Secured M-Commerce Transaction Using Mixed Fingerprint Authentication

[1]Mr.K.Shanmugam, [2]Dr.B.vanathi, [3]Mr.R.Arunprakash,[4]R.Swaminathan,[5]S.Vijayanand
[1,3]Assistant Professor,[2]Professor, [4,5]UG scholar
[1,2,3,4,5]Department Of Computer Science and Engineering
[1,2,4,5]Valliammai Engineering College, Chennai,Tamilnadu
[3]University College of Engineering –Ariyalur

Abstract - Forth coming banking applications won't be on desktop or mainframes but on the small devices we carry every day. Secured commerce on the mobile is the latest issue for all mobile users. The present security issues surround the loss of personal information through the theft of the cell phone. The use of biometrics has been virtually eliminated the possibility of someone gaining access to a third party cell phone directly. Biometrics handles authentication of individuals on the basis of biological and/or behavioral characteristics (measurements of the human body). As a primary advantage, biometric features are typically unique and, therefore, cannot be misplaced and forgotten since these are always inherently associated with human beings. The major biometric features include voice, face, fingerprint, irises, retinas, palm print, signature, and so on. To provide more security in this work we explore the possibility of mixing two different fingerprints at the image level in order to generate a new fingerprint. The mixed fingerprint is dissimilar from the original fingerprints and they provide virtual identity from the fixed fingerprints. To mix two fingerprints, each fingerprint is decomposed into two different components, viz., the continuous and spiral components. After pre-aligning the components of each fingerprint, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint image. Biometrically secured mobile payment system is much safe and secure and very easy to use, also no need to remember passwords and secrete codes. This paper explores the possibility of mixing two different fingerprints at the image level in order to generate a new fingerprint. Bio-metric authentication relieves the users from the pain of remembering numerous secret passwords. People tend to believe that biometrics would provide better security in authentication systems, and such biometric authentication systems are being developed for use in areas like border security, airport security, banking, and so on.

Keywords **- M-Commerce, mobile banking mobile payment, mixed fingerprint, biometric authentication**

I.INTRODUCTION

Today we are living in digital kingdoms having computer slaves, who make our life much easier, but not necessarily more secure. With the advancement of science and technology our daily activities have become faster and easier at the cost of having complex tools and technologies. The online banking transactions are part of daily routine for an individual. The existing online banking system has several drawbacks. Firstly hacking, from the internet any one can hack the username and password and the result is third person gets access to owner account. As anyone is not with twenty four hours on the Internet, i.e. access bank website, it takes some time to know that your account get hacked and third one can get transfer the money to his own account. Secondly, every time one has to carry laptop or PC with you. So for this issue secured payment applications on mobile device i.e. M-commerce is proposed.

Today is the era of mobile, everyone having the mobile in his hands, instead of using the laptop or PC, mobile is the best option to use for the banking purpose. The next generation of banking applications won't be on desktops or mainframes but on the small mobile devices we carry every day. Secured e-banking on the mobile is the latest issue for all mobile users. M-commerce, in the context, provides a lot of services like Mobile ticketing, Mobile banking, Mobile location based services, Mobile auctions, Mobile purchasing and so on.

Mobile devices are rapidly becoming a key computing platform, transforming how people access business and personal information. Access to business data from mobile devices requires secure authentication, Authentication is the act of verifying that an individual is who he claims to be. Today we're using usernames and passwords, but passwords are weak in that many people write them down, or forget them. Passwords may be captured by spyware or Trojan horses on an infected computer and they are 'easy' to guess.

The ease of guessing depends on the password strength, which is up to the user to define. Traditional authentication systems requires the user perform the cumbersome task of memorizing numerous passwords, personal identification numbers (PIN), pass-phrase, and/or answers to secret questions like "what is your nick name?", etc. in order to access various databases and systems. More often, it becomes almost impossible to the different formats due to case sensitivity, requirement of alphanumeric text, and the necessity to change passwords or pass-phrases periodically to prevent from accidental compromise or theft. Many users choose passwords to be part of their names, phone numbers, or something which can be guessed. Moreover, to handle the hard task of remembering so many passwords, people tend to write them in files, and conspicuous places such as desk calendars, which expose chances of security violation.

Another authentication approach is biometrics, which is a way of authentication through something your body is or can do, rather than something you know (a password). Biometric authentication is the process of verifying if a user or identity is who they claim to be using digitized biological pieces of the user [1]. It comes in all sorts of flavors' - fingerprint, iris scan, hand geometry, face recognition, voice recognition, handwriting and typing dynamics -most of these have different variants.

