Secure Biometric Authentication System using Chaotic Encryption

Abirami S[1], Harini T[2], Annapoorani N[3]

[1]*Assistant Professor, Dept. of ECE, Mepco Schlenk Engineering College, Sivakasi, India*
[2]*Student, Dept. of ECE, Mepco Schlenk Engineering College, Sivakasi, India*
[3]*Student, Dept. of* ECE, *Mepco Schlenk Engineering College, Sivakasi, India*

---***---

Abstract -*Biometrics based authentication systems recognize individuals based on their anatomical traits or behavioral traits and therefore offers several advantages over traditional authentication methods such as passwords and identity documents. Fingerprint recognition is a one reliable solution in biometrics based authentication systems. Despite their advantages the potential breaches of security and secrecy of the user's data are a still a lingering concern. Therefore, biometric template protection to avoid identity theft has become a major concern in today's security needs. In this paper, a robust fingerprint template protection scheme based on chaotic encryption which has extreme sensibility on initial conditions with confusion and ergodicity with diffusion is presented by using the logistic map and Murillo-Escobar's algorithm. In contrast with other approaches presented in literature, a complete security analysis in both statistical level and implementation level is presented inorder to justify the cryptographic strength of the proposed methodology. Based on the obtained results, it can be inferred that the proposed embedded authentication system is highly secure, effective and cheap, which are vital for any authentication system to gain public confidence for implementation in real time secure access control systems.*

Key Words: Biometric Template, Fingerprint, Logistic Map, Murillo-Escobar's algorithm, Cryptographic Strength etc

1. INTRODUCTION

At First, Feature transformation and biometric cryptosystem are designed for biometric template protection scheme. But these two system are not satisfy the requirement of biometric template protection algorithm and then the security provided by this two systems is very poor, when the value is stored in the database. The attacker can get the value which is stored in the database. To prevent this, DES algorithm is used for protection this system also easily hack by the attacker because of low number bits used in thus system. (Jain & Uludag, 2003; Soutar, Roberge, Stoianov, Gilroy, & Vijaya Kumar,1999). Currently, 3DES (Triple Data Encryption Standard) and AES (Advanced Encryption Standard) are used as symmetric data encryption. AES has advantage as speed, low memory space, easy to implement, and it is based in permutation-diffusion architecture. But its drawback is its speed, it does the process at low speed and the number of keys it considered is also high. It is not a secure system to keep the encrypted template to be safer. The RSA (Rivest, Shamir, Adleman) algorithm is an asymmetric data cipher with security advantage but it is slow than any other symmetric cipher. Recently, the DNA (Deoxyribonucleic acid) characteristics have been proposed for text encryption where the four DNA basis are characterized by binary data, DNA complement operations are used to data encryption, and DNA sequences are used as secret key. (Bordoa, M., & Tornea, O. (2010). DNA secret writing techniques. In 8th InternationalConference on communications (pp. 451-456)). By other hand, chaos has excellent properties as mixing data, ergodicity, initial condition sensitivity, control parameters sensitivity, etc., all them are very useful to design cryptographic algorithms for text or images. In this paper, a novel symmetric text encryption algorithm based on chaos is presented. The algorithm uses the plain text characteristics to resist a chosen/known plain text attack with just one permutation, diffusion round (change the position and the symbol value) and two logistic maps. Also, a 32 hexadecimal digits (128 bits) secret key is used. In addition, the four properties of chaos system are verified.

