{th} February 1993

Place of Birth : Banteaymeanchey, Cambodia

Undergraduate and Graduate Education:

Master of Engineering in Computing in Engineering Systems,
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand, 2018

Bachelor degree in Information and Communication Engineering,
Institute of Technology of Cambodia, Phnom Penh, Cambodia, 2016

Major: Computing in Engineering Systems

Presentations and Publications:

- Paper's name : **"A New Key Generator for Data Encryption Using Chaos in Digital Filter"** 04-05, August, 2017, ICSGRC 2017, Grand Blue Wave Hotel, Shah Alam, Malaysia
- Paper's name : **"A Single, Triple Chaotic Cryptography Using Chaos in Digital Filter and Its Own Comparison to DES and Triple DES"** 07-10, January, 2018, IWAIT 2018, Chiang Mai, Thailand