Match-on-Card Biometric Framework

Rupali Bhardwaj[1,] Swetleena Panda[2]

[1,2] Department of Computer Science & Engineering

Thapar Institute of Engineering and Technology, Patiala, Punjab,

India

[1]rupali.bhardwaj@thapar.edu

Abstract- *Biometric based access control system acts as a weapon against the challenges for reliable authentication mechanism. Although there are many advantages of biometric system, still it is vulnerable to attacks, which decline its security. This leads to propose a new approach to address these open issues and challenges for biometric data security. Smart card have been already used in past with various degree of success to store biometric credentials. Match-on-card biometric framework locks the biometric data inside the microcontroller of the smart card, which leads to minimal risks if card is lost or stolen. It is fast and accurate, balancing security and convenience by never exchanging user data outside the system of smart card and performs fingerprint enrollment as well as matching within a tamperproof environment of smart card.*

Key words: Java Cards, Security, Fingerprint Match-on-Card

1. Introduction

Verification and identification are basics for compelling security where verification procedure is to design to prove someone’s identity. Now a days, different recognizable identity systems are available such as password, PIN (Personal Identification Number), PAN card, adhaar card, identity cards, security token, biometrics (retinal pattern (iris), fingerprint, signature, voice, body odour) and so on. Now a day, mobile phone's memory/SD card memory, laptop's hard disk or application's database store PIN/password/pattern for identification and verification purpose. At the point when the client enters the secret key/PIN/pattern design for identification purpose, system will compare it with the stored PIN/password/pattern and grants access to the system (or denies access to system). Drawback of this system is that highly vulnerable to attacks through hacking of application's database. One existing alternative that access control system used cards with magnetic stripes but problem is that these cards can cloned effortlessly. Smart card have been already used in past with various degree of success to store biometric credentials. Microcontroller based smart cards are more similar to PCs which can store and process the keys inside the card itself. It is difficult to recover the information from the chip card regardless of whether the attacker has physical access to the card. Smart cards are fit for handling and processing data, and equipped for encryption, decoding marking and so forth, which can be utilize for secure correspondence and safe storing of data. Instead of PIN/password/patterns, biometric traits like unique finger impression, iris etc. give more elevated amount of security. Finally, system or framework utilizes individual's exceptional and lasting physical qualities like fingerprint as verification factor to make the framework more secure.

In this paper, we propose an enhanced biometric framework, which can be utilize to distinguish an individual identity through his/her fingerprint. Effective identification and verification will give access to a specific system or resource.

The rest of the paper is organize as follows. Section 2 presents literature review. Section 3 presents our proposed algorithm. Section 4 presents the experimental study. Finally, the paper is conclude in Section 5.

2. Literature Review

Smart card structure has ended up being more reliable than other machine-readable cards [1]. They guarantee against a full extent of security threats, from careless storage of user's passwords to advanced system hacks. Around the globe, people are now a day using smart cards for a wide arrangement of daily undertakings, which include payments, health care, transportation, access control systems etc. There are many biometric access control system exists, some are listed below-

2.1 Match-on-Server

In traditional biometric based match-on-server access control system, a user first have to provide an identity proof at the time of enrollment. Then fingerprint is scan, which further extracts fingerprint features and convert it to fingerprint template. This generated template representation is compact and can be matched quicker. Fingerprint templates are stored in the central server alongside recognizing data. For verification purpose, user's unique finger template is generate and match with already saved fingerprint template in the central server (fig.1).

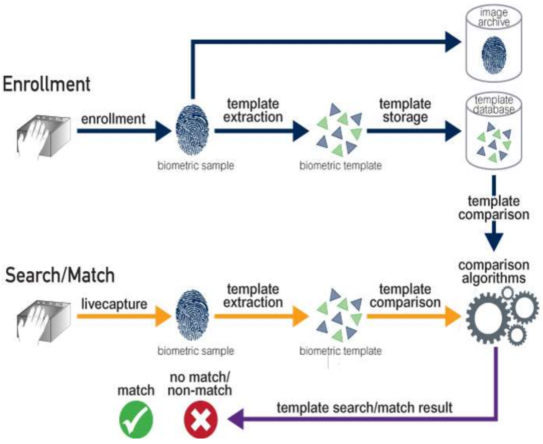

Fig. 1: Match on Server

2.2 Template-on-card

At the time of enrolment, user' fingerprint is scan, which further extracts fingerprint features and convert it to fingerprint template. This fingerprint template is then stored in the smart card. For verification purpose, core system takes out the reference template from the smart card and performs matching of it with newly generated candidate template (fig.2).