Generally speaking, there are four factors of physical attributes that are used or can be used in user authentication:

- Finger print scans, which have been in use for many years by law enforcement and other government agencies and is regarded as a reliable, unique identifier.
- Retina or iris scans, which have been used to confirm a person's identity by analyzing the arrangement of blood vessels in the retina or patterns of color in the iris.
- Voice recognition, which uses a voice print that analyses how a person says a particular word or sequence of words unique to that individual.
- Facial recognition, which use unique facial features to identify an individual.

The rich set of input sensors on mobile devices, including cameras, microphones, touch screens, and GPS, enable sophisticated multi-media interactions. Biometric authentication methods using these sensors could offer a natural alternative to password schemes, since the sensors are familiar and already used for a variety of mobile tasks.

Biometrics has made it possible to identify individuals rapidly, based on biological traits. Biometric system is essentially a pattern recognition system that operates by acquiring physiological and/or behavioral characteristics from individual (such as fingerprint, iris scan, retina scan, hand geometry, etc.) [2], extracting a set of features from the acquired data, and comparing this feature set against the set of templates pre-stored in the database. In a biometric system, each reference template stored in the database is usually associated with only a single individual[3].

Fingerprint is probably the most used for biometric authentication. It is also likely to be the oldest biometric in use. There is archeological evidence that fingerprints as a form of identification have been used at least since 7000 to 6000 BC by the ancient Assyrians and Chinese. However, biometric authentication is not the silver bullet for secure authentication. We cannot use fingerprint biometrics everywhere instead of passwords or Tokens. Nothing is perfect, and fingerprint biometric authentication methods also have their own shortcomings. Spoofing of biometric systems for misappropriation of biometric data is a realistic security threat. The consequences hereof can be very severe, because biometric characteristics in principle cannot be changed, unless biometric are used in a revocable way. In order to fake a fingerprint, one needs an original first. The hack is to create an artificial finger using a mold that is manufactured using the legitimate user's actual finger. This type of attack is not really usable in real life as people are usually wise enough not to give their fingers as a mold material. However, this hack demonstrates that the scanner can be fooled using a gelatine finger instead of a live finger and can be taken further in technology. Latent fingerprints are nothing but fat and sweat on touched items. Thus to retrieve someone else's fingerprint (in this case the fingerprint you want to forge) one should rely on well tested forensic research methods.

In this paper, unlike previous work, two fingerprint impressions acquired from two different fingers are fused into a new fingerprint image resulting in a new identity1. The mixed image incorporates characteristics from both the original fingerprint images, and can be used directly in the feature extraction and matching stages of an existing biometric system. There are several benefits for mixing fingerprints. For example, the proposed approach could be used to fuse images of the thumb and the index fingers of a single individual, or index fingers of two different individuals. Therefore, the concept of mixing fingerprints could be utilized in a multifinger authentication system. In the case of Joint account banking application we can utilize this method.

Figure1: Mixed Fingerprint

Existing smart phones in market an open, programmable software framework is vulnerable to typical smart phone attacks. Such attack can make the phone partially or fully unusable and cause unwanted SMS/MMS billing. The statistics shows online transactions are hacked. avoid the general device attack, authors have used the Android mobile for the payment application. Android has software stack based on the Linux Kernel and it contain the Android Native libraries. Android is very powerful device. As it having the in build in libraries, and top level security mechanism to secure the rich application. It also includes the Image processing library that can be used for the processing input images.

PDAs and cell phones these days come with finger print scanners for authentication and transactions. There are various methods to take the runtime fingerprint. Android is having the inbuilt fingerprint scanner. It is also possible to install the fingerprint scanner software to the android device, and take the finger print at run time. Even if biometrics mobile is not available, the camera with high mega pixel can take the picture and can be processed further for the secured banking in android based mobile device [4][5].

To better understand security issues concerned with biometric authentication, it should be useful to study individual components of a typical biometric system, communication channel among the components, and their vulnerabilities. So here the payment application is secured on all the ways, i.e. it uses the secure device, biometric security mechanism to open the payment application and wireless channel security.

