
**UNIVERSITI PUTRA MALAYSIA**

# *RECONSTRUCTING APPLICABLE CHAOTIC BAPTISTA-TYPE SYMMETRIC CRYPTOSYSTEM*

**MUHAMAD AZLAN BIN DAUD**

**IPM 2014 13**

# RECONSTRUCTING APPLICABLE CHAOTIC BAPTISTA-TYPE SYMMETRIC CRYPTOSYSTEM

By

**MUHAMAD AZLAN BIN DAUD**

© COPYRIGHT UPM

**Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirement for the Degree of Master of Science**

**September 2014**

**COPYRIGHT**

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia



© COPYRIGHT UPM

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

**RECONSTRUCTING APPLICABLE CHAOTIC BAPTISTA-TYPE SYMMETRIC CRYPTOSYSTEM**

By

**MUHAMMAD AZLAN BIN DAUD**

**September 2014**

**Supervisor : Muhammad Rezal Bin Dato' Kamel Ariffin, PhD**
**Department : Institute for Mathematical Research**

This work, introduces a method to repair a cryptosystem based on a chaotic dynamical system. Baptista exploited the chaotic property of the logistic equation $f(x) = bx(1-x)$ to develop a cryptosystem. This cryptosystem has the ability to produce various ciphers responding to the same message input. Alvarez through his one-time pad attack successfully attacked the Baptista cyptosystem. Ariffin attempted to modify the cryptosystem to enhance the security of the original Baptista's cryptosystem. Rhouma identified a flaw in the method Ariffin put forward, specifically in step 4 of the encryption procedure, where it does not implement a one-to-one operation resulting in failure to decrypt the ciphertext. The method is based on the Fractal and Iterated System (IFS), where an in-depth study on Fractal, Chaos and Cryptography is needed to assist in actualizing the research objectives. The algorithm is developed to counter the one-time pad attack. This recommended encryption algorithm also overcomes the flaw in Ariffin's encryption procedure. The modified Baptista type cryptosystem suffers from message expansion that goes against the conventional methodology of a symmetric cryptosystem. As a result, we studied the idea of Huffman encoding. We then designed a new compression algorithm developed using ideas from the Huffman coding. Finally, the compression algorithm is applied onto the modified Baptista cryptosystem to show a possible practical deployment of the Baptista cryptosystem and to also produce better compression ratio.

© COPYRIGHT UPM

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

**MEMBINA SEMULA SISTEM KRIPTO SIMETRIK KALUT JENIS BAPTISTA YANG BOLEH DIGUNAPAKAI**

Oleh

**MUHAMMAD AZLAN BIN DAUD**

**September 2014**

**Penyelia : Muhammad Rezal Bin Dato' Kamel Ariffin, PhD**
**Institut : Institut Penyelidikan Matematik**

Penyelidikan ini akan memperkenalkan satu kaedah untuk membaik pulih satu sistem kripto berasaskan kekalutan sistem dinamik. Baptista telah mengeksploitasi ciri kekalutan pemetaan logistik $f(x) = bx(1-x)$ untuk membentuk suatu sistem kripto. Sistem kripto ini mempunyai kemampuan untuk menghasilkan sifer-sifer berlainan walaupun merujuk kepada teks asal yang sama. Alvarez melalui serangan lembaran sekali sahaja telah berjaya menyerang sistem krito Baptista tersebut. Ariffin mencuba untuk mengubahsuai sistem kripto untuk meningkatkan keselamatan asal sistem kripto Baptista. Rhouma mengenalpasti kelemahan pada sistem yang diubahsuai oleh Ariffin kemukakan dalam langkah 4 prosedur penyulitan. Ianya bukan operasi satu ke satu. Penyelidikan adalah berdasarkan kepada kajian Fraktal dan Sistem Terlelar (IFS), yang memerlukan kajian yang mendalam terhadap fraktal, kekalutan dan kriptografi untuk membantu dalam mencapai objektif kajian. Algoritma dibangunkan untuk mengatasi serangan lembaran sekali sahaja. Sistem kripto jenis Baptista yang diubah suai mengalami perkembangan mesej yang bertentangan dengan kaedah konvensional yang sistem kripto simetri. Untuk ini kami mengkaji idea pengekodan Huffman. Seterusnya, satu algoritma mampatan baru telah dibangunkan mengunakan idea yang diguna pakai dalam pengekodan Huffman. Akhir sekali, algoritma mampatan yang dibangunkan ini telah digunakan keatas sistem kripto Baptista yang telah diubahsuai sebagai memungkinkan sistem kripto Baptista diguna pakai dan disamping memberikan nisbah mampatan yang lebih baik.

