MasterPrint: Enhanced User Authentication Using Partial FingerPrints

K.L.Neela [1], T.G Rathika [2], B.Nagakarthika [3], Ram K Shivany [4]
Department of Computer Science and Engineeering,University College of Engineering Nagercoil, Tamil Nadu, India.

Abstract – User authentication is considered a key factor in almost any software system and is often the first layer of security in the digital world. The method investigates the possibility of generating a "Masterprint", a synthetic or real partial fingerprint that serendipitously matches one or more of the stored templates for a significant number of users. Sensor output is filtered using Gaussian filter and then with median filter. The Fast Fourier Transform(FFT) algorithm is used to enhance the clarity of images. The Support Vector Machine(SVM) based fuzzy cluster compares the trained and test data. The work expose a potential vulnerability of partial fingerprint based authentication systems, especially when multiple impressions are enrolled per finger.

Index Terms – Gaussian filter, median filter, Fast Fourier Transform, Support Vector Machine, fuzzy cluster.

1. INTRODUCTION

Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control.It is also used to identify individuals in groups that are under surveillance.Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics.Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent.

Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.Some researchers have coined the term behaviometrics to describe the latter class of biometrics.More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number.Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.Fingerprint recognition is nowadays one of the most widely diffused biometric authentication techniques.Biometric based solutions are able to provide confidential outcomes for financial sectors and for authentication.The fingerprint is unique for each and every individual person.By using this technique only authenticated users get enrolled. Fingerprint scanners are security systems of biometrics..Everyone has marks on their fingers. They can not be removed or changed. These marks have pattern and this pattern is called the fingerprint.

Every fingerprint is special, and different from any other in the world. Because there are countless combinations, fingerprints have become an ideal means of identification. Fingerprint scanners are security systems of biometrics. They are now used in police stations, security industries and most recently, on computers.Everyone has marks on their fingers. They can not be removed or changed. These marks have a pattern and this pattern is called the fingerprint. Every fingerprint is special, and different from any other in the world.

2. RELATED WORK

Kai et al.[1] Minutiae based matching may cause various problems due to cluster formation and low clarity.The paper explains how to overcome this bugs.Since minutiae is a unique feature for each person it is used for individual biometric identity.This method fails when the finger is physically damaged, dry, wet, etc,.

Sonia et al.[2] Text based passwords becomes easily exposed to the attackers. So graphical password method clued comes into existence. The user will set the password based on the clicks made on the images which is displayed for the users.The advantage is highly secured when compared to text based password.It is difficult to setup the password and also time will be allocated for password entry.

Wei et al.[3] 3D concept investigates about touchless fingerprint sensor. The sensor will scan the fingerprint without having any physical contact with the device.Physical damage in the fingers cannot be an issue,since scanning is done.The problem here is that the obtained 3D image should be converted in to 2D image which is time consuming.

Zubayr et al.[4] Static password will be exposed to the attackers.so a new concept of dynamic or changeable passwords is used.Here the passwords are generated based on the position shifted of the primary password.Changing password becomes a great challenge to the hackers (Brute force attack).Less difficulty when compared to 3D password.Password size is difficult.Loss of the initial password will make it to difficult to access.

S.Vaithyasubramanian, et al.[5] Singlefactor authentication, either text password or graphics password can be easily broken.So two factor authentication both text and graphical password can be used.Two step authentication will take more time for the intruder to get into the core.Space and time complexity.Difficult for remembering both the password.

Wazir Zada Khan et al.[6] Human brain has more power to remember images rather than text so this paper provides the idea of using images password grid for setting password.Password will be resistant against brute force,shoulder attack, dictionary attack and so on…Disadvantage is server need to store large amount of images and transmission of images over network is tedious.

Yimin et al.[7] RhyAuth a novel two factor rhythm-based authentication scheme for multitouch mobile devices.RhyAuth requires user to perform a sequence of rhythmic taps/slider on advice screen to unlock the device.The user is authenticated only when the rhythm matches with the stored rhythm.Both user chosen rhythm and users metric is used which is better than alphanumerical and graphical password.The problem here is that the password size cannot be determined.

