International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 8 (2017), pp. 2113-2123
© Research India Publications
http://www.ripublication.com

Implementation of Arduino based Enhanced Fingerprint Biometric System for Secured Data Exchange

R.Gayathri[1], E.Roshith[2], B.S. Roshini[2], Snehaa Murugan[2], Sakthi Priya[2]

[1,2]Department of Electronics and Communication Engineering,

Sri Venkateswara College of Engineering,
Sriperumbudur, Tamil Nadu, 602117, India,

Abstract

As an emerging biometric for secured data exchange the fingerprint biometric would be a good choice for biometric application because they are unique for a person. Fingerprint is a prominent technology for use in various applications such as forensic, access control, military applications. The proposed arduino based biometric system is to develop a product that it is aimed at providing robust confidentiality and authentication to data used within a closed group of team of members. The product would enable secure data exchange without the need for any conventional methods like keys/passwords. Fingerprint biometric would be the sole security scheme in this device. The product would be independent of software and network.

Keywords - robust, confidentiality, secure data exchange, fingerprint, biometric.

I. INTRODUCTION

Biometrics is the ID of people by their attributes or characteristics. Biometrics is utilized as a part of software engineering as a type of recognizable proof and get to control. Biometric can recognize the novel; quantifiable qualities used to name and portray people. Since biometric identifiers are exceptional to people, they are more dependable in checking character than token and learning based techniques, the accumulation of biometric identifiers raises protection worries about a definitive utilization of this data.

A wide range of parts of human physiology, science or conduct can be utilized for biometric validation. Jain et al. (1999)[1] recognized seven such variables to be utilized while surveying the reasonableness of any quality for use in biometric verification. Comprehensiveness implies that each individual utilizing a framework ought to have the characteristic. Uniqueness implies the characteristic ought to be adequately extraordinary for people in the applicable populace with the end goal that they can be recognized from each other. Furthermore, obtained information ought to be in a frame that grants consequent handling and extraction of the significant capabilities. Execution identifies with the precision, speed, and strength of innovation utilized. Circumvention identifies with the simplicity with which an attribute may be imitated utilizing an antiquity or substitute. No single biometric will meet every one of the necessities of each conceivable application. The principle innovations used to catch the unique mark picture with adequate detail are optical, silicon, and ultrasound. There are two primary calculation families to perceive fingerprints: Minutia coordinating looks at particular subtle elements inside the unique finger impression edges. The first run through an individual uses a biometric framework is called enlistment. At enlistment, the minutia focuses are found, together with their relative positions to each other and their headings. At the coordinating stage, the unique mark picture is handled to concentrate its minutia focuses, which are then contrasted and the enrolled format ‘Positive recognition’ is a common use of the verification mode, “where the aim is to prevent multiple people from using same identity” Jain et al. (1999)[1].

Design coordinating looks at the general attributes of the fingerprints, not just individual focuses. Unique finger impression attributes can incorporate sub-regions of certain enthusiasm including edge thickness, ebb and flow, or thickness. Amid the enlistment stage, the format is just put away some place (on a card or inside a database or both). Amid the coordinating stage, the got format is passed to a matcher that contrasts it and other existing layouts, assessing the separation between them utilizing any calculation. The coordinating project will dissect the format with the info. This will then be yield for any predetermined utilize or reason. Ranges of intrigue are the region around a minutia point, territories with low arch span, and zones with abnormal mixes of edges. The two primary elements of a biometrics framework are putting away and contrasting. The putting away process varies between various frameworks, as a few frameworks store significantly more data and will digitize and pack the data. Once the print data is put away in an open database, a client's prints can be analyzed at whatever point the framework is gotten to. You are confirmed when both the put away and client's print coordinate. Unique mark per users utilize this uniqueness to create a code - once in a while do they really utilize the full print for distinguishing proof - in view of ranges where print lines consolidation, frame, or circle like the round "spin" that you can discover amidst all fingerprints.

The different applications ought to consider Execution, Worthiness, Circumvention, Strength, Populace scope, Measure, Data fraud prevention in selecting a specific biometric. Determination of biometric in view of client prerequisite considers Sensor accessibility, Gadget accessibility, Computational time and unwavering quality, Cost, Sensor region and power utilization.