2. BIOMETRIC SYSTEM

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. The physiological characteristics are related to the shape of the body such as fingerprint, palm veins, face recognition, DNA, Hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, such as typing rhythm, gait, and voice. Due these properties, biometrics has been used to identify or authenticate users in a biometric system. (Mihailescu ,2014). Biometric authentication systems can be more convenient for the users since there is no password to be forgotten or key to be lost and a single biometric trait (e.g., fingerprint) can be used to access several accounts without the burden of remembering passwords. This technique is becoming more popular than traditional identification techniques such as identification card (ID), password and personal identification number (PIN).Biometric identification follows the following steps: At first, the biometric sample is taken from an individual and the corresponding algorithm is done to protect the data. Similarly, the same procedure is repeated for group of individuals and stored in a database. All these steps are known as enrollment process. (Admek, Matsek, & Neumann, 2015, Kevenaar et al., 2010).At one time a person performs the enrollment process, he/she can identify or distinguish an individual from a larger set of individual biometric records, i.e. one-to-many matching or authenticate (a live biometric sample or test sample presented by a person is compared with a stored sample, i.e. one-to-one matching) by presenting his/her biometric sample in the system, which will compare the submitted sample with stored sample in the database and further, the matching process is done. If the live biometric sample is matched with any one of the sample in a database, the person is recognized and the system will accept him/her. Otherwise, the person is not recognized,i.e.,he/she will be rejected. While dealing with the reliability of a biometric system, there be some variance in the presented sample with the stored reference sample in the matching process by an inexact process i.e., the biometric system is not 100% accuracy to produce the result. There are two methodologies to measure the accuracy of the biometric system, False rejection rate (FRR) and false acceptance rate (FAR). FRR is how many rejects (incorrectly) performs the biometric system, i.e. when the system rejects a legitimate user. FAR is how many acceptances (incorrectly) perform the biometric system, i.e. when the system incorrectly matches a biometric sample with a wrong stored reference sample, leads to misidentification.

3. ATTACKS IN BIOMETRIC SYSTEM

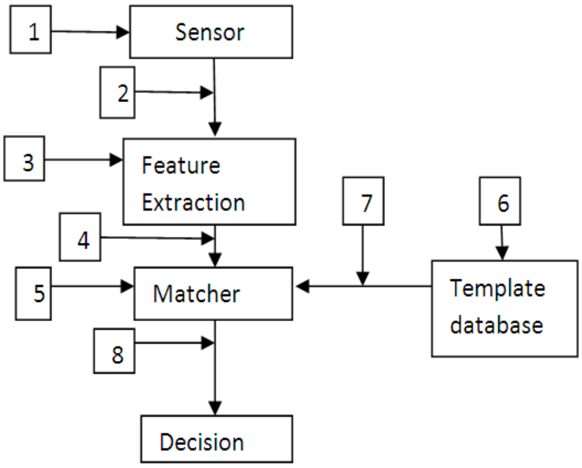


Fig 1: Shows the attacks in biometric system

The biometric template will experience 8 type of attacks such as, attack on sensor, attack on Feature extraction, in matching process, in decision making, template database is shown in the above fig 1. Comparing with all attacks, the attack on template database is a serious attack since it leads to wrong decision. Due to the security challenges, the Feature Transform and Biometric cryptosystem have been introduced in biometric system with some advantages and also it consists of some disadvantages but its main objective is to keep biometric template to be revocable. There are four main requirements while designing biometric template algorithm, they are revocability, Diversity, Security and Performance. So in order to pacify all the security attacks and the requirements to meet biometric algorithm, the biometric scheme is combined with the chaotic encryption. The reason to choose the chaotic encryption is because of its cryptographic property. The algorithm followed to increase the security is known as *Murillo Escobar's Algorithm*.

4. AUTHENTICATION SYSTEM

The enrollment process starts with the registration of a new authorized user. At first, from the fingerprint reader module, the fingerprint's plaintext value is taken. The random secret key of 32 hexadecimal digits is chosen and the secret key is divided into four sections, with the help of this initial condition and control parameter is found out. Then the 2172 iteration is made for logistic map 2. Then another logistic map is designed using the values of previous logistic map. Then encryption is performed. Similar process is repeated for group of samples and stored in a database. The test sample is compared with the database samples, if matched, the user is authenticated. Otherwise the user is not authenticated. The following fig 2 shows the flow of authentication system involved in our proposed scheme.