II. Background

The term biometrics comes from the Greek words bios, meaning life, and metrics, meaning measure. Biometrics can be defined asmeasurable physiological and/or behavioural characteristics that can be utilized to verify the identity of an individual, and includefingerprint verification, hand geometry, retinal scanning, iris scanning, facial recognition and signature verification. Biometricauthentication is considered the automatic identification, or identity verification, of an individual using either a biological featurethey possess physiological characteristic like a fingerprint or something they do behaviour characteristic, like a signature. Inpractice, the process of identification and authentication is the ability to verify and confirm an identity. In this paper, we explore authentication techniques on mobile devices from the users' point of view. To allow for comparison between authentication methods, the voice and gesture conditions use the same 8-digit authentication token. We find that speaking was the fastest biometric authentication method, but taking a photograph supported better performance in the memory recall task. Speaker verification was considered less usable than password, face and gesture (writing an 8-digit PIN). Combination conditions – simultaneously entering two biometric samples – were very unpopular. Failure rates were not significantly different among single conditions, but combining methods led to high error rates. So in this paper we proposes fuzzy logic comparision for mixed fingerprint. That will reduce the error rate as well as provide more security for online mobile transaction. Based on literature review, this paper identifes security issues of biometric authentication systems and possible security attacks on biometric systems.

Face

Face recognition for its easy use and non intrusion has made it one of the popular biometric. Face recognition uses the spatial geometry of distinguishing features of the face. It is a form of computer vision that uses the face to identify or to authenticate a person.

An important difference with other biometric solutions is that faces can be captured from some distance away, with for example surveillance cameras. Therefore **face recognition** can be applied without the subject knowing that he is being observed [2][6]. Further, a survey of existing face recognition technologies and challenges is given [Abate et al. 2007]. A number of algorithms have been proposed for face recognition. Such algorithms can be divided into two categories: geometric feature-based and appearance-based. Appearance-based methods include: Eigenfaces [Turk and Pentland, 1991], Fisherfaces [Belhumeur et al. 1997], Independent Component Analysis (ICA) [Bartlett et al. 2002], Kernel Principal Component Analysis (KPCA) [Scholkopf et al. 1999, Kim et al. 2002], Kernel Fisher Discriminant Analysis (KFDA) [Liu 2004, Yang 2002], General Discriminant Analysis (GDA) [Baudat and Anouar, 2000], Neural Networks [Lawrence et al. 1998], and Support Vector Machine (SVM) [Phillips, 1999; Jonsson et al. 2002].

Recognition of faces from still images or 2D images is a difficult problem, because the illumination, pose and expression changes in the images create great statistical differences and the identity of the face itself becomes shadowed by these factors. To overcome this problem 3D face recognition has been proposed which has the potential to overcome feature localization, pose and illumination problems, and it can be used in conjunction with 2D systems. Research using 3D face data to identify humans was first published by [Cartoux et al. 1989]. The 3D face data encodes the structure of the face and so is inherently robust to pose and illumination variations. Applying HMMs to 3D face verification was first attempted by [Achermann et al. 1997]. A recent advance for 3D face verification has been to show the applicability of the Gaussian Mixture Model (GMM) parts-based approach [Mccool et al. 2008]. The drawbacks of 3D face recognition include high cost and decreased ease-of-use for laser sensors, low accuracy for other acquisiton types, and the lack of sufficiently powerful algorithms. Two of the biggest challenge with face recognition are image capture and pose correction. Clear facial images are extremely hard to capture when subjects are moving fast in a crowd. Despite the fact that surveillance video may be able to capture hundreds of frames of a subject's face, there may only be one or two frames that are actually useable.

Iris

The human iris is so unique that no two irises are alike, even among identical twins, in the entire human population. Recently, human iris biometric based identification has attracted the attention of research and development community. The iris has many features that can be used to distinguish one iris from another. One of the "primary visible characteristic is the trabecular meshwork, a tissue which gives the appearance of dividing the iris in a radial fashion"4 that is permanently formed by the eighth month of gestation. During the development of the iris, there is no genetic influence on it, a process known as "chaotic morphogenesis" that occurs during the seventh month of gestation, which means that even identical twins have differing irises.

A survey on the current iris recognition technologies is available in [Bowyer et al. 2008]. [Flom and Ara, 1987] first proposed the concept of automated iris recognition. It was John Daugman who implemented a working automated iris recognition system [Daugman, 1993; Daugman, 2003]. Though Daugman's system is the most successful and most well known, many other systems have also been developed. An automatic segmentation algorithm based on the circular Hough transform is employed by [Wildes, 1997]. [Boles and Boashash, 1998] extracted iris features using a 1-D wavelet transform. [Sanchez-Avila and Sanchez-Reillo, 2002], further developed the iris representation method proposed by Boles et al. [Lim et al. 2001] extracted the iris feature using 2-D Haar wavelet transform and [Park et al. 2003] utilized directional filter banks to extract the normalized directional energy as a feature. [Kumar et al. 2003] employed correlation filters.

