Implementation of a Chaos-Based Symmetric Text Encryption Using Arduino Microcontrollers

Zahraa A Msekh\textsuperscript{1*}, Saad S Hreshee\textsuperscript{2}

\textsuperscript{1,2} Electrical Eng. Dept., College of Engineering, Babylon University
\textsuperscript{*} Corresponding author e-mail: zahraaaltay11@gmail.com
eng.saad.saffah@uobabylon.edu.iq

Abstract. Over the last few years, security becomes more important in any communication system. Several techniques have been implemented to transfer information in a secure way. One of the most important encryption techniques used in security is encryption based on a chaotic system. In this paper, a security chaotic algorithm has been proposed, studied and implemented for encrypting a text message. This work based on using two levels of one-dimensional chaotic maps (logistic map) with different initial conditions. In the experimental process, the original text on the receiver side was decrypted correctly 100\% (without any error). The key space measured by this system was (16×10\textsuperscript{64}) which is greater than the minimum key space value necessary to resist any brute-force attack. Also another analysis has been studied in this paper proved that the time plays a very important limitation in the encryption. The time effect on the attacker during its attempts to obtain the original text was very large and it could not get the text in the real or nearly the real-time.

Keywords: Communications Security, Chaotic Systems, logistic map, key space, Arduino.

1. Introduction
There are some problems in the security of information, especially in the text and voice communication, these problems represented by attackers. To prevent the attacks, the security system must have high-level of encryption. By encryption processes, the transmitted data will not be available for the people not have permission to get it [1, 2]. Cryptography was used since the beginning of the last century in military, diplomatic and government services [3]. Today communication system becomes the most necessary part of our daily lives with a variety of techniques. This variety gives the necessity to study the performance of the encryption methods. One of the important techniques used in cryptography is based on using chaotic algorithms [4, 5]. Chaos theory is applied in many areas like secure Communications, Spread Spectrum Modulation, Computer science, Physics, Engineering Mathematics, etc. [5, 6, 7]. Some researchers have pointed out that there exists a close relationship between chaos and cryptography, because chaos has properties such as ergodicity, mixing, randomness, complexity, unpredictably and the sensitivity to initial conditions [8, 9, 10]. There are two types of chaotic systems, chaotic map and chaotic flow. Chaotic map used with discrete time systems and represented by difference equations. Chaotic map has many types of representation such as logistic map, Henon map, Cat map, etc. [11]. Chaotic flow represented by differential equations that used with continuous-time systems and has various types such as Lorenz flow, Rössler flow, Chen's flow, etc. [12].
In this paper, the proposed system is based on using discrete information and the suitable chaos algorithm for this system is the chaotic map. Also, will achieving a high-security system to resist all types of brute force attacks. Where the size of the key space greater than $2^{100}$ (approximately $10^{30}$) [5,9].

1.1. Logistic map

Logistic map is a kind of chaos in discrete-time with one-dimensional chaotic function. It was first studied in the 1960s and it has characteristics that the values created by it are completely random and these values do not repeat itself even after a number of iteration in the period. Another characteristic is the high sensitivity to the initial values as show in Figure 1 and this increment the importance of the function [13].

![Logistic map sensitivity to initial conditions](image)

The difference equation that represent chaotic logistic map is [13]:

$$\chi_{n+1} = r \chi_n (\chi_n - 1)$$  \hspace{1cm} (1)

where: $\chi_n$ : the logistics parameter that ranges from (0 to 1), $r$ is the parameter of the system with range (0 to 4).

The logistic map behavior depends on the bifurcation parameter $r$, so, when $r$ is equal to:-

1) [0 to 1] the system has a fixed and stable point near to 0
2) [1 to 3] the system has a fixed and stable point near to $(r-1)/r$
3) [3 to 3.57] the will be a periodic attractor of $2m$ where $m=1,2,…$
4) [3.57 to 4] the system acts as chaotic system.