© COPYRIGHT UPM

**ACKNOWLEDGEMENT**

Bismillahirrahmanirrahim.

All praise to the Almighty Allah S.W.T for His blesses and mercy that enable me to enrich my knowledge and by His grace I was able to complete the Master's thesis. Without inspiration, patience and istiqamah that is blessed by Him where I am able to complete a thesis as a result of three years of study at Universiti Putra Malaysia. The names of the people that I have listed here have had a significant role in the writing of this thesis. For it is their guidance, support, and most importantly, encouragements that have helped me survive these years.

First and foremost, my utmost appreciation goes out to my mother Mrs. Jaharah binti Saamah, for her often encouragement and advice that acts as an amulet which is helpful in the twists and turns that lead to my master studies. I also want to thank Assoc. Prof. Dr. Muhammad Rezal Bin Dato Kamel Ariffin, who was brave enough to undertake the job of supervising my project for his utmost expertise in this field. On this note, I also would like to thank the benevolent En. Zahari bin Mahad because he has helped me about C++ programming and Excel.

Sorry for all the inconveniences caused, especially to my friends from UPM. Thank you for all the evaluations and suggestions to help me write better. And to my family and friends, who form an important group of people outside of Mathematics, for their prayers, encouragements and faith in me. My family for working hard to send me to UPM so that I can fulfill my dream; my fiancee, Wan Nur Afeza binti Shah Haibi for putting up with my mood swings and mathematical idiosyncrasies during the stressful periods; and to everyone else that have encouraged me throughout the years.

© COPYRIGHT UPM

I certify that a Thesis Examination Committee has met on 8 September 2014 to conduct the final examination of Muhamad Azlan bin Daud on his thesis entitled "Reconstructing Applicable Chaotic Baptista Type-Symmetric Cryptosystem" in accordance with Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.
Members of the Thesis Examination Committee were as follows:

**Mat Rofa b Ismail, PhD**
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

**Siti Hasana bt Sapar, PhD**
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

**Zuriati Ahmad Zulkarnain, PhD**
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

**Nadia Mohammed Ghanim Al-Saidi, PhD**
Dr.
Branch of Applied Mathematics
Applied Science Department
University of Technology, Iraq
(External Examiner)

_____
**NORITAH OMAR, PhD**
Associate Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

© COPYRIGHT UPM

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

**Muhammad Rezal Bin Dato' Kamel Ariffin, PhD**
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

**Mohamad Rushdan Bin Md Said, PhD**
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

_____

**BUJANG BIN KIM HUAT, PhD**
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

© COPYRIGHT UPM

**Declaration by graduate student**

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: _____

© COPYRIGHT UPM

**Declaration by Members of Supervisory Committee**

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

| | | | |
|---|---|---|---|
| Signature: | | Signature: | |
| Name of Chairman of Supervisory Committee: | Assoc. Prof. Dr. Muhammad Rezal Bin Dato' Kamel Ariffin | Name of Member of Supervisory Committee: | Assoc. Prof. Dr. Mohamad Rushdan Bin Md Said |

© COPYRIGHT UPM

## TABLE OF CONTENTS





© COPYRIGHT UPM

© COPYRIGHT UPM

## LIST OF TABLES



© COPYRIGHT UPM

## LIST OF FIGURES



© COPYRIGHT UPM

## ABBREVIATIONS / GLOSSARY OF TERMS

| | |
|---|---|
| AES | : Advanced Encryption Standard |
| CCF | : Correlation Coeficient Factor. |
| DES | : Data Encryption Standard |
| IFS | : Iterated Function System. |
| SAC | : Strict Avalance Criterion. |
| ZIP | : PKzip file name extension. |
| LSB | : Least Significant Bits. The most significant bit is on the left side. |
| Attractors | : The smallest unit which cannot be itself decomposed into two or more attractors with distinct basins of attraction. |
| Collage | : A collection or combination of various things. |
| Contraction | : The process of becoming smaller. |
| Ciphertext | : The result of encryption performed on plaintext using an algorithm. |
| Decryption | : The reverse process to Encryption (open hidden messages). |
| Decrypt | : Convert Ciphertext into Plaintext (Original Message). |
| Encryption | : Process of encoding/hiding messages or information in such a way that only authorized parties can read it. |
| Encrypt | : Convert Plaintext (Original Message) into a Ciphertext. |
| Plaintext | : Original message. |