Jiali Cui, Yunhong Wang, JunZhou Huang, Tieniu Tan and Zhenan Sun have proposed the iris recognition algorithm based on PCA (Principal Component Analysis) is first introduced and then, iris image synthesis method is presented. The

synthesis method first constructs coarse iris images with the given coefficients. Then, synthesized iris images are enhanced using super resolution. Through controlling the coefficients, they create many iris images with specified classes.

Extensive experiments show that the synthesized iris images have satisfactory cluster and the synthesized iris databases can be very large. Recently Ma et al. proposed two iris recognition methods, one using multi-channel Gabor filters [Ma et al. 2002] and the other using circular symmetric filters [Ma et al. 2002]. Later, they proposed an improved method based on characterizing key local variations with a particular class of wavelets, recording a position sequence of local sharp variation points in these signals as features [Ma et al. 2004]. Iris and face recognition devices are already being used by the U.S. military to identify and track suspected terrorists and other enemies. Although such devices have proven extremely helpful to the military, the underlying technology is not without its drawbacks. Iris scanners, for example, only work when targets are stationary and within very close range, making it impossible to capture iris images from moving targets at a distance [2][7].

Several other methods have also been developed for iris recognition. [Chen et al. 2006] proposed using Daugman‘s 2-D Gabor filter with quality measure enhancement. [Du et al. 2006] proposed using 1-D local texture patterns and [Sun et al. 2005] proposed using moment- based iris blob matching. The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye. A survey on the current iris recognition technologies is available in [Bowyer et al. 2008]. [Flom and Ara, 1987] first proposed the concept of automated iris recognition. It was John Daugman who implemented a working automated iris recognition system [Daugman, 1993; Daugman, 2003]. Though Daugman‘s system is the most successful and most well known, many other systems have also been developed. An automatic segmentation algorithm based on the circular Hough transform is employed by [Wildes, 1997]. [Boles and Boashash, 1998] extracted iris features using a 1-D wavelet transform. [Sanchez-Avila and Sanchez-Reillo, 2002], further developed the iris representation method proposed by Boles et al. [Lim et al. 2001] extracted the iris feature using 2-D Haar wavelet transform and [Park et al. 2003] utilized directional filter banks to extract the normalized directional energy as a feature. [Kumar et al. 2003] employed correlation filters. Recently Ma et al. proposed two iris recognition methods, one using multi-channel Gabor filters [Ma et al. 2002] and the other using circular symmetric filters [Ma et al. 2002]. Later, they proposed an improved method based on characterizing key local variations with a particular class of wavelets, recording a position sequence of local sharp variation points in these signals as features [Ma et al. 2004]. Several other methods have also been developed for iris recognition. [Chen et al. 2006] proposed using Daugman‘s 2-D Gabor filter with quality measure enhancement. [Du et al. 2006] proposed using 1-D local texture patterns and [Sun et al. 2005] proposed using moment-based iris blob matching.

Fingerprint

Fingerprint is the pattern of ridges and valleys on the tip of a finger and is used for personal verification of people. Fingerprint based recognition method because of its relatively outstanding features of universality, permanence, uniqueness, accuracy and low cost has made it most popular and a reliable technique and is currently the leading biometric technology [Jain et al. 2004]. There is archaeological evidence that Assyrians and Chinese ancient civilizations have used fingerprints as a form of identification since 7000 to 6000 BC [Maltoni et al. 2003]. Henry Fauld in 1880 laid the scientific foundation of the modern fingerprint recognition by introducing minutiae feature for fingerprint matching [Maltoni et al. 2003]. Current fingerprint recognition techniques can be broadly classified as Minutiae-based, Ridge feature-based, Correlation-based [Jain and Prabhkar, 2001] and Gradient based [Aggarwal et al. 2008]. Biometrics can be destroyed, and a biometric characteristic's ability to be read by a system can be reduced. An individual's fingerprints, for example, can be affected by cuts and bruises and can even be destroyed by excessive rubbing on an abrasive surface. Also, Accuracy of Biometrics depends mainly on the software that is dealing with them[4][12].

Most automatic fingerprint identification systems employ techniques based on minutiae points [Jain and Prabhkar, 2001]. Although the minutiae pattern of each finger is quite unique, noise and distortion during the acquisition of the fingerprint and errors in the minutiae extraction process result in a number of missing and spurious minutiae [Chikkerur et al. 2006]. To overcome the difficulty of reliably obtaining minutiae points from a poor quality fingerprint image, ridge feature-based method is used. A ridge is a pattern of lines on a finger tip. This method uses ridge features like the orientation and the frequency of ridges, ridge shape and texture information for fingerprint matching. However, the ridge feature-based methods suffer from their low discrimination capability [Maltoni et al. 2003]. The correlation-based techniques make two fingerprint images superimposed and do correlation (at the intensity level) between the corresponding pixels for different alignments. These techniques are highly sensitive to non-linear distortion, skin condition, different finger pressure and alignment [Yousiff et al. 2007]. Most of these techniques use minutiae for alignment first [8].