2. Proposed Model

The proposed system model is shown in Figure 2 and implemented by using Arduino microcontroller board ATmega2560. The information used in this system that may be letters, numbers or symbols which converted to ASCII code. This code will pass through two levels of encryption. The first level includes the first chaotic map that generates a sequence of pseudo random numbers used to encrypt the input data through an exclusive OR gate (XOR1). The second level used to encrypt the output of the first level with a code generated by the second chaotic map with another exclusive OR gate (XOR2). The second level used to increase the security by increasing the key space. Both sequences are generated from two logistic maps but with different initial conditions. The numbers of samples in the generated code by the two logistic maps are equal to the number of samples in the data. After these stages, the data encrypted (cipher text) will be transmitted through the channel to the receiver side. The cipher text will be decrypted with the same key of the transmitter side. After the decryption process, the final code is reconverted to characters, and finally, the sent text will be recovered again.
3. Experimental Implementation of the Proposed System

The circuit that represents the proposed system shown in Figure 1 is illustrated in Figure 3 and 4. The microcontroller used in this work is the Arduino boards ATMEGA2560 (two boards: one for the transmitter circuit and the second for the receiver circuit) in addition to a keypad 4×4 and two LCD to view the sent and received text. The LCD in the transmitter stage displayed firstly the entered text from the keypad and then the cipher text that will be sent. The keypad was programmed in the Arduino to make each button gives four characters to produce the missing characters. C language was used for programming Arduino.

The Transmitter part: Arduino of the transmitter circuit takes the message (plain text) entered from the keypad (keypad convert each character to ASCII code) and encrypts it with the code generated by the first chaotic map (map1) through the first exclusive OR gate (XOR1). The output of this stage then encrypted by the second chaotic map (map2) through another exclusive OR gate (XOR2). The implemented circuit for the transmitter part of the proposed system is shown in Figure 5. The receiver part: The receiver of Arduino will receive the encrypted data that transmitted through a wire channel, and decrypts it by revering the processes done in the transmitter side. The receiver has the same secret
keys used in the transmitter. Finally convert the data that decrypted into characters and display it on the LCD. The Practical model for the receiver part in the proposed system is shown in Figure 6.

![Figure 5. Practical implementation of the transmitter circuit.](image1)

![Figure 6. Practical implementation of the receiver circuit.](image2)

### 3.1. Experimental Results

Figure 7 illustrates some experimental results, which is show some examples of transmitted and received texts.

![Figure 7. Experimental implementation and work](image3)

### 4. Mathematical Model and Results

A Simulation Analysis to Study The Proposed System and compare its results was achieved by using MATLAB by building a program to describe the mathematical model of the experimental work. Figure 8 shown below the encryption and decryption codes had programmed by MATLAB:

```matlab
%Encryption
orgainltext="chaos system"
%r=3.99;
xel1=0.1;
xel2=0.4;
for i=1:length(orgainltext);
xel1=r*xel1*(1-xel1)
str1 = dec2bin(xel1);
a(i)=bitxor(uint8(orgainltext(i)),uint8(100*xel1));
ciphertext3(i)=char(a(i));
xel2=r*xel2*(1-xel2);
map2(i)= xel2;
b(i)=bitxor(uint8(a(i)),uint8(100*xel2));
ciphertext2(i)=char(b(i));
end

%Decryption
r=3.99;
xd2=0.4;
xd1=0.1;
for i=1:length(orgainltext);
xd2=r*xd2*(1-xd2);
xd1=r*xd1*(1-xd1);
c(i)=bitxor(b(i),uint8(100*xd2));
ciphertext(i)=char(c(i));
d(i)=bitxor(c(i),uint8(100*xd1));
recivedtext(i)=char(d(i))
end
```

![Figure 8. The mathematical model for the proposed system (a) Encryption process, (b) Decryption process](image4)
Table 1 shows some plain and encrypted text that sent to receiver side.