© COPYRIGHT UPM

## NOTATIONS

| | |
|---|---|
| $\oplus$ | : XOR , binary operator. |
| $\|b\|$ | : Be the length of the corresponding data string $b = \{0,1\}^n$. |
| $w_j$ | : Codeword to represent on the difference between the length of $\|b_{j-1}\|$ and $\|b_j\|$, $w_j = \|\|b_j\| - \|b_{j-1}\|\|$. |
| $\|m\|$ | : Be the length of the messages before compression. |
| $\|m_c\|$ | : Be the length of the messages after compression. |
| $\|p_0\|$ | : Be the sum of length between codeword $\|w_k\|$ and $\|b_k\|$, $\|p_0\| = \|w_k\| + \|b_k\|$. |

© COPYRIGHT UPM

# CHAPTER 1

# INTRODUCTION

## 1.1 Information Theory

The father of information theory, Claude E. Shannon has developed the theoretical framework for the information theory, shortly after the end of Second World War in 1948 in a seminar paper entitled "A Mathematical Theory of Communication". He had presented all the main theoretical ingredients of modern information theory in this paper. In particular, as we will see later, Shannon formulated and provided proofs for the two main coding theorems.

### 1.1.1 Shannon Paradigm

Shannon theory of communication is based on the so-called Shannon Paradigm, illustrated below:


**Figure 1.1.1 Shannon Paradigm**

The source produces a message (chosen at random) which is sent to a receiver through an imperfect communication channel. Information can be generated by a sequence of symbols, from the source which may come from different medium, which may appear as random to another party or receiver. In other words, before the message is sent to the receiver, there is some "uncertainty" about what will next message be or sometimes known as the missing information. After the message has been received, the corresponding "uncertainty" will be measured and removed. Then, with some probabilistic formula, the information will be measured by this reduction in uncertainty. Entropy will be introduced after this.

In real life, physical channels are imperfect due to the existence of some form of noise. This means that the receiver may receive a message that is already damaged, as a result of the message being sent in readily damaged form: the damage is unpredictable by either the receiver or the sender of the message.

## 1.2 Symmetric Chaos Cryptosystem

### 1.2.1 Symmetric Cryptography (Private-Key Cryptography)

Symmetric cryptography also known as private-key cryptography is a branch of cryptography study which acts as a single private key to encrypt and decrypt data. Any individual that has the key can use it to encrypt and decrypt data. It is also not possible for a person who views the encrypted data with a symmetric cipher to be able to do so without having access to the key used to encrypt it in the first place. They are also referred to as block ciphers. Symmetric cryptography algorithms are typically faster and are suitable to process large streams of data.

© COPYRIGHT UPM

Symmetric key ciphers use the same key to both encrypt and decrypt data. This type of cipher is valuable because it is relatively inexpensive to produce, the key tend to be much smaller for the level of protection they afford and the algorithms are relatively inexpensive to process.

Here, a private key cryptosystem analogy will be illustrated. Symmetric-key encryption provides secrecy when two parties, say Alice and Bob, communicate. An adversary who intercepts a message should not get any significant information about its contents. Symmetric-key algorithms are generally much less computationally intensive than asymmetric key algorithms. It is known as symmetric encryption and decryption, because both communication partners use the same key $k$ for encryption and decryption. The encryption and decryption algorithm $E$ and $D$ are publicly known. Anyone can decrypt a ciphertext, if he or she knows the key. Thus the key $k$ has to be kept secret.