II. **RELATED WORK**

Qijun Zhao et al. [2] proposed a versatile pore demonstrate for unique mark pore extraction. Sweat pores have been as of late utilised for computerised unique finger impression acknowledgement, in which the pores are typically removed by utilizing a computationally complex, costly skeletonization strategy. A unique finger impression picture is parceled into squares and a neighbourhood pore model is resolved for every piece. With the nearby pore show, a coordinated channel is utilised to remove the pores inside every square. Probes a high determination (1200dpi) unique mark data set are performed and the outcomes show that the proposed pore model and pore extraction technique can find pores all the more precisely and heartily in correlation with other pore extractors.

Moheb R. et al. (2014) [3] proposed an approach to manage picture extraction and exact skin distinguishing proof from pages. This paper proposes a structure to think pictures from site pages and after that recognize the skin shading regions of these photos. As a feature of the proposed framework, utilizing Band question control, they assemble a device bar named "Channel Instrument Bar" by adjusting the Pavel Zolnikov execution.

Manvjeet Kaur et al. (2008) [4], Gayathri and Ramamoorthy (2015) [5] proposed a unique mark check framework utilizing details extraction procedure. Most unique finger impression affirmation frameworks rely on upon particulars planning and have been all around analyzed. Be that as it may, this innovation still experiences issues related with the treatment of low quality impressions. One issue plaguing unique mark coordinating is bending. Twisting changes both geometric position and introduction, and prompts to troubles in setting up a match among numerous impressions gained from a similar fingertip. Meaning every one of the points of interest exactly and also expelling false particulars is another issue still under research. Our work has combined various procedures to produce a minutia extractor and a minutia matcher.

Hoi Le et al. (2009) [6] proposed online interesting imprint ID with a brisk and reshaping tolerant hashing methodology. National ID card, electronic business, and access to PC frameworks are a couple of circumstances where tried and true conspicuous confirmation is an outright need. Existing confirmation frameworks depending on learning based methodologies like passwords or token-based, for example, attractive cards and international IDs contain genuine security chances

because of the powerlessness to designing social assaults and the effortlessness of sharing or trading off passwords and PINs. Whereas Biometrics, unique mark, eye retina, and voice offer a more dependable means for confirmation and increased security. In any case, because of huge biometric database and muddled biometric measures, it is hard to plan both an exact and quick biometric acknowledgment. In this paper, they display a particular commitment by presenting another powerful ordering plan that is capable to secure the unique mark acknowledgement handle as well as enhance the exactness of the framework.

III. METHODOLOGY

The cryptographic procedure utilized inside our framework configuration is to play out the accompanying. The plain content is encoded as a matter of course utilizing an encryption standard E1. After the default encryption of information, the message is encoded and the unique finger impression of the proposed collector is affixed to the scrambled message. To secure the unique finger impression added, a last layer of encryption is forced over the past substance.

Because of the utilization of exclusive encryption standard, the gadgets planned by the maker are just fit for decoding the documents with the nearness of the proposed collector. The unscrambling procedure is the turned around procedure of the encryption, wherein the gave scrambled message is initially decoded to reveal the unique finger impression reference. The unique mark reference is then used to confirm the expected recipient which if legitimate, triggers the last unscrambling to uncover the plaintext. Figure 1.1 (i) shows the flow of how the encryption takes place and (ii) shows how decryption takes place.

(i)

(ii)

Fig 1.1 Block Diagram of the proposed system (i) Encryption (ii) Decryption

The Arduino 2.8 TFT Touch Shield is designed for all the Arduino compatible boards. It works in 3.3V voltage level. It can be directly plugged on the Arduino and other

compatible boards. It will offer display, touch and storage functions for the Arduino board. [7]

The AES algorithm was implemented using matlab software. The simulation results are as follows