Vijayshri et al.[8] Two authentication schemes which provide a secret username as well as graphical password.The secret username is valid only for particular session.The graphical password used here is grid.Protects against shoulder surfing graphical password are easy to remember.Problem is that Different user may select same grid format so there may be a chance for collision

AryaKumar et al.[9] Brute force and dictionary attacks are increasing day to day. Password guessing resistant protocol is used to reduce the login attempts from unknown source IP address. This would make password guessing more difficult for the attackers. Significantly improves the security, usability, trade off and can be more efficient beyond browser based authentication. The drawback is that while listed IP address expires after a certain time span.

Eko et al.[10] The combination of one time password,SMS gateway and MD5 hash encryption algorithm are used to develop a more secured login procedure to access the web-based.Acadamic information system.One time password is generated only once and it is not repeated.Drawback is generation of one time password take more time.OTP is valid only for short times.

3. PROPOSED SYSTEM

The proposed system investigates the possibility of generating the masterprint the combination of one or more users.The fingerprint which matches with the Masterprint will be authenticated.

3.1 OVERALL ARCHITECTURE

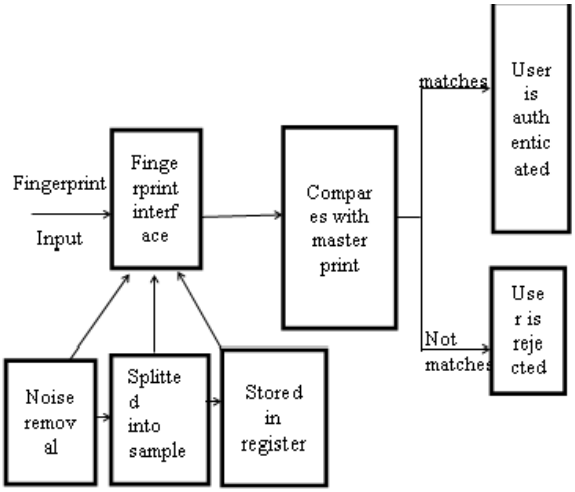

Fig 3.1 Overall Architecture

The fig3.1 explains the overall architecture of the project .The overall architecture contains three stages preprocessing,comparison and authentication.The preprocessing and comparison is done in the digital persona device and comparison is done in the demo server.The input is given through the finger print interface and it is preprocessed using gaussian and median filters .the processed input is splitted into 256 samples using FFT algorithm and stored in the register.The stored samples is compared and if it matches the user is authenticated.

3.1.1 FILTER:

The filter that can be used in the preprocessing stages are low pass,high pass and band pass filter.The output coming from the low pass and high pass is in the form of triangular wave. So the fingerprint output will be damaged.The fig 3.1.1 used here is band pass filter since the output produced is rectangular waveform.The band pass filters used here is Gaussian and median filters.By using the Gaussian and median filters the noise in the image is removed .The preprocessing stage is completed after the noise is removed.

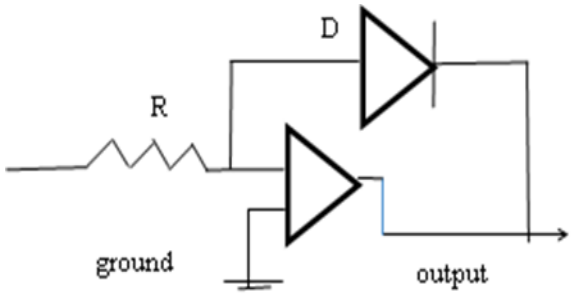

Fig 3.1.1 Band Pass Filter

3.1.2 SAMPLE SPLITTING

The processed data coming from the Gaussian and median filters is splitted into 256 samples using FFT algorithm (Fast Fourier Transform). Here MC,DSP and VLSI chips can be used.MC is 4 bit ADC,2^4=16 so resolution of image which is produced is low and VLSI is of 10 bit ADC,2^10=1024 and produces a good resolution of image but is of high cost so DSP is used.It is of 8 bit ADC so 2^8=256.The fingerprint image is converted into 256 samples to increase the clarity of the image.

$f(s)=f0+\sum f(x)\ cosnxdx+\sum f(x)\ sinnxdx$

where ,

f0 →Starting point.

cosnxdx→Decreasing samples.

sinnxdx→Increasing samples.