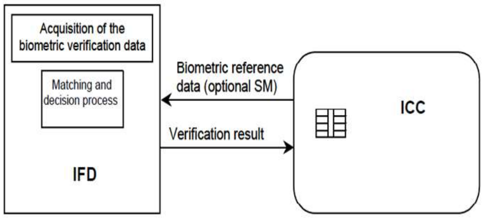
Acquisition of the biometric verification data
Matching and decision process
IFD
Biometric reference data (optional SM)
Verification result
ICC

Fig. 2: Template-on-card

3. Proposed Algorithm

Traditional biometric based access control systems are highly subjected to man in the middle attack because during both enrolment and verification process there is a transmission of secret and sensitive data over a non- secure communication channel. These limitations and drawbacks of existing systems (Match-on-server and Template-on-card) are eliminate by proposed algorithm, based on Match-on-card process. Below figures (Fig.3 &.4) gives a good idea to differentiate the security limitations between the existing systems and the proposed framework (Fig. 8).

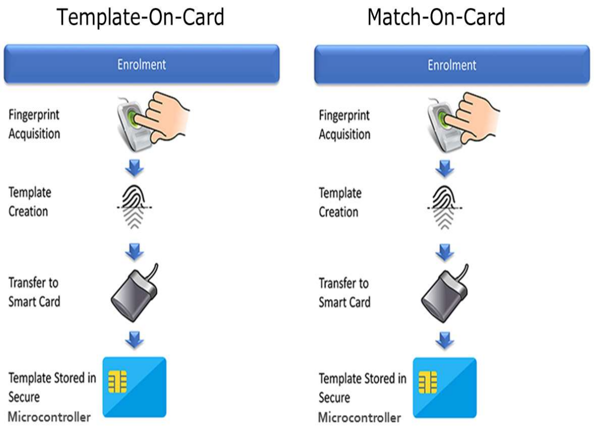

Fig. 3: Enrollment Process

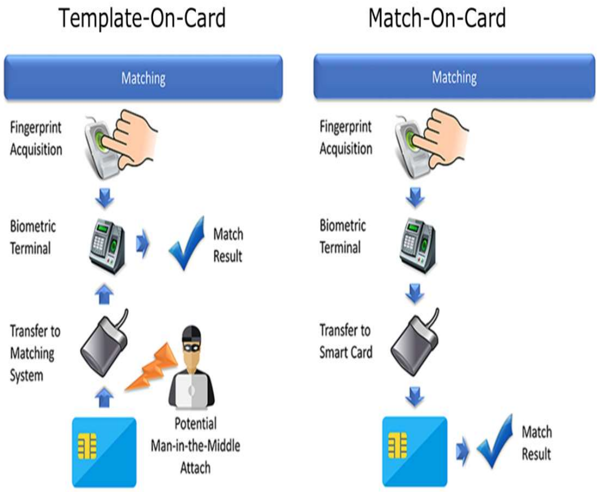

Fig. 4: Verification Process

From the above Fig. 4, it can be observe that the Match-on-card process works as a shield to potential man in the middle attack. Instead of fingerprint image, compact fingerprint minutiae template is stored inside the card. While extracting the minutiae points it should be taken care that no minutiae points to be place on crease, outside of fingerprint image boundary, sweat pores etc. Minutiae points are place at ridge ending or bifurcation. Then to store or match the extracted fingerprint data which is into a standard TVL (Tag-length-value) minutiae template (Fig. 5).

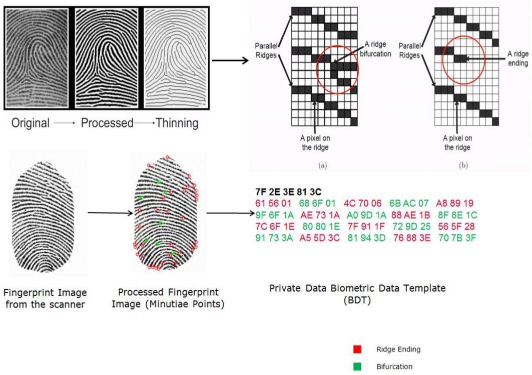
Original
Processed
Thinning
Parallel Ridges
A ridge bifurcation
A pixel on the ridge
(a)
Parallel Ridges
A ridge ending
A pixel on the ridge
(b)
7F 2E 3E 81 3C
61 56 01 68 6F 01 4C 70 06 6B AC 07 A8 89 19
9F 6F 1A AE 73 1A A0 9D 1A 88 AE 1B 8F 8E 1C
7C 6F 1E 80 80 1E 7F 91 1F 72 9D 25 56 5F 28
91 73 3A A5 5D 3C 81 94 3D 76 88 3E 70 7B 3F
Fingerprint Image from the scanner
Processed Fingerprint Image (Minutiae Points)
Private Data Biometric Data Template (BDT)
Ridge Ending
Bifurcation