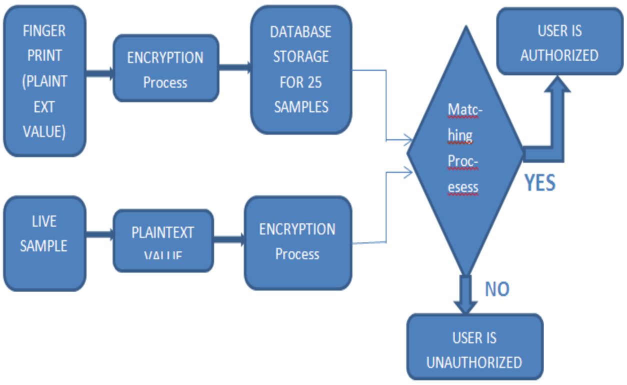


Fig 2: Flow diagram for authentication system

5. ENCRYPTION ALGORITHM

The proposed encryption algorithm is based on Murillo Escobar's algorithm. A plain text template $P^{\in(0,255)}$ of length 2072 bytes from the data is read by the fingerprint module. (Murillo-Escobar et al., 2014, 2015).The pseudorandom sequences generated by a chaotic system are used to convert the plaintext template into encrypted template. The one-dimensional logistic map is known as the simplest non-linear chaotic system that achieves clearly the chaos route. The logistic map is described as:

$$x_{i+1} = ax_i(1-x_i)$$

where, $x_i \in (0, 1)$ and control parameter $a \in (3.999, 4)$.

The one-dimensional logistic map is used due to its several advantages such as simple structure, easy to implement in digital systems due to its discrete nature, low implementation resources, low memory consumption and high speed data generation. Nevertheless, the logistic map has some disadvantages when it is used in cryptography such as chaotic ranges discontinues, distribution not uniform, small space key and periodicity in chaotic ranges . In countermeasure, the proposed solutions in encryption algorithm avoids the disadvantages while maintaining its advantages.

5.1. SECRET KEY DEFINITION

A 32 Hexadecimal digit is initially assumed as the secret key (112233445566778899AABBCCDDEEFF), which is a random key characterized by 32 hexadecimal digits. The secret key is divided in four sections to generate the initial condition and control parameter of two logistic maps. Any key used here is considered as strong since it follows chaotic sequence. These considerations avoid the chaotic ranges discontinues, small space key and periodicity in chaotic ranges of the logistic map. By using the expression in the below table 1,the control parameter and initial condition for logistic map 2 are calculated.

5.2. CALCULATION OF Z

The Z value is essential to calculate since Confusion and Diffusion requires Z value and it also increase the sensitivity at bit level in both plain text and secret key. All plain template elements are summed with chaotic data from logistic map 2 to calculate Z. First, the logistic map 2 is iterated for 2172 times by using $a_2$andx_{20}.This generates the chaotic sequence x^{L2} with 10^{-15} decimal precision. Then all plain elements are summed with xL2 as follows

$$S = \{S + [P_i * x^{L2}_{2173-i}] + x^{L2}_{2173-i}\} \bmod 1$$

where i=1,2,3.....2072.

P_i represents the plaintext element I, S is a variable initialized to zero, x^{L2} is the chaotic sequence and do the modulo operation.The next operation is determined by

$V = round(S * 94) + 32$ where V Є [1,255]

Finally, Z value is calculated by,

Z=V/256 where V Є [0,1]

5.3. ENCRYPTION PROCESS:

The confusion and diffusion process is implemented in encryption algorithm, where all plaintext elements are permuted and transformed according with chaotic data generated by the logistic map 1.

The chaotic sequence x^{L1}= {x_1^{L1}, x_2^{L1} ... x_T^{L1}}is calculated by using Z, T=5000 iterations, control parameter a_1 and initial condition x_{10} from table given below. It has decimal precision of 10^{-15} and x^{L1} Є (0, 1).For the confusion process, the sequence is calculated by the below expression

$$Q_i = round(x^{L1}_{2928+i} * 2071) + 1$$

where i=1,2,3.....2072. QЄ [1, 2072] is the pseudorandom position vector for confusion process. If all plaintext elements are permuted, then the encryption has an optimized confusion process.

For Diffusion process, the sequence is calculated by

$$F_i = \{(x^{L1}_{2928+i} * 1000) + Z\}$$

where i=1,2,3. . . 2072 and F_i Є(0,1) is a vector with 2072 length with 10^{-15} decimal precision. This process increase the security of the encryption process against the powerful chosen/known plain template Cokal & Solak, 2009; Li, Chen, &Halang, 2009; Rhouma, Solak attack, which have broken several cryptosystems based on chaos. (Alvarez & Li,2009; Balaji & Nagaraj, 2008;, & Belghith, 2010; Solak, Cokal,Yildiz, & Biyikiglu, 2010; Wang, Liao, Xiang, Wong, & Yang, 2007).