Table 1. plain text and cipher text in the simulation

| Plain text   | Cipher text    |
|--------------|----------------|
| chaos system | #5{4v'vlT-n   |
| we are done  | 78::wb%qH7     |
| zahraa abdulrazzak | :<r)df%tE=ovgKR# |

5. Strength Tests of the System

In this paper the strength of the system studied through two elements that prevent any attack to get the encrypted message. The first one is the key space and the second one is the time needed to break the encryption key.

5.1. Key Space

The size of the key space (Secret Keys) should be greater than $2^{100}$ (approximately $10^{30}$) to prepare high-security system and resist all types of Brute force attack [14, 15, 16]. If the key is strong, the attacker's chances are very weak. To prove that the system has high security the key space (sensitivity) must be Measured and analysis. This is the main part of the performance analysis in security to design a system of perfect encryption for resisting the attacker. The key space measured by applying very small change in the initial conditions which achieved by using Lyapunov Exponents.

The key space for one dimension

$$K = \frac{1}{S} \times R_i$$

(2)

Where $K$ is the key space, $S$ is the sensitivity in each dimension, $R_i$ is the range of function to each dimension.

The key space for n dimensions is:

$$K_n = \prod_{i=1}^{n} K_i$$

(3)

Table (2) illustrates the probabilities in which the attacker tries to get the original text.

Table (2). The Probabilities of attacking.

| The probabilities                        | Results                                                                 |
|------------------------------------------|-------------------------------------------------------------------------|
| 1 The attacker does not recognize the    | He cannot get any information, because he                              |
| system used.                             | must define the type of the system.                                     |
| 2 The attacker recognizes that the       | He cannot get any information, because there are many types of chaos   |
| system used is chaos system.             | systems and it is divided into discrete and continuous with map and    |
|                                          | flow characteristics.                                                 |
| 3 The attacker recognizes that the       | He cannot get any information, because the map also has many types.   |
| system used is chaos system and select   |                                                                          |
| the map type.                           |                                                                          |
| 4 The attacker recognizes that the       | He cannot get any information, because he does not know the number of  |
| system used is chaos system and select   | stages used, and does not known the using of the XOR gate.             |
| Logistic map.                           |                                                                          |
| 5 If the attacker has the knowledge      | He cannot get any information, because that his trial and error will  |
| about all the system without the         | take very very long time.                                              |
| parameters and initial conditions.       |                                                                          |
| 6 If the attacker has the knowledge      | He cannot get any information, because that his trial and error will  |
| about the system type and has all the    | take very long time.                                                   |
| parameters and initial                   |                                                                          |
Depending on table 2 (step-6), logistic map1 is proposed to be changed in one of its initial conditions. The changes are illustrated in table 3 with steps $10^i$ ($i=1, 2, 3, \ldots$). Table 3 will explain how the original and encrypted text will be changed with each step of key changing and the number of detected characters received in each case. The value of the sensitivity that we obtained in this work (according to table 3 and based on the Lyapunov exponent) is $(10^{16})$

Then:

$$K_i = 10^{16} \times R_i$$

The key space for n dimensions

$$K_n = \prod_{i=1}^{n} [10^{16} \times R_i] = (10^{16})^n \prod_{i=1}^{n} [R_i]$$

Table 3. Original text (plaintext) and encrypted text (Cipher text) for each step of sensitivity.

| Step of $S$ | plaintext | Cipher text | No. of detected char. |
|-------------|-----------|-------------|-----------------------|
| $10^1$      | "There are several points of interest for using chaos in encryption." | FTkc~g([&^#F^A^Cf/KQpj:nID)\_U%7] e.\z2s~2r_y#*gw* C Yj | 0 |
| $10^2$      | "There are several points of interest for using chaos in encryption." | !We+f+b[*SF _#C |1z1.kys0zbJ-7UV8 lhh0 XH8nwKa,&K | | | |
| $10^3$      | "There are several points of interest for using chaos in encryption." | "Tkcx+B#&jsMHU %Do4hmwyK.Y][07#nt[hPH&@J*2[yj4_zS%`u* H!H- | 2 |
| $10^4$      | "There are several points of interest for using chaos in encryption." | "These!c{T3M'+-_3R XZ_6$*UD_0|Jy*xoL_+=/Y!(J|B7LC5-F^A^k | 4 |
| $10^{14}$   | "There are several points of interest for using chaos in encryption." | "There are several points of interest | 37 |
| $10^{15}$   | "There are several points of interest for using chaos in encryption." | "There are several points of interest | 40 |
| $10^{16}$   | "There are several points of interest for using chaos in encryption." | "There are several points of interest for usi%h` mas %GeVa 9sS4'K1 $ | 45 |
| $10^{17}$   | "There are several points of interest for using chaos in encryption." | "There are several points of interest for using chaos in encryption." | 70 |