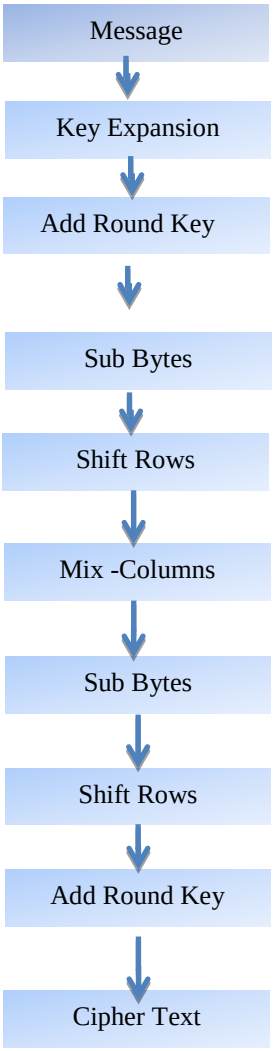

Figure 1.2 Flow of AES algorithm

Step 1: Message

A 4*4 matrix is considered as the Plain text [A] for transmission

Step 2 - Key Expansion

Actual Key Size used in this algorithm for encryption is 8 bytes. As plain text is a 4*4 matrix, key is expanded to – 44*4 matrix using reshape Transformation.

Step 3 – Add Round Key

In this step 16 bytes of this expanded key called as round key is added(Bitwise XOR ed) to the plain text to get a new text A'.

Step 4 – Sub Bytes ( )

Substitute bytes — Uses an S-BOX to perform a byte-by-byte substitution of the block. If first element in plain text is 05 it is replaced a by 0th row 5th column s-box element.

Step 5 - Shift Rows ( )

This step is a simple permutation where each byte in row is shifted left. Elements in 1st row are shifted 1 position left, in 2nd row are shifted 2 positions left and at the end again we got a new text A.

Step 6- Mix Columns( )

Transformation on the Stae column by column , treating each column as a four-term polynomial , the columns are considered as polynomials over GF(28)

After encryption plain text is converted in completely new cipher text

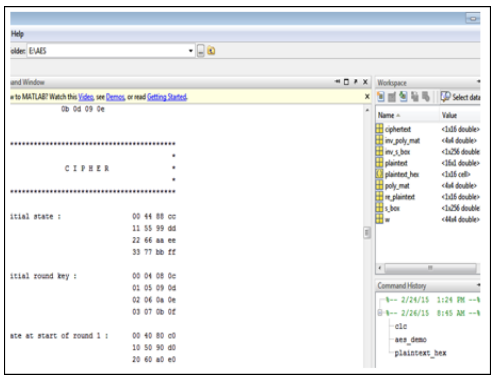

Figure 1.3 AES Algorithm

A. Fingerprint matching

The fingerprints were gotten from every individual utilizing a unique finger impression sensor. Therefore procured fingerprints are put away on-board the unique mark detecting module. The FPS module is fit for accumulating to 200 IDs. However

for our application, we have restricted the client base to 8 IDs. The accompanying were contemplated from papers and MATLAB recreations.

Techniques for Fingerprint Recognition

Following are Fingerprint Recognition Techniques:

- Minutiae Extraction Technique.
- Pattern Matching or Ridge Feature Based Techniques.
- Correlation Based Technique.
- Image-based Techniques.

Most of the finger-scan technologies are based on Minutiae. Figure 1.5 shows the Minutiae extraction. Minutia-based strategies speak to the unique mark by its nearby elements, similar to terminations and bifurcations. This approach has been seriously considered, likewise is the foundation of the current accessible unique mark acknowledgment items. This work also concentrates on same approach.

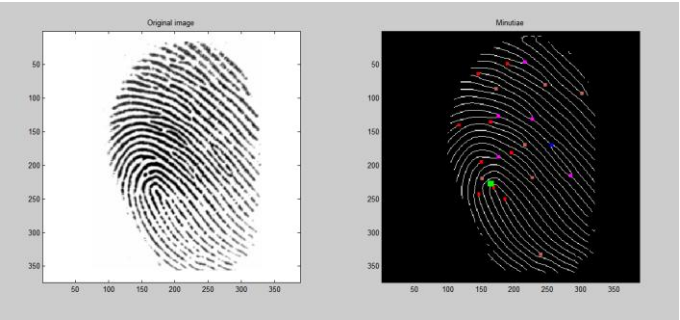

Figure 1.4 Minutiae extraction

B. Encryption and Decryption algorithms

The cryptography algorithm used within the hardware is AES algorithm. The algorithm is meant to proprietary. However, for the purposes of proof of concept, the AES algorithm is used. Cryptography is a very basic technique for data security in WSN. Depending on key used this technique is classified in two categories symmetric encryption and asymmetric encryption. Both techniques have some benefits as well as some limitations. Symmetric key cryptography is fast in operation but as same key is need to be shared between sender and receiver security to this key is a challenging task. Whereas asymmetric key cryptography solves problem of secure exchange of key but it is comparatively slow than symmetric key cryptography. To increase competency and to minimize drawbacks we propose a hybrid encryption scheme which combines two algorithms Advance Encryption Standard (AES) and Elliptical Curve Cryptography (ECC). 2. AES Algorithm AES is a symmetrical encryption

algorithm mostly suitable for encrypting bulk of data. It operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field.