The smooth flow pattern of ridges and valleys in a fingerprint can be also viewed as an oriented texture [Jain and Prabhkar, 2001]. [Jain et al. 2000] describe a global texture descriptor called Finger Code‘ that utilizes both global and local ridge descriptions for an oriented texture such as fingerprints. A variation to this method is used by [Chikkerur et al. 2006] that use localized texture features of minutiae and another one by [Zhengu et al. 2006] that uses texture correlation matching. Further, [Aggarwal et al. 2008] proposed gradient based approach to capture textural information by dividing each minutiae neighbourhood locations into several local regions of which histograms of oriented gradients are then computed to characterize textural information around each minutiae location. Recently, [that et al. 2011] proposed that Texture feature of Energy of a fingerprint can be used for effecting fingerprint verification [5][12].overall Comparison as shown in figure 2.

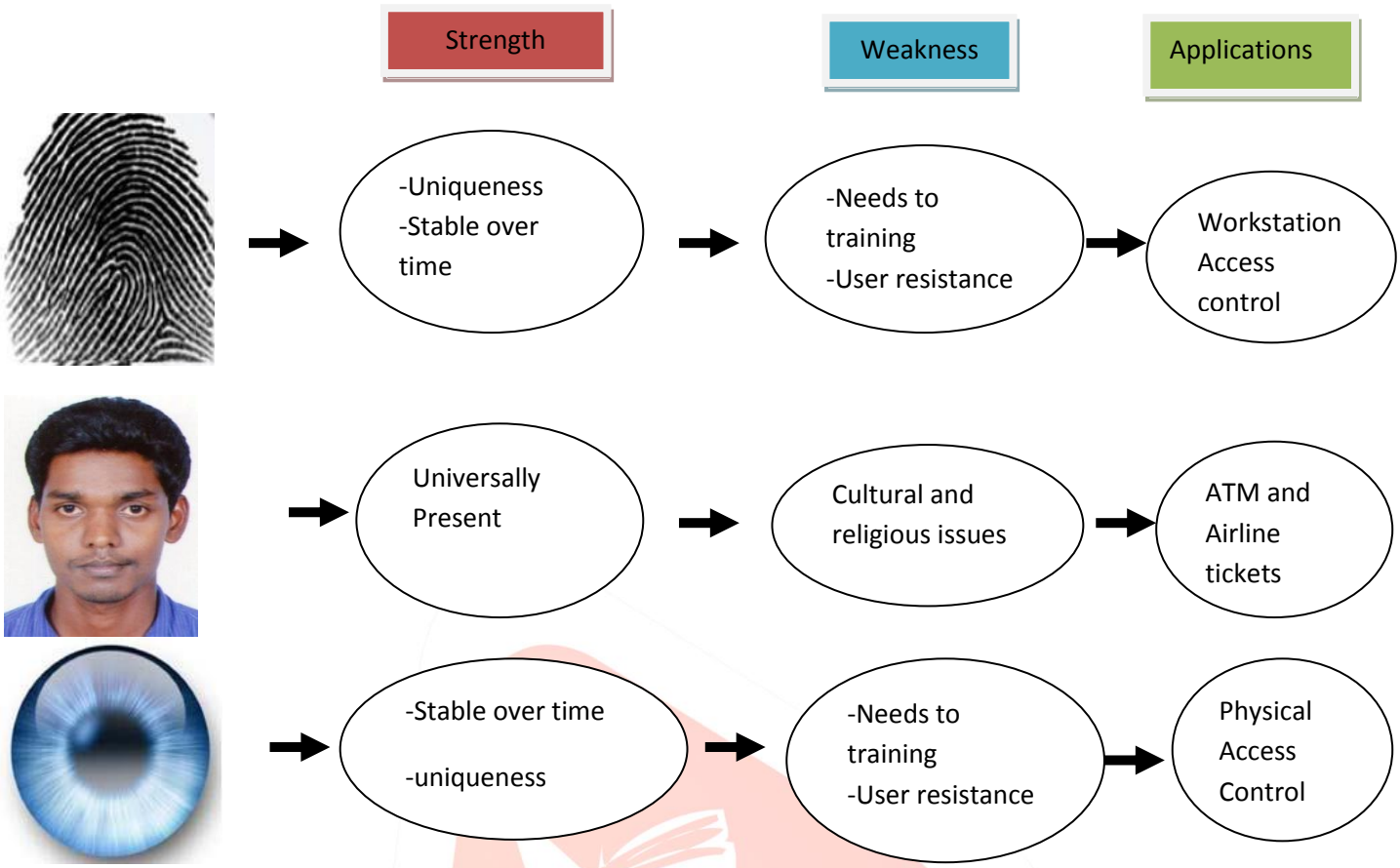


Figure 2: Comparison of Biometric Authentication

III. PROPOSED METHODOLOGY:

Biometric authentication technologies such as face, finger, hand, iris, and speaker recognition are commercially available today. In our proposed scheme we are using mobile client and biometric server architecture. Mobile will act as a client and the bank website will act as a server (host server). Once fingerprint is taken as a login, it sent to the server for matching as request, and server send the reply message. If it is matching then only login will be successful and user can do the transaction. In the client server module for providing the enhanced security authors use the encryption technique so at the wireless transmission no one can hack the fingerprint template [8].Over all architecture as shown in figure 3.

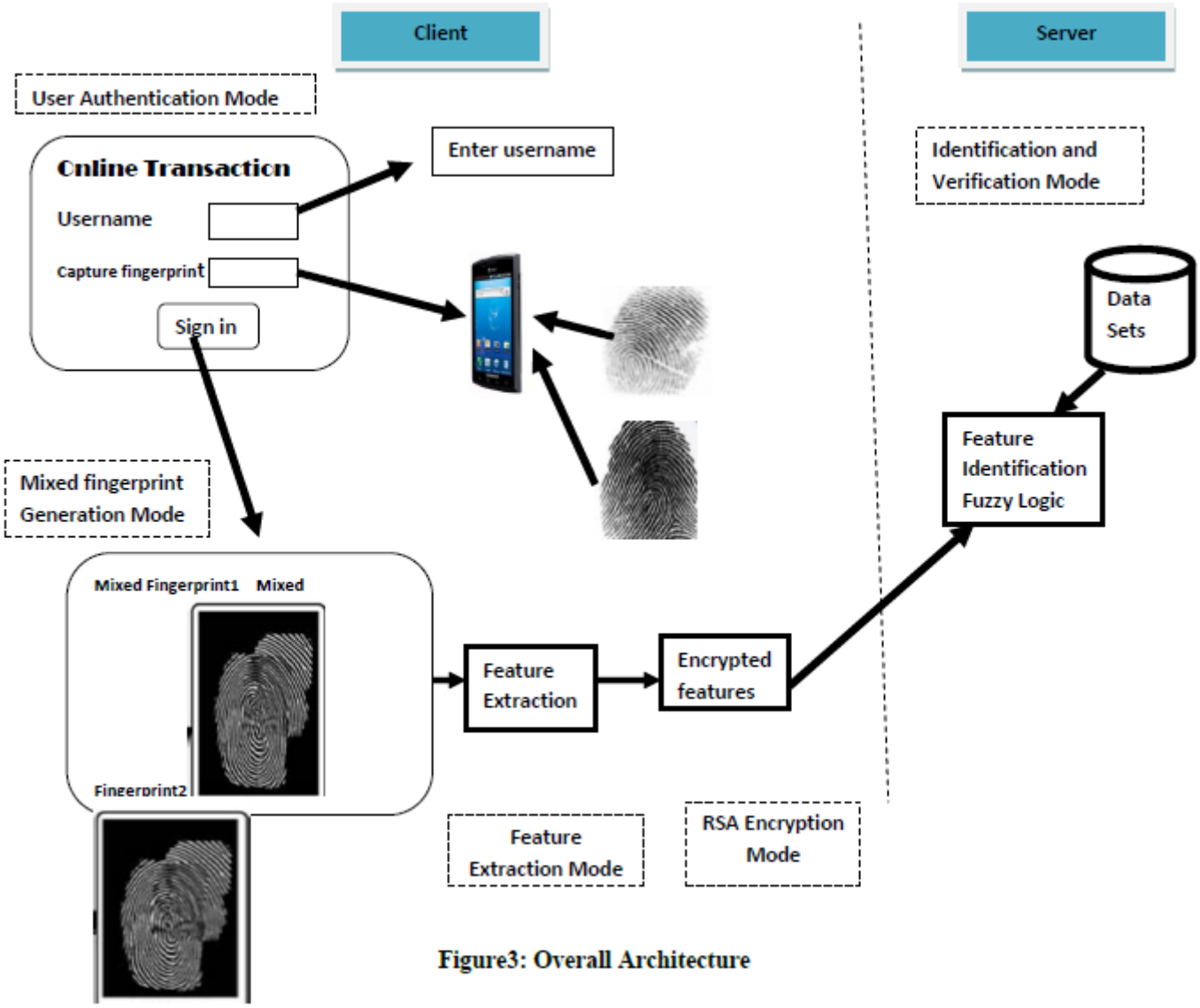


Figure3: Overall Architecture

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the context, a biometric system may operate either in verification mode or identification mode. In the context of fingerprints, image-level fusion has been used to combine multiple impressions of the different finger. In our proposed system fingerprint mixing can be used to generate a large set of virtual identities.