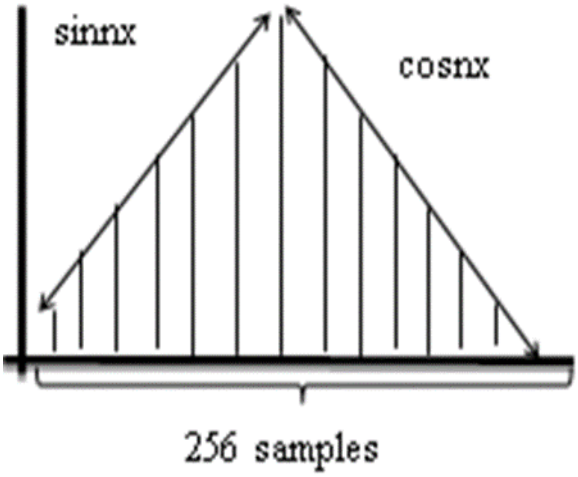

Fig:3.1.2 Sample splitting

The fig3.1.2 explains the preprocessed image splitting into 256 samples by using the Fast Fourier Transform algorithm.

3.1.3 DIGITAL PERSONA ARCHITECTURE

The fig 3.1.3 represents the components of digital persona

FINGERPRINT MODULE:

Fingerprint module is the place where fingerprints of the users get enrolled.

POWER SUPPLY:

The overall power supply is given.

RELAY:

The relay is used for controlling the fluctuation that occurs.Any fluctions or voltage problems which may causes damage to the systems will be controlled by the relay which is used.

MICROCONTROLLER:

Microcontroller is used for comparison of the fingerprint samples.The Microcontroller used here the Audinouno.

MAX 232:

Max232 is used for translation of RS232 protocol to TTL protocol.RS232 protocol is the serial communication protocol in which 256 samples are sent one after one in a bit by bit manner.So this cannot be given directly to microcontroller which work in a TTL protocol.Inorder to convert 256 samples in a single image by TTL protocol Max232 is used.

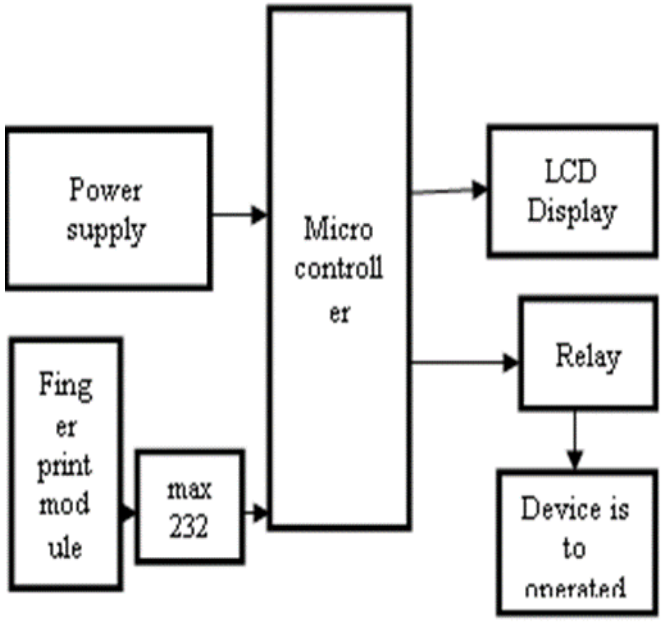

Fig 3.1.3 Digital Persona Architecture

3.2SERVERAUTHENTICATION

A website is designed and an user interface page is created and whenever the user wants to use the particular website the user needs to get authenticated by using the finger print the website which is created is executed in the local server.

4. PERFOMANCE ANALYSIS

The metrics compared here are accuracy, sample splitting and time. Digital Persona has a good performance in all the metrics. All participants suggested that the login process is more user friendly.The participants are chosen by the mixing category of computer familiar and computer non-familiar. Both categories of people can operate the system in easy manner.In the fig 4.1 and table 4.1,the n value represents the the number of samples splitted(2^n)

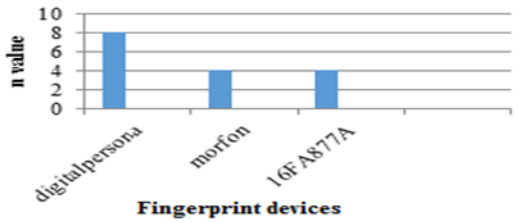

Fig 4.1 Sample splitting

FINGERPRINT DEVICE	SAMPLE SPLITTING(N VALUES)
Digital persona	8
Morfon	4
16FA887A	4

Table 4.1 Sample splitting.