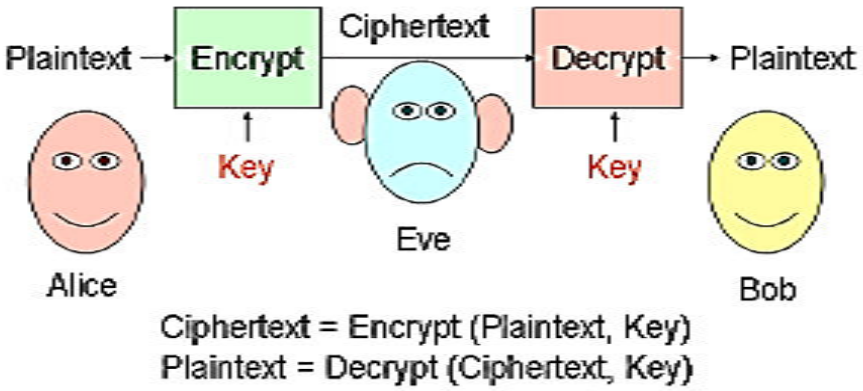


**Figure 1.2.1 Analogy Symmetric-key Cryptosystem**

In practice, asymmetric key algorithms are typically hundreds to thousands times slower than symmetric key algorithms. One disadvantage of symmetric-key algorithms is the requirement of a shared secret key, with one copy at each end. In order to ensure secured communications between everyone in the population of $n$ people, a total of $\frac{[n(n-1)]}{2}$ keys are needed, which is the total number of possible communication channels. To limit the impact of a potential discovery by a cryptographic adversary, the users should be changed regularly and kept secure during distribution and in service. The process of selecting, distributing and storing keys is known as key management, and is very difficult to achieve reliably and securely.

The modern study of symmetric key ciphers related to the study of block ciphers and stream ciphers and also to their applications. Block ciphers take input as a block of plaintext and key, and generate output as a block of ciphertext of the same size. Since the message is always longer than a single block, some method of knitting the block is required. Several methods have been developed with better security. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are the two block cipher designs that have been created by the US government.

### 1.2.2 Exponent Lyapunov

Let two points in a space $x_0$ and $x_0 + \Delta x_0$, where the two points will generate an orbit in space, based on an equation or a system of equations. This orbit is assumed to use time as its parameter. If we use one of the orbits as the reference orbit, the separation between the two orbits can also be assumed to use time as a parameter. Since the system may become sensitive at certain parts of the system (such as the logistic maps), this separation also serves as the function of the initial point location and comes in the form of $\Delta x_0(x_0, t)$. In a system with an attractors fixed point or periodic attractors, $\Delta x_0(x_0, t)$ will vanish after a time interval. If a system is not stable, the orbits will diverge in exponent for a while, but then stabilized again. For chaotic points, $\Delta x_0(x_0, t)$ function will be erratic. To study the rate of divergence of two originally close points, we will use Lyapunov exponent which is given by:

$$\lambda = \lim_{t\to\infty, \Delta x_0 \to 0} \frac{1}{t} ln \ \frac{|\Delta x(\Delta x_0, t)|}{\Delta x_0} \tag{1.2.2}$$

For practical purposes, Lyapunov exponents are used to characterize the Chaotic. The orbits of a mapping is said to have its chaotic features if the Lyapunov exponent, $\lambda$ the mapping is positive (i.e. $\lambda > 0$).

Consider a dynamic system with dimension 1 $f : I \to I$. When $\lambda > 0$,

$$\forall \varepsilon > 0, \exists n_1, n_2 \in \mathbb{N}, \exists x \in U_{n_1, n_2}, \forall n \in [n_1, n_2], \forall z_1, z_2 \in U_{n_1, n_2},$$

$$\exp(\lambda - \varepsilon)n|z_1 - z_2| < |f^n(z_1) - f^n(z_2)| < \exp(\lambda + \varepsilon)n|z_1 - z_2|.$$

These means that the initial distance $|z_1 - z_2|$ between any two points (which is an element of the neighborhood $U_{n_1, n_2}$ for point $x$) will increase at least exp $(\lambda - \varepsilon)n$ times after $n$ iteration,

### 1.2.3 Chaos Dynamical System

Modern telecommunication networks, especially with the internet and mobile phone network expanding its limits and the possible methods of communication and transmission of information. With the increasingly rapid growth of this, there is an escalating need to ensure that the information to be in transmission made known only to the parties required only. Therefore, the current cryptographic techniques, gaining attention, and indirectly causes drastic change in the results of this research in cryptography. (Stinson D.R. 1995), (Menzes G.J. et al. 1977).

Since the 1990s, many researchers have observed an interesting relationship between chaos and cryptography. For example, sensitive to its initial value and has a cascading trajectory that covers the entire interval seems to be a classic model fulfills confusion and diffusion given by Shannon. (Shannon C.E. 1949).