In this work, two logistic One-dimensional maps are used and each map has two parameters ($X_n$ and $r$), then the key space will have four dimensions.

$$K_4 = (10^{16})^4 \left[(R_x1 \times R_t1) \times (R_x2 \times R_t2)\right]$$

Where $R_x$ and $R_t$ the ranges of parameters are depends on the bifurcation theorem.

For ($R_x = 1$ and $R_t = 4$)

$$K_4 = 16 \times 10^{64}$$
The obtained key space \( K_4 \) for this system is greater than \( (10^{30}) \) which indicates that the proposed system is very strong and resistant against the brute force attack.

5.2 Time

Time spent by the attacker to break the encryption is one of the basic elements in the encryption standard. If the system contains a high security keys. It will effect on attacker to get the original text, because the attacker will try to decode and get the keys for the system, this will take a very long time. If the key is high, the attacker’s time to get the text will be very long and the message will be expiring.

In this paper the attacker's time needed to get the original text with an assumption that he knows the system and all its parameters except one in one map only (for example the parameter \( (X_n) \)) (see table (2) (step-6)) are calculated depending on the properties of the personal computer that used in this simulation: (Processor: Intel Core i7, Operation System: 64bit, Speed: 2.5GHz, RAM: 4GB).

In the first step, we calculate the time spent at each step of the sensitivity from \( (10^{-1} \) to \( 10^{-16} \)). While the cumulative time is calculated in the second step. Table 4 shows the calculated time in seconds for each step of the sensitivity and the cumulative attack time in seconds and hours.

| Step of S | Cumulative time [sec] | Cumulative time [Hrs] |
|-----------|-----------------------|-----------------------|
| \(10^{-1}\) | 0.04863 | 0.04863 | 0.0000013508 |
| \(10^{-2}\) | 0.442533 | 0.491163 | 0.00013643 |
| \(10^{-3}\) | 4.381563 | 4.872726 | 0.00135354 |
| \(10^{-4}\) | 43.771863 | 48.644589 | 0.013512 |
| \(10^{-5}\) | 437.674863 | 486.319452 | 0.135089 |
| \(10^{-6}\) | 4376.704863 | 4863.024315 | 1.3508 |
| \(10^{-7}\) | 43767.004863 | 48630.02918 | 13.5083 |
| \(10^{-8}\) | 437670.0049 | 486300.0341 | 135.08 |
| \(10^{-9}\) | 4376700.005 | 4863000.039 | 1350.8 |
| \(10^{-10}\) | 4.3767*10^4 | 48630000.04 | 13508.33 |
| \(10^{-11}\) | 4.3767*10^5 | 48.63000*10^5 | 13508.333*10^4 |
| \(10^{-12}\) | 4.3767*10^6 | 4.863000*10^9 | 13508.333*10^7 |
| \(10^{-13}\) | 4.3767*10^7 | 4.863*10^10 | 13508.333*10^10 |
| \(10^{-14}\) | 4.3767*10^8 | 4.863*10^11 | 13508.333*10^13 |
| \(10^{-15}\) | 4.3767*10^9 | 4.863*10^12 | 13508.333*10^16 |
| \(10^{-16}\) | 4.3767*10^10 | 4.863*10^13 | 13508.333*10^20 |