There are many basic steps to implement AES algorithm. This basically includes repetitive rounds of some permutations and combinations to change a simple text into complex data. We have performed such 10 rounds to convert plain text into cipher text.

IV HARDWARE IMPLEMENTATION

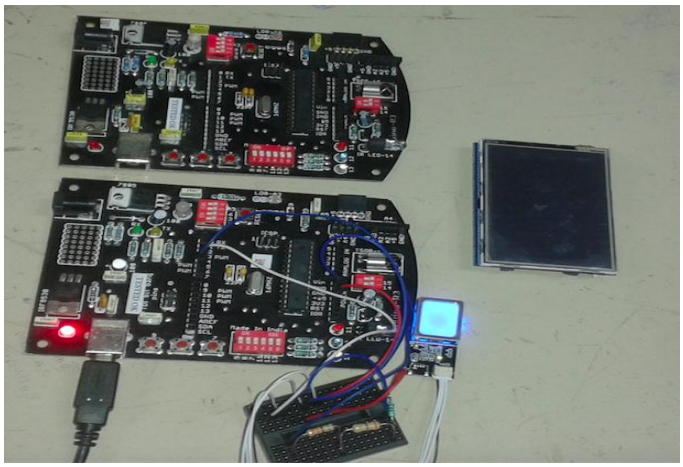

Figure 1.5 Hardware Prototype

Figure 1.5 shows the Hardware prototype of the proposed model

1. Initialization

All members within a team that intend to send and receive data are to meet once and register their fingerprints in each and every member's device.

2. Operation

The following operation takes place at both sender and receiver.

Sender

First sender needs to prepare a SD card with the classified record. And embed the

SD card into the sender's gadget. Then choose the Encryption operation and the receiver .Then send an acknowledgement. Finally encrypted SD Card is prepared.

Receiver

To obtain the encrypted file the receiver has to do the following steps. Firstly insert encrypted SD Card received, into his/her (receiver's) device.
Then Receiver is to choose the decryption operation.
Then Receiver would have to insert his/her fingerprint to a prompt, and the SD card would be stored with the decrypted file if fingerprint is a match, else the files inside will self-destruct.
Finally SD card can be removed for use of the decrypted confidential file.

Results:

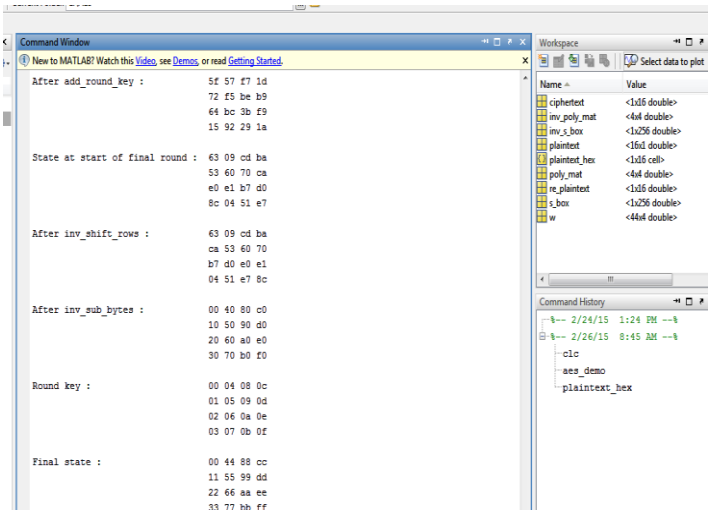

Figure 1.6 AES Results

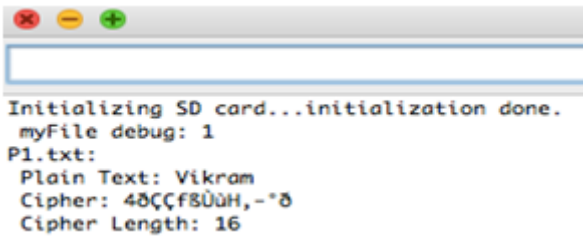

Figure 1.7 Encryption Output

After implementation of the AES algorithm the result is displayed in Figure 1.6 .
The sender has to encrypt the data before sending , the encrypted output obtained in Figure 1.7.