Fig. 5: Fingerprint minutiae extraction and BDT formation

The tag 7F2E denotes that it is biometric data template (BDT) i.e. the actual fingerprint data. This BDT template is concatenate with the biometric information template (BIT). The tag 7F60 denotes that it is biometric information template (BIT) .The BIT contains further nested TLV representing specific meaning (refer ISO 7816-11) [2]. First BIT is send to card and then BDT at the time of enrollment (Fig. 6). This way the fingerprint data is stored into the card as hexadecimal data. During verification, only BDT data is send to the card that match with the previously enrolled data and sends only the verification result outside the card (Fig. 7).

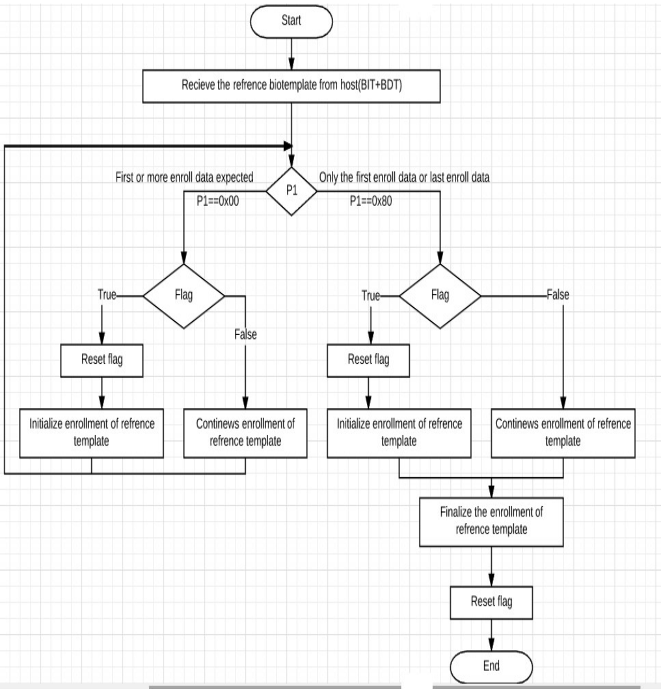
Start
Recieve the refrence biotemplate from host(BIT+BDT)
First or more enroll data expected
P1==0x00
P1
Only the first enroll data or last enroll data
P1==0x80
True
Flag
False
True
Flag
False
Reset flag
Reset flag
Initialize enrollment of refrence template
Continews enrollment of refrence template
Initialize enrollment of refrence template
Continews enrollment of refrence template
Finalize the enrollment of refrence template
Reset flag
End

Fig. 6: Fingerprint Enrolment Framework

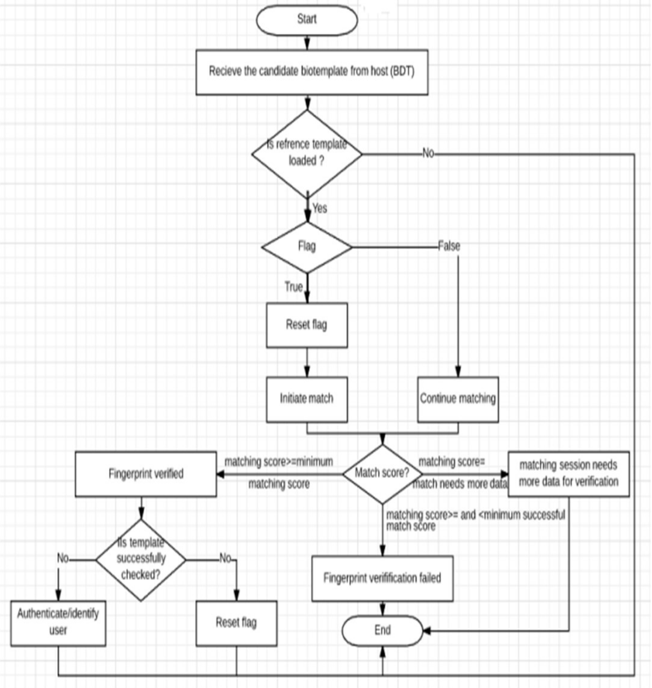
Start
Recieve the candidate biotemplate from host (BDT)
Is refrence template loaded ?
No
Yes
Flag
False
True
Reset flag
Initiate match
Continue matching
Fingerprint verified
matching score>=minimum matching score
Match score?
matching score= match needs more data
matching session needs more data for verification
matching score>= and <minimum successful match score
Is template successfully checked?
No
No
Fingerprint verification failed
Authenticate/identify user
Reset flag
End