Then, Fi is transformed from [0,1] to [0,255] as follows

$$Y_i = round(M_i * 255)$$

where i=1,2,3. . . 2072, Y_i Є [0,255] is a vector with 2072 length.

Finally, the encryption process is based on Q as pseudorandom confusion vector and Y as

pseudorandom diffusion vector. The encryption process is as follows

$$E_i = (P(Q_i) + Y_i) \bmod 256$$

Where i =1, 2, 3. . . 2072, P is the plain template and E Є [0, 255] is the encrypted template to store in data base or transmit over an insecure channel.

The Z value must be add in the cryptogram E in the position 2073 as follows

$$E_{2073} = V$$

5.4. DECRYPTION PROCESS:

First, Z is extracted from the cryptogram with the following expression

$$Z = E_{2073} / 256$$

Then, x^{L1} is generated with the same secret key used in encryption process. Then, Qi and Yi are calculated as in encryption process. Finally, the encrypted template is decipher with the following expression

$$D(Q_i) = (E_i - Y_i) \bmod 256$$

where i =1, 2, 3. . . 2072, Q is the pseudorandom confusion vector, Y is the pseudorandom diffusion vector, E is the cryptogram and D is the recovered fingerprint template.

Table 1: Initial condition and control parameter

Secret Key	Control Parameter	Initial Condition
32 HEX digits	$H_1, H_2, \ldots\ldots, H_{32}$ Where H Є[0-9,A-F]	
Calculation	$A = ((H_1, H_2, \ldots, H_8)_{10})/(2^{32}+1)$ $B = ((H_9, H_{10}, \ldots, H_{16})_{10})/(2^{32}+1)$	$C = ((H_{17}, H_{18}, \ldots, H_{24})_{10})/(2^{32}+1)$ $D = ((H_{25}, H_{26}, \ldots, H_{32})_{10})/(2^{32}+1)$
Logistic 1	$a_1 = 3.999 + [((A+B+Z) \bmod 1) * 0.001]$	$x_{1_0} = (C+D+Z) \bmod 1$
Logistic 2	$a_2 = 3.999 + [((A+B) \bmod 1) * 0.001]$	$x_{2_0} = (C+D) \bmod 1$
Range	$3.999 < a_{1,2} < 4$	$0 < x_{1_0}, x_{2_0} < 1$
Precision	10^{-15},where (a mod b) = (a – b) *(a/b) with b ≠ 0	

6. MATCHING PROCESS:

The fig 3 shows the flow of matching process. At first, 25 fingerprints from fingerprint scanner were read and then the encryption and decryption process is done using the matlab software. After this, the encrypted value for 25 samples are stored in the database. The test image is given through the fingerprint reader and the encryption process is done for that particular test image. Finally, the encrypted value of test image is compared with the 25 samples which is already stored in the database in the matlab software. If it is matched, then the user is authenticated and if not, the user is unauthorized to access the system. This flow is shown below using the flow diagram.

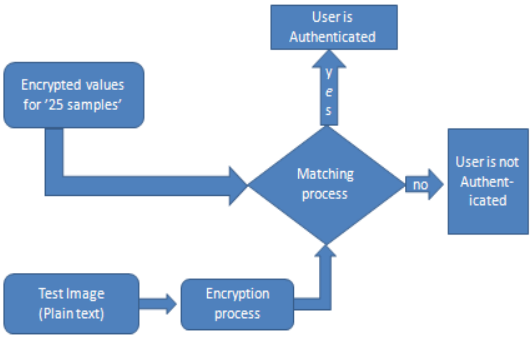


Fig 3: Flow diagram of matching process

7. EXPERIMENTAL RESULTS:

7.1. ENCRYPTED TEMPLATE ANALYSIS:

A secure encryption algorithm must be highly sensitive at input, i.e. small variations (one bit) in a plaintext should produce large variations in the encrypted template. This can be proved the comparing the encrypted values obtained for small variations of the position of the finger (for authenticated person). In the below fig 4, the 'red color' indicates the encrypted template for authenticated person by placing a finger in a proper manner and the 'green color' indicates the same authenticated person by slightly varying the position of their finger. Through this analysis the sensitivity of encrypted value for plain template can be proved.