Figure 1.8 is the decrypted output at the receiver's side.

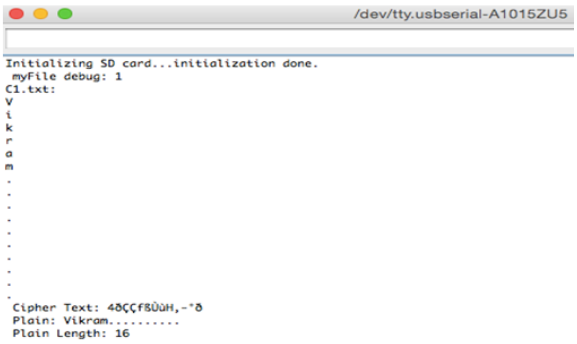

Figure 1.8 Decryption Output

V. CONCLUSION

Biometric technology has mainly been for highly secretive environments with extreme security measures. The objective of the project is to develop a product that it is aimed at providing robust confidentiality and authentication to data used within a closed group of team members. The fingerprint biometric data can be a very promising tool for identification of individuals. The accuracy of the proposed system is further enhanced by fusion technique. However sophisticated public algorithm of encryption, theoretically there can be a computer or a cluster of computers powerful enough to decrypt the cipher text. The most popular algorithms are public. The presented idea chooses to keep it private. Hence, even with very powerful computers, immunity to brute force attack is introduced. Fingerprint authentication, in an embedded and portable context, requires complex signal, network, and security-protocol processing in a resource-constrained implementation. The paper presents a platform- based design approach for this application, based on a hierarchy of virtual machines (VM). We present a platform-based design strategy for such devices, based on our recent design experience with an embedded-fingerprint-authentication device. A hierarchy of virtual machines (VMs) obtains multiple levels of platforms. Platform specialization is expressed as a native interface design on this VMs. Biometrics has been innovatively used in our project to simultaneously provide confidentiality and authentication.

The future work would be to improve the authentication performance using fusion technique or using some other algorithms. Therefore sharing that reliable personal recognition is critical to many business processes. As Biometric Technologies advance, uses and applications become more prevalent and relevant to many different industries.

REFERENCES

[1] D. Maltoni, D. Maio, and A. Jain, S. Prabhakar, "Minutiae-based Methods' (extract) from Handbook of Fingerprint Recognition", *Springer, New York*, pp. 141-144, 2003.

[2] Qijun Zhao, Lei Zhang, David Zhang, Nan Luo,(2008) "Adaptive Pore Model for Fingerprint Pore Extraction." Proc. IEEE. *2008 19th International Conference on Pattern Recognition*, Tampa, FL, 2008, pp. 1-4. doi: 10.1109/ICPR.2008.4761458

[3] Moheb R. Girgis, Tarek M. Mahmoud, and Tarek Abd-El- Hafeez, "An Approach to Image Extraction and Accurate Skin Detection from Web Pages." *World academy of Science, Engineering and Technology*, page no. 27, 2007.

[4] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu.(2008), "Fingerprint Verification System using Minutiae Extraction Technique*", World Academy of Science, Engineering and Technology* Volume 2, 2008, pp. 10-20.

[5] Gayathri R. and Ramamoorthy P., "Performance Evaluation of Multimodal Multifeature Authentication System Using KNN Classification," *The Scientific World Journal*, vol. 2015, Article ID 762341, 9 pages, 2015. doi:10.1155/2015/762341

[6] Hoi Le, The Duy Bui, "Online Fingerprint Identification with a Fast and Distortion Tolerant Hashing." *Journal of Information Assurance and Security*, Vol. 4, pp. 117-123, 2009.

[7] Arduino, 2.8" TFT Shield Datasheet: http: //imall. iteadstudio.com/IM1204 17020_2.8_TFT_LCD_Touch_Shield / DS_IM120417020_2.8_ TFT_LCD_ Touch_Shield. Pdf UTFT Library: http://henningkarlsen.com/ electronics/ library.php?id=52.