At the highest level, all fingerprint recognition systems contain two main modules mixed finger *feature extraction* and mixed finger *feature matching*. Feature extraction is the process that detects singular and all other minutiae points which are ridge ending and ridge bifurcation which differentiate one fingerprint from another which impart individuality to each fingerprint. "from the original image that can later be used to represent each fingerprint. Feature matching involves the actual procedure to identify the unknown person by comparing extracted features from his/her fingerprint with the ones from a set of known persons.

The objects of interest are generically called patterns and in our case are images of fingerprints matrix called vectors codes or fingercodes that are extracted from an input image using the techniques described in the later section. The classes here refer to individual person. Since the classification process in our case is applied on extracted features, it can be also referred to as feature matching.

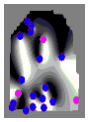
***USER AUTHENTICATION MODE*:**

In the user authentication mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, (usually via a PIN Personal Identification Number), a user name, a smart card, etc., and the system conducts a one to-one comparison to determine whether the claim is true or not [11]. Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

MIXED FINGERPRINT GENERATION MODE

Fingerprint mixing can be used to generate a large set of virtual identities. These virtual identities can be used to conceal the original identities of subjects or be used for large-scale evaluation of algorithms. The mixing process begins by decomposing each fingerprint image into two different components, viz., the continuous and spiral components (see Figure 1). Next, the two components of each fingerprint are aligned to a common coordinate system. Finally, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint.