> "*A transformation that has a good mix often formed by the combination of two simple operations are not cumulative. For example, Hopf has shown that a powder is kneaded in such a way can be blended with a sequence of operations. Flour is kneaded initially stocked to be a thin layer, then folded in two and continued operation of the fold, etc*"



© COPYRIGHT UPM

From the above statement, clearly shows that Shannon had actually discussed a mean toward chaos by stretching and then folding the information. This is a method that has been known in chaos theory (Devaney R. L. 1989). In fact, it is a basic rule to implement one or more non-linear mapping to design a modern ciphers, a non-linear mapping which can be considered as discrete values or discrete time representation of a chaotic system. As an effort to find the correlation between the latest encryption techniques and a study of the chaotic system of chaos and the AES cipher system was conducted. (Ruggiero D. *et al.* 2004), (Kocarev L. *et al*. 2004)

In order to discuss the relationship between chaotic dynamic system and its potential to form a cryptosystem, mathematical characteristics of chaotic dynamic system will be the core of discussion. Following denotes the dynamic system

$$X(k+1) = f\big(X(k)\big), X(0) \in I, k = 0,1,2, \ldots \quad (1.2.3)$$

where $I$ is either interval unity (Hatbusu T. *et al*. 1991) or square unity (Fridrich J. 1998) and $f: I \to I$ is non-linear continuous functions. The chaos of a dynamic system associated with the chaotic dynamic system Lyapunov's exponent. Lyapunov's exponent measures the strength of the sensitivity of the dynamic system of initial value. If a dynamic system is chaotic on the interval $I$, the existence of periodic points is limited to a set of zero measure. Next, it can be guaranteed that all periodic points of a chaotic dynamical system $f$ is characteristically rejected (Devaney R.L. 1989) is even a trajectory $X(k)$ will approach to a periodic cycle of a value $k$, it would avoid the cycle of the index that is greater than $k$.

Apart from having the knowledge of the periodic points, should we want to use the output of a chaotic dynamical system for the purpose of encryption, we will need to know the characteristics of output distribution. Previous studies and mathematical techniques related to it are available (Collet P. *et al*.1980).

### 1.2.4 Chaos based Symmetric Cryptosystem

Many of the features found in a chaotic dynamic system have its equivalence in cryptography. Table 1.2.3 shows the characteristics of equivalence.

**Table 1.2.3 Desirable characteristics of Chaos and Cryptography**

| Chaos property | Cryptographic property | Explanation |
|---|---|---|
| Ergodic | Confusion | The output has the same distribution for any input |
| Sensitive to initial values / parameters control | Diffusion with very small changes in the original text / secret key | A very small change in input can produce large changes in output |
| Mixed characteristic | Diffusion occurs with very small changes in the original text block from the entire original text | A very small change in the local area can produce a very large change in the whole space |

© COPYRIGHT UPM

| | | |
|---|---|---|
| Dynamics can be determined | Pseudo-randomness can be determined | A process can be determined can produce random behaviour (pseudo-random) |
| Structural complexity | Complexity (the attack on the algorithm) | A simple process has a very high rate of complexity |

In 1998, Baptista proposes a chaos-based cryptography system that uses a dynamic system with ergodic properties of the chaotic logistic mapping. Each "letter" will have a particular site in the interval [0,1]. Cryptographic system is implemented by iterating the logistic map. When the iteration is an element of a site specific alphabet, the number of iterations passed, $n$ will be taken. Then a random number will be generated, $k$ and compared with $n$. If $k > n$ then $n$ will be different cipher text of identical letters. Then, someone who wants to overcome these cryptographic systems will have to deal with text ciphertexts ciphers that can represent different characters. Therefore, the attacker is then confronted with a high probability of text ciphers (because each text ciphers have the same probability to represent any letter).

In 2003, Alvarez has reviewed the cryptographic system in his paper entitled "Cryptanalysis of a Discrete Chaotic Cryptosystem Using External Key" and has produced a one-time pad attack, a type of attack that can occur once the original text is known. This attack successfully overcomes chaos-based cryptography system dynamic system proposed by Baptista. This attack has been exploited successfully for text ciphers with ergodic nature that resembles a one-time pad attack by assuming the key. Method of attack is based on the symbolic dynamics of one-dimensional quadratic mapping.