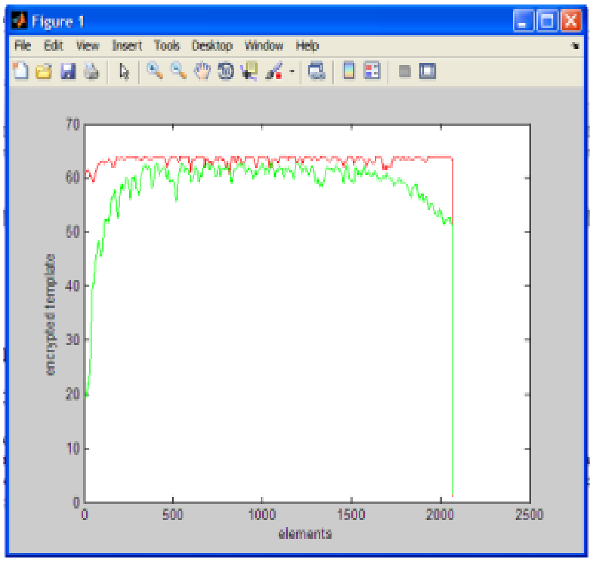


Fig 4: Sensitivity of encrypted value

7.2 KEY SENSITIVITY ANALYSIS:

A cryptographic system must be highly sensitive at small variations (at bit level) in secret key, in both encryption and decryption process. The analysis on the sensitivity of the key between the proper secret key and random key which is given by the user is done inorder to estimate the cryptographic strength of the algorithm. Through this the strength of the encrypted value is proved. If only the user knows the secret key they can access the system. The analysis of key sensitivity is shown in the following fig 5, in which the red color indicates the proper secret key given by the user and the blue color indicates the random key.

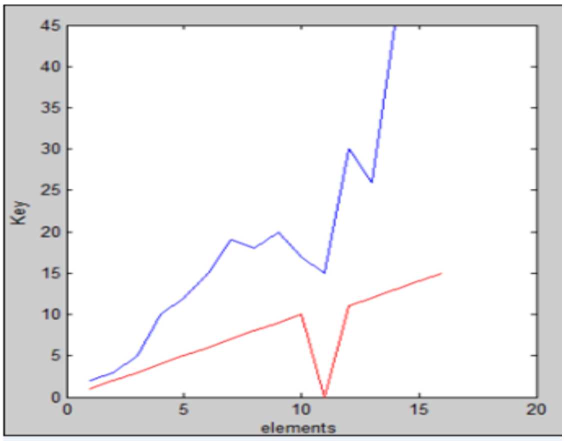
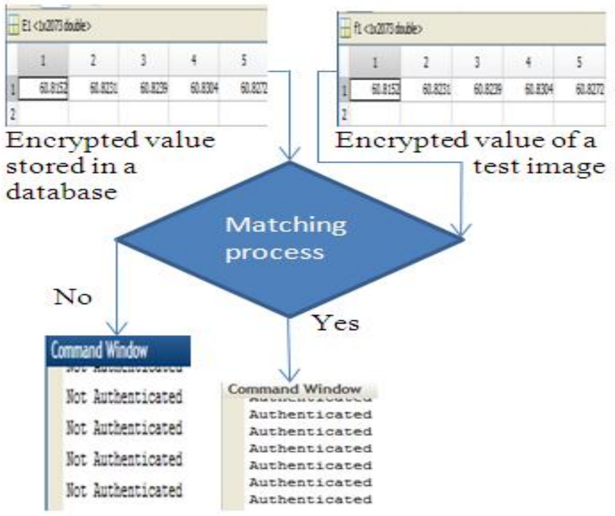


Fig 5: Analysis of Key Sensitivity

7.3 IMPLEMENTATION:

The above Murillo Escobar's algorithm is applied for 25 fingerprint images using matlab software. The results of Encrypted value for 25 images are stored in a database i.e., the encrypted for all 25 samples are stored in a text file and it is retrieved by using matlab. Then the test image is obtained from a fingerprint reader module and encryption process is done for it. Thus the encrypted results of test image are compared with the results stored in a database. If it is matched, the user is authenticated. If not, the user is not authenticated. Fig 5 shows the implemented result which was obtained in matlab software. Here, encrypted value was taken for matching process which gives the security to the proposed system.