Fig. 7: Fingerprint Verification Framework

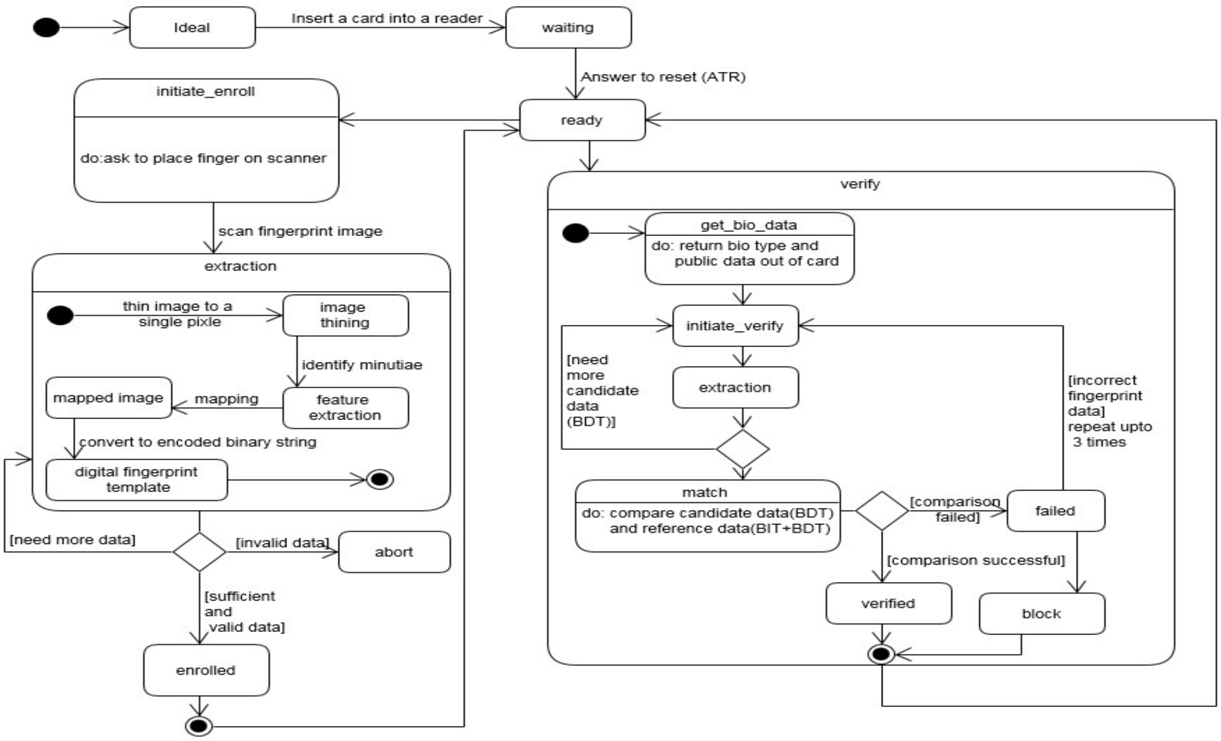
Ideal
Insert a card into a reader
waiting
Answer to reset (ATR)
ready
initiate_enroll
do:ask to place finger on scanner
scan fingerprint image
extraction
thin image to a single pixle
image thining
identify minutiae
feature extraction
mapping
mapped image
convert to encoded binary string
digital fingerprint template
[need more data]
[invalid data]
abort
[sufficient and valid data]
enrolled
verify
get_bio_data
do: return bio type and public data out of card
initiate_verify
[need more candidate data (BDT)]
extraction
[incorrect fingerprint data] repeat upto 3 times
match
do: compare candidate data(BDT) and reference data(BIT+BDT)
[comparison failed]
failed
[comparison successful]
verified
block

Fig. 8: Fingerprint Match on Card Framework State chart

4. Experimental Study

The main evaluation metrics of biometric based access control systems are performance and accuracy. The performance is measure in terms of matching time. In software system, performance testing is the way toward deciding how a framework or system reacts under a specific workload or task. Generally, performance testing tests the speed and stability of a system. Accuracy is measure in terms of FAR (false acceptance rate) and FRR (false rejection rate).