Since Baptista's original proposal, many variant cryptosystems based on chaotic maps have been proposed for cryptographic implementation. In 2008, Ariffin attempted to modify the cryptosystem to enhance the performance of the original Baptista's cryptosystem via an example. Rhouma identified a flaw in the example that Ariffin put forward, specifically in step 4 of the encryption procedure, where it does not implement one-to one operation, resulting in failure to decrypt the ciphertext (Rhouma R. 2009).

A fractal set is a set that fits a physical world model better than regular arrangements involving smooth curves and surfaces. Iterated Function Systems (IFS) provide a convenient framework for the description, classification, and communication of fractals. Due to their complicated mathematical structure and deterministic nature, especially their recursive construction, it has many applications in physics, chemistry, biology, engineering, and recently in cryptographic systems. In this thesis a fractal map is discretized in order for it to be suitable for cryptographic applications. The discritized map will be utilized to enhance a cryptosystem utilizing the Baptista mechanism. Each resulting consecutive ciphertext from the Baptista encryption technique will be paired to represent a coordinate on the $xy$-plane. A discretized fractal map will then be in use to continue with the encryption operation. The result will be resistant toward Alvarez's one time pad attack.

Mathematical and empirical analyses are conducted to determine the security of our suggested cryptosystem. Careful considerations are conducted during the design of

this cryptosystem such that weaknesses that arise from the Baptista design will not occur. Mechanisms explaining the design of this new cryptosystem such that it does not inherit the weaknesses of the previous Baptista design are also detailed out.

### 1.2.5 Background for Fractal and Iterated Function System (IFS)

The theory of fractal sets is a modern domain of research. Iterated function systems have been used to define fractals. Such systems consist of sets of equations, which represent a rotation, a translation, and a scaling. These equations can generate complicated fractal images.

Given a metric space $(X, d)$, the space of all nonempty compact subset of $X$ is called the Hausdorff space $H(X)$. The Hausdorff distance $h$ is defined on $H(X)$ by,

$$h(P,Q) = max\{inf\{\varepsilon > 0; Q \subset N\varepsilon(P)\}, inf\{\varepsilon > 0; P \subset N\varepsilon(Q)\}\}, \qquad (1.2.5)$$

**Definition 1.2.5.1**

For any two metric spaces $(X,\ d_X)$ and $(Y,\ d_Y)$, a transformation $\beta: X \to Y$ is said to be a contradiction if and only if there exists a real number $s$, $0 \leq s \leq 1$, such that $d_y\left(\beta(x_i), \beta(x_j)\right) < sd_x(x_i, x_j)$, for any $x_i, x_j \in X$, where $s$ is the contractivity factor for $\beta$.

The following theorem, known as the contraction mapping theorem, states an important property of contractive transformations of a complete metric space within itself.

**Theorem 1.2.5.1** (Barnsley M. F. 1993)

Let $\beta: X \to Y$ be a contraction on a complete metric space $(X, d)$. Then, there exists a unique point $x_f \in X$ such that $\beta(x_f) = x_f$. Furthermore, for any $x \in X$, have $\lim_{n\to\infty} \beta^{o_n} = x_f$, where $\beta^{o_n}$ denotes the $n$-fold composition of $\beta$.

A fractal is constructed from a collage of transformed copies of itself. It is inherently self-similar and infinitely scalable. The transformation is performed by a set of affine maps. An affine mapping of the plane is a combination of a rotation, scaling, a sheer and a translation in $\mathbb{R}^2$.

**Definition 1.2.5.2**

Any affine transformation $\beta: \mathbb{R}^2 \to \mathbb{R}^2$ of the plane has the form,

$$\begin{pmatrix} u \\ v \end{pmatrix} = \beta \begin{bmatrix} x \\ y \end{bmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} = A\vec{X} + b \qquad (1.2.5.2.1)$$

where $(u, v), (x, y) \in \mathbb{R}^2$, are any point on a plane.