6. Conclusions

Chaotic encryption system has been proposed, studied and implemented for encrypting a text massage. The system based on using two level of one-dimensional chaotic maps (two logistic maps) with different initial conditions. The implemented system has been designed with simple encryption process to reduce the microcontroller operating time. The system implemented by Arduino microcontroller and the speed of the operations in the experimental test of the system was perfect and very accurate to be in the real time. From the experimental results, it is clear that there is no expansion founded in the encrypted text (size of the encrypted text is equal the size of the original text) and the received text correct 100% (without any error). Using more than one Logistic Map lead to increase the key space because the system will have more dimensions and will be very good for encryption, very strong to prevent any attack from any brute force. In this work the key space is \( (16*10^{64}) \) which is greater than specified value of key space to resist brute force attack. Time effect: the attacker takes a very long time to get and recover the original plain text, where it may take several days, months or years in some cases depending on the attacker PC speed. This characteristic put the proposed system
in one of the best ways to get very secure communication systems and make it stronger to prevent any attack.

7. References

[1] Nguimdo RM. Chaos and Synchronization in Opto-electronic Devices with Delayed Feedback. Thesis. 2011;

[2] Principles and Applications of Chaotic Systems William Ditto and Toshinori Munakata. Commun ACM. 1995;38(11).

[3] Linda FR, Hammami S, Benrejeb M, Borne P. Synchronization of discrete-time hyperchaotic maps based on aggregation technique for encryption. Int Multi-Conference Syst Signals Devices, SSD 2012 - Summ Proc. 2012;(2).

[4] R Ekhande R. Chaotic Signal for Signal Masking in Digital Communications. IOSR J Eng. 2014;4(2):29–33.

[5] Hreshee SS, Mahdi A, Jawad AK. Digital Chaotic Scrambling of Voice Based on Duffing Map. Commun Eng J [Internet]. 2016;1(2):16–21.20160102.11

[6] Andrievskii B. Control of Chaos: Methods. 2004;65(4):505–33.

[7] Mahdi A, Hreshee SS. Design and implementation of voice encryption system using XOR based on Hénon map. Al-Sadiq Int Conf Multidiscip ITCommun Tech Sci Appl AIC-MITCSA 2016. 2016;4(1):82–6.

[8] Riaz A, Ali M. Chaotic communications, their applications and advantages over traditional methods of communication. Proc 6th Int Symp Commun Syst Networks Digit Signal Process CSNDSIP 08. 2008;21–4.

[9] Hikmat N. Abdullah and Saad S. Hreshee, Ameer K. Jawad, "Design of Efficient Noise Reduction Scheme for Secure Voice Masked by Chaotic Signals", Journal of American Science Vol. 11, Issue 7, pp. 49-55, 2015

[10] Management IM, Url E. Northumbria Research Link. 2018;25–35

[11] Shaerbaft S, Seyedin SA. A secure chaos-based communication scheme in multipath fading channels using particle filtering. Iran J Electr Electron Eng. 2012;8(1):1–9.

[12] Tang S, Chen HF, Hwang SK, Liu JM. Message encoding and decoding through chaos modulation in chaotic optical communications. IEEE Trans Circuits Syst I Fundam Theory Appl. 2002;49(2):163–9.

[13] M. Atheer, “FPGA Based Image Encryption Using Chaotic Systems”, PhD. thesis in Electronic Engineering University of Technology, October 2016.

[14] Sivasankari S, Balamurugan CR. E Mbedded C Ontroller B Ased M Ultilevel. 2014;3(2):81–9.

[15] Weik MH, Weik MH. Encryption Standard. Comput Sci Commun Dict. 2000;6(1):518–518

[16] Kharel R, Busawon K, Ghassemlooy Z. Modified chaotic shift keying using indirect coupled chaotic synchronization for secure digital communication. 3rd Chaotic Model Simul Int Conf CHAOS 2010. 2010;(June):1–4.

[17] Kamran Yeganegi et al 2020 J. Phys.: Conf. Ser. 1530 012110.