	1	2	3	4	5
1	60.8152	60.8231	60.8239	60.8304	60.8272
2					

	1	2	3	4	5
1	60.8152	60.8231	60.8239	60.8304	60.8272
2					

```
Not Authenticated
Not Authenticated
Not Authenticated
Not Authenticated
```

```
Authenticated
Authenticated
Authenticated
Authenticated
Authenticated
Authenticated
```

Fig 6: Implemented result in software

After simulation analysis the proposed algorithm was implemented using Aurdino[UNO R3] to prove its versatility for any embedded authentication system required for the security of the appliances. The red light glows on the Aurdino[UNO R3] when the users encrypted fingerprint matches with that of the template. The cost of implementation is cheap making it cost less for embedding in biometric authentication system.

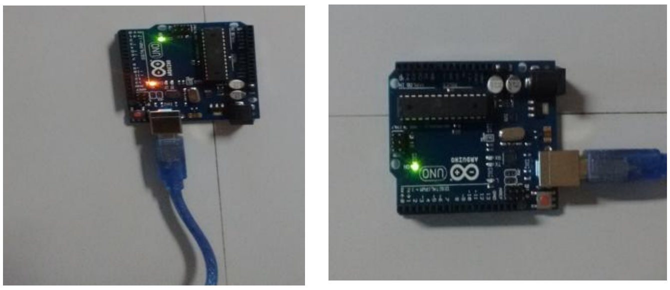


Fig 7: Implementation in Aurdino

8. APPLICATION:

The proposed algorithm implementation can be used in the areas, where the high level of security is needed. Especially, in the mobile devices such as, in smart phones which is more convenience and secure. The following image shows the authentication system involved in the smart phones by using fingerprint recognition technique.

Fig 8: Authentication in smart phones

9. CONCLUSION:

In this paper, a robust fingerprint template protection algorithm based on chaotic encryption is proposed for a highly secure embedded biometric authentication system. The confusion and diffusion introduced due to chaotic encryption proves the robustness of the algorithm. The analysis of key sensitivity and sensitivity of encrypted value validates the algorithm to be highly efficient for real time applications. Apart from analysis the algorithm is also implemented in embedded biometric authentication system which proves it versatile for all electronic gadgets introduced in modern era.

REFERENCES

[1] Admek , M., Mastek M.,Pneuman p," Security of Biometric systems", Procedia Engineering, vol.100, 2015, pp.169-176.

[2] Mihailescu, M.I ," New enrollment scheme for Biometric template using chaos based cryptography", Procedia Engineering, vol.69, 2014, pp. 1459-1468.

[3] Liu, R,"Chaos-based fingerprint images encryption using symmetric cryptography" In 9th International conference on fuzzy systems and knowledge discovery, 2012, pp. 2153–2156.

[4] M.A. Murillo-Escobar , C. Cruz-Hernández ,F. Abundiz-Pérez , R.M. López-Gutiérrez," A robust embedded biometric authentication system based on fingerprint and chaotic encryption",vol.42, 2015, pp.8198 -8211.

[5] Kevenaar, T., Korte, U., Merkle, J., Niesing, M., Ihmor, H., Busch, C., & Zhou, X,"A reference for the privacy assessment of keyless biometric template authentication system",in proceeding engineering, 2010,pp.45-56

[6] Abhyankar, Vijayat, Kumar, & Schuckers,"Encryption of biometric templates using one time biometric transform algorithm",in CIIT International Journal of Biometric and Bioinfomatics,2009, pp.1-8.

[7] Alvarez & Li,"Some basic cryptograpic requirements for chaotic basedcryptosystem",in International Journal of Bifurcation and Chaos,vol.16(8),2006, pp.2129-2151.

[8] Jain A.K, Nandakumar.K,& Nagar.A,"Biometric Template Security"in EURASIP Journal on advances in signal processing,2008, pp.17.

[9] Bordoa, M., & Tornea, O, "DNA secret writing techniques",In 8th International Conference on communications", 2010, pp. 451-456.

[10] Cokal.C & Solak.E,"Cryptanalysis of a chaos based image encryption algorithm",vol.373(15), 2009, pp.1357-1360.