By considering a metric space $(X, d)$ and a finite set of contractive transformation $\beta_n: X \to X, 1 \leq n \leq N$, with respective contractivity factor $s_n$, proceed to define a transformation $B: H(X) \to H(X)$, where $H(X)$ is the collection of nonempty, compact subsets of $X$, by :



© COPYRIGHT UPM

$$A = B(A) = \bigcup_{i=1}^{N} \beta_i(Q) \; for \; any \; Q \in H(X) \qquad (1.2.5.2.2)$$

It is easily shown that $B$ is a contraction, with contractivity factor

$$s = \max_{1<n<N} sn \qquad (1.2.5.2.3)$$

The mapping $B$ is usually referred to as the Hutchinson operator. It follows from the contraction mapping theorem that, if $(X, y)$ is complete, $B$ has a unique fixed point $A \in H(X)$, satisfying the remarkable self covering condition.

$$A = B(A) = \bigcup_{i=1}^{N} \beta_i(A) \qquad (1.2.5.2.4)$$

### 1.2.6 The Relationship between Fractal, Chaos and Cryptography

Chaos theory has a close tie-in with fractals. Most of the attractors produced by chaotic dynamical systems are fractal sets. For example, the Lorenz attractor is a fractal of Hausdorff dimension equal to 2.073. The chaotic behavior of a fractal is used to encrypt data, in fractal cryptography there are no rounds, iterations are used instead, and the security is based in the non-determinism of a recursive function (for calculating the $n$-th iteration of a function you need to calculate $(n-1)$iteration first)

In the literature, fractal theory has proved to be suitable in many fields and particularly interested in various applications of image processing. First important advances are due to Barnsley M.F., who introduced the term of Iterated Function System (IFS) for the first time based on the self-similarity of fractal sets (Barsley M.F. 1996). Barnsley's work assumes that many objects can be closely approximated by self-similarity objects that might be generated by the use of IFS simple transformations. From this assumption, the IFS can be seen as a relationship between the whole image and its parts, thus exploiting the similarities that exist between an image and its smaller parts.

Consider that an IFS consisting of the maps,

$$w_i(x, y) = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e_i \\ f_i \end{pmatrix}, i = 1,2, \dots, N \qquad (1.2.6.1)$$

for $i = 1$. That is,

$$w_1 = \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix}, \qquad (1.2.6.2)$$

and let the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad (1.2.6.3)$$

consist of only elements within set $\{0, 1\}$.

Next, the $2 \times 1$ matrix



© COPYRIGHT UPM

$$B = \begin{pmatrix} x_i \\ y_i \end{pmatrix} \tag{1.2.6.4}$$

will consist of Baptista ciphertext values, and the matrix

$$C = \begin{pmatrix} e \\ f \end{pmatrix} \tag{1.2.6.5}$$

will be equal to zero (i.e. $C = 0$).

## 1.3 Thesis Organization

This thesis begins with the discussion on this research direction and notations will often be used. In Chapter two, the compression technique will be introduced. Introduction to data compression techniques will be classified broadly into their own category. In Chapter three, the definitions that will be used in a new approach to compression algorithm are presented. We will also discuss the options that we have on compression schemes. In Chapter four, researches related to chaotic dynamical systems, logistics and chaos mapping are discussed. This research aims to give a treatment for the one-time pad attack and for encryption procedures to implement one-to-one operation. The definitions and mathematical explanations for this phenomenon will also be introduced. We give an algorithm, if satisfied by a 'counter measure' method, would result in this cryptosystem being invulnerable against the one-time pad attack. As for the encryption procedures, we have implemented one-to-one operation to overcome the flaw in the example that Ariffin (2008) has put forward in step 4 of the encryption procedure. Next, a strategy has been developed, and if there is a 'counter measure' method that can meet the requirements in the strategy, then this strategy has facilitated the deployment of the practical possibility of Baptista cryptosystem. An example of a counter measure method that meets the requirements of these strategies is also given in this chapter. In the final chapter, conclusions for study are presented and further research that may take place to give this area a further depth has been recommended.

## 1.4 Research Objective

The objectives of this thesis are to

i. design an enhanced compression technique.
ii. design a formal treatment method to overcome attacks on the one-time pad attack.
iii. design methods to overcome the flaw found in the example that Ariffin has put forward in step 4 of the encryption procedure.

© COPYRIGHT UPM

## REFERENCES


Alvarez, Fernandez,E., Garcia,A., Jimenez,P., J. and Marcano, A.1999. New approach to chaotic encryption from *Phys. Lett. A* 263:373-375.