Accuracy and performance are complement to each other. So that it becomes important to select the parameters, which gives a reasonably high accuracy with sufficiently high performance. The experiments carried out in this paper are aim to give an insight for such a balanced Match-on-card framework. The experiment was carried out by using the following hardware and software -

Card side

Hardware	
Card type	*Duel interface card*
Microcontroller	*16 bit*
Memory	*128 Kb*
Software	
Platform	*Java card for government ID*
S/W type	*Java card*
Security and architecture	*Integrity guard*
Cryptography implementation	*Symmetric and asymmetric*

Host side

Hardware	
Card reader	*Duel interface readers (uTrust 4701F , Identive cloud)*
Finger print scanner	*EikonTouch 700 (Sensor type: Capacitive, fingerprint image size: 256 x 360 pixels, resolution: 508 ppi)*
Software	
Operating system	*Microsoft Windows (32-bit and 64-bit)*
IDE	*Java card IDE(version 3.2)*
Widget toolkit	*SWT*

4.1 Accuracy

Improving the accuracy and security of a biometric based access control system is the challenge. The best and most common way of plotting of accuracy and security level evaluation of biometric based access control system is FAR and FRR. Through variation of minutia points counts at the time of enrollment and verification, accuracy is shown in Fig. 8 in term of FAR and FRR.

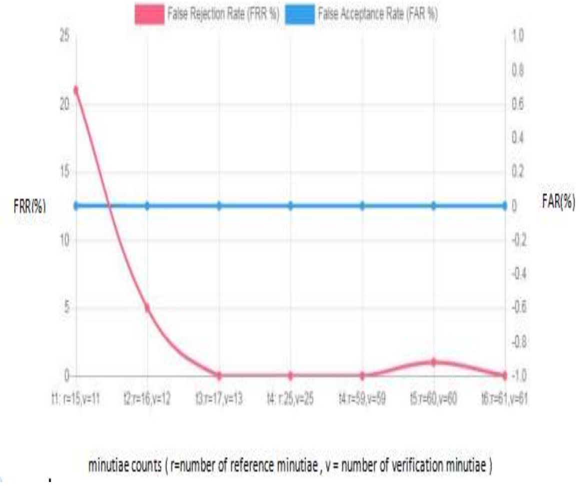

Fig. 8: Minutiae counts vs FRR(%) and FAR(%)

From Fig. 8 it can be show clearly that FAR is zero, regardless of minutiae count and FRR decreases with the increase in minutiae count. We can also observe from the graph that the FRR is high when we consider the system to work with minutiae points less than the recommended range in ISO 19794-2 whereas at boundary values the system is bit deviating. Finally, it is conclude that Match-on-card tool never let the unauthorized user to get access to the system.

4.2 Performance Time

Average time taken for enrolment and verification with variation in the minutia count. From Fig. 9 it is to be conclude that with increment in minutia counts average time for fingerprint verification is also increased.

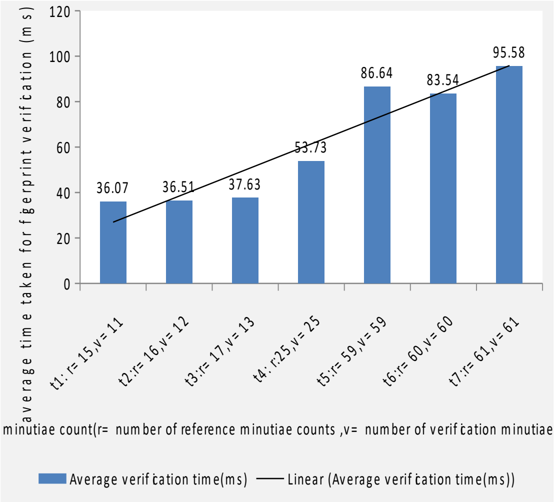

Fig. 9: Minutiae count vs average time taken for fingerprint verification

5. Conclusion

Location of matching is major difference between traditional biometric framework and proposed match-on-card framework. Match-on-card framework never exchanging user data outside the system of smart card and performs fingerprint enrollment as well as verification within a tamperproof environment of smart card. As a result, Match-on-card framework is more secure than traditional biometric framework. Limitation of proposed framework is that process all things inside the card, which decrease the performance in terms of efficiency.

Future scope of proposed framework is to store multiple fingers template at a time during enrollment process so that at time of verification $\mathbf{1}:\boldsymbol{n}$ matching can be execute.

References

[1] Chen, Zhiqun. "*Java card technology for smart cards: architecture and programmer's guide", Addison-Wesley Professional, 2000.

[2] "*ISO/IEC 7816-11:2004 Identification Cards-Integrated Circuit Cards—Personal verification through biometric methods*", https://www.iso.org/standard/31419.html