The performance metrics of the proposed work includes matching speed. Matching speed is the time taken for matching the already stored samples with the input of the candidate's fingerprint samples. The fig 4.2 and table 4.2 represents the matching speed of digital persona, morfon and 16FA887A devices. It is clearly shows that the time taken for digital persona is lesser than the other devices.

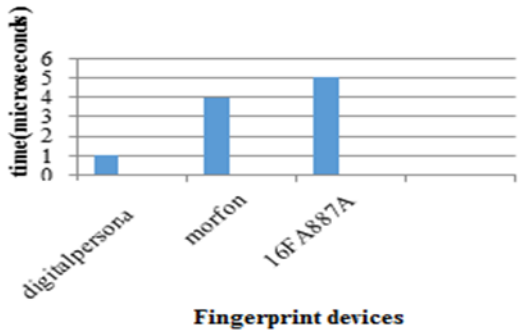

Fig 4.2 Matching speed

FINGERPRINT DEVICE	TIME(MICROSECONDS)
Digital persona	1
Morfon	4
16FA887A	5

Table 4.2 Matching speed

The performance metrics of the proposed work also includes accuracy. The accuracy represents the minimal false rate of the devices. Here digital persona has minimal false rate that is it produces high accuracy when compared to morfon and16Fa887A

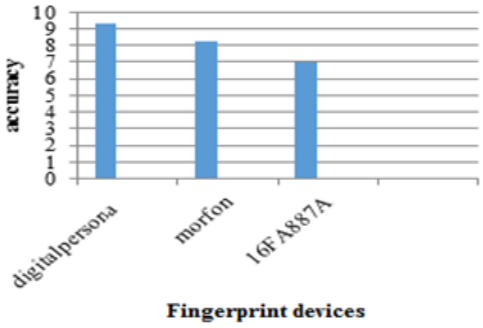

Fig 4.3 Accuracy

FINGERPRINT DEVICE	ACCURACY LEVEL
Digital persona	9.3
Morfon	8.2
16FA887A	7

Table 4.3 Accuracy

5. CONCLUSION

All existing applications are having different types of security. Login security and data robbery are most important areas in internet security. Nowadays we are using security system in interdisciplinary areas example, ecommerce, internet banking, cyber security, cloud computing network etc. But these all are met dissimilar difficult in login security. Because all existing login security systems are login to the particular site with username and password. Some network hackers are burglary the login and password and they are misuse the another person account. The propose system supports higher security to the login system because of username and fingerprint utilization. So this type of security is shunning the unauthorized login.The future work can be extended towards authentication of face mechanism.

REFERENCES

[1] Kai Cao, Eryun Liu, Liaojun Pang, Jimin Liang, Jie Tian, **"**Fingerprint matching by incorporating minutiae discriminability**",**IEEE transaction on information forensics and security,978-1-4577-1359-0,2011.

[2] Sonia Chiasson, Elizabeth Stobert, Alain Forget,Robert Biddle, and Paul C. van Oorschot," Persuasive clued click points"IEEE

[3] Zubayr Khalid, Pritam Paul, Soummyo Priyo Chattopadhyay, Anik Naha Biswas," Secure authentication with dynamic password" Information Forensics and security,978-1-5090-0996-1,2016.

[4] S. Vaithyasubramanian, A. Christy and D. Saravanan," Two factor authentication for secured login"Information Forensics and Security**,**VOL. 10,1819-6608,2015.

[5] Wazir Zada Khan**,** Mohammed Y Aalsalem and Yang Xiang**,"** A graphical password based system for small mobile devices**"**International Journal of Computer Science Issues, Vol. 8,1694-0814 ,2011.

[6] Yimin Chen, Jingchao Sun, Rui Zhang, and Yanchao Zhang," Rhythm based two factor authentication"computer communications,978-1-4799-8381-0,2015.

[7] Vijayshri D. Vaidya ,Imaran R. Shaikh ," Grid based authentication scheme and graphical password"Science, Engineering and Technology Research, Volume 4,2278 – 7798 ,2015.

[8] Arya Kumar, A. K. Gupta," Password guessing resistant protocol" Engineering Research and Applications , Vol. 4,2248-9622,2014.

[9] Eko Sediyono, Kartika Imam Santoso, Suhartono," Secure login by using one time password authentication"Advances in Computing, Communications and Informatics,978-1-4673-6217-7,2013.