Alvarez, Montoya,G., Romera,F., M. and Pastor, G. 2000. Cryptanalysis of a chaotic encryption system from *Phys. Lett.A* 276: 191-196.

Alvarez, Montoya,G., Romera,F., M. and Pastor, G. 2003(a). Cryptanalysis of a chaotic secure comunication system from *Phys. Lett. A* 306: 200-205.

Alvarez, Montoya,G., Romera,F., M. and Pastor, G. 2003(b). Cryptanalysis of an ergordic chaotic cipher from *Phys. Lett. A* 311: 172-179.

Alvarez, Montoya,G., Romera,F., M. and Pastor, G. 2003(c). Cryptanalysis of a discrete chaotic cryptosystem using external key from *Phys. Lett.A* 319: 334-339.

Alvarez, Montoya,G., Romera,F., M. and Pastor, G. 2004. Cryptanalysis of dynamic lookup table based chaotic cryptosystems from *Phys. Lett.A* 326: 211-218.

Alvarez, G. and Li, S. 2006. Some basic cryptographic requirement for chaos- based cryptosystem from *Int. J. Bifur. Chaos* 16(8): 2129-2151.

Ariffin, M.R.K. and Nooraini, M.S.M., 2008. Modified Baptista type chaotic cryptosystem via matrix secret key from *Phys. Lett. A* 327: 427-430.

Ariffin, M.R.K. and Nooraini, M.S.M., 2010.Mathematical treatment for constructing a countermeasure against the one time pad attack from *Chaos Synchronization and Cryptography for Secure Communication*: *Applications for Encryption*, pp. 463-475.

Baptista, M.S. and 1998. Cryptography with chaos from *Phys. Lett.* A 240: 50-54.

Barnsley, M.F. and 1996. Fractal image compression from *Notice of the AMS* pp. 657-659.

Barnsley M.F. 1993. Fractal Everywhere, *2nd Ed. Academic Press Professional, Inc. , San Diego, CA, USA.*

Collet, P. and Eckmann, J.P., 1980. Iterated maps of the interval as dynamical systems from *Birkhuser,Basel.*

Devaney, R.L. 1989. An introduction to Chaotic Dynamical Systems from *Addison-Wesley, Redwood City, Carlifornia, USA*.

Fridrich, J. 1998. Symmetric ciphers based on two-dimensional chaotic maps from *Int. J. Bifurc. Chaos* 8:1259-1284.

Habutsu, T., Nishio, Y., Sasase, I. and Mori, S. 1991. A secret key cryptosystem by iterating a chaotic maps from Advances in Cryptology EUROCYPT91, Lecture notes in Computer Science 547: 127-140.


© COPYRIGHT UPM

Kocarev, L., Amato, P., Ruggiero, D. and Pedaci, I. 2004. Discrete Lyapunov Exponent for Rijndael block cipher from *Proceedings 2004 International Symposium on Nonlinear Theory and its Applications* NOLTA 2004: 609-612.

Menzes, G.J, van Oorschot, P.C. and Menzes, S.A. 1977. Handbook of Applied Cryptography from *CRC press/*

Ruggiero, D., Pedaci, I., Amato, P. and Kocarev, L. 2004. Analysis of the chaotic dynamic of Rijndael block cipher from *Proceedings RISP Int. Workshop on Nonlinear Circuit and Signal Processing* NCSP'04: 77-80.

Rhouma, R., 2009. Comment on modified Babtista type chaotic cryptosystem via matrix secret key from *Phys. Lett. A* 373: 3398-3400.

Shannon, C.E. 1949. Communication theory of secrecy systems from *Bell Systems Tech. J.* 28: 656-715.

Stinson, D.R. 1995. Cryptography: Theory and Practice from *CRC Press.*

Vergili, I. and Ycel, M.D., 2001. Avalanche and bits independence properties for the ensembles of random chosen $n \times n$ S-boxes from *Turkish J. Elect. Eng. Comput. Sci.* 9(2): 137-145.

Webster, A. and Tavares, S., 1986. On the design of S-boxes from *Proceedings of the Advances in Cryptology,* pp 523-534.

Ziedan, I.E., Fouad, M.M. and Salem, D.H., 2003. Application of data encryption standard to bitmap and JPEG image from *Proceedings of the Twentieth National Radio Science Conference* pp.1-8.

© COPYRIGHT UPM