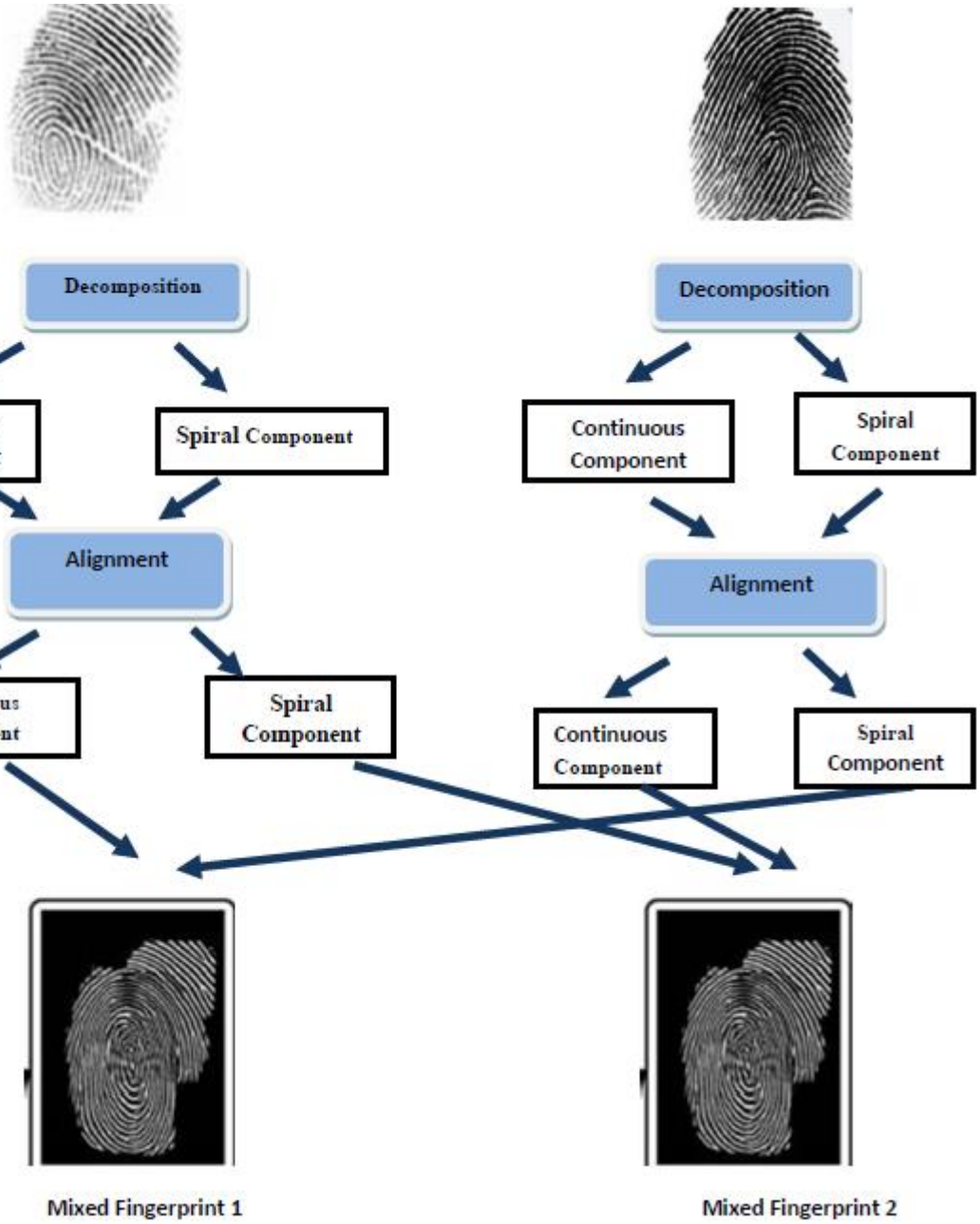




a) Finger print image b)Continuous component c) Spiral component

Figure 4: classification of Finger image

The experimental results confirm that (a) the new fingerprint .representing a new identity, can potentially be used for authentication; (b) the mixed fingerprint is dissimilar from the original fingerprints; and (c) the proposed method can be utilized to generate different-sized databases of virtual identities from a fixed fingerprint dataset. Mixed fingerprint process as shown in figure 5.



RSA Encryption Mode

Here authors prefer Android mobile for secure payment application. The mobile phone landscape changed last year with the introduction of smart phones running Android, a platform marketed by Google. Android phones are the first credible threat to the iPhone market. Not only did Google target the same consumers as iPhone, it also aimed to win the hearts and minds of mobile application developers. On the basis of market share and the number of available apps, Android is a success.

Android is an application execution environment for mobile devices. It includes an operating system, application framework, and core applications. The Android software stack is built on the *Linux kernel*, which is used for its device drivers, memory management, process management, and networking. The next level up contains the *Android native libraries*. Various system components in the upper layers use these libraries, which are written in C/C++. A payment application would be installed onto a android device, for authentication finger print is taken at run time. The finger print template would be captured by the phone and compared against a stored template on a database
server.

The fingerprint template is encrypted by using the RSA algorithms and sends it to the host server (i.e .Bank). Fingerprint is used for the login purpose for the bank application on mobile. The RSA cryptography is one of the well known public-key cryptosystem that offers both encryption and digital signatures (authentication). The RSA cryptosystem is the de facto standard for public-key encryption and signature worldwide. It is implemented in the most popular security products and protocols in use today, and can be seen as one of the basis for secure communication in the Internet [9].

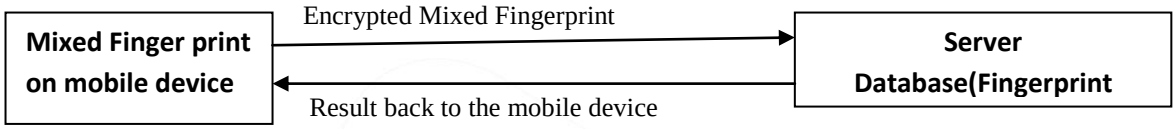


Figure 6: Encryption process

Proposed Fuzzy Logic System

A commercial fingerprint-based authentication system requires a very low False Reject Rate (FRR) for a given False Accept Rate (FAR) where FAR is the probability that the system will incorrectly identify and FRR is the probability of failure in identification.

Fuzzy logic here is used to calculate the percentage of various features presents in the given mixed fingerprint. If feature matching percentage is 100% then the biometric system successfully authenticate the user. Or else the matching percentage is 60% to 99% then the system will ask some security questions that are already stored in the database system during registration process. In case of below 50% matching the user authentication should be failed and user may reenter the fingerprint and try it again.So it will Generally fuzzy logic consists of three important steps. This includes fuzzification, generating fuzzy rules and defuzzification. In the fuzzification process the system data is converted in to fuzzy data. For fuzzification process triangular membership function is used. Next process after this is generating fuzzy rules.

Our method is, also, based on the minutiae points of the fingerprints. We can identify at least 40 minutiae points on a fingerprint, depending on its quality. In general, the number of the minutiae points varies from 0 to 100. All the methods mentioned above can be applied to a fingerprint verification. But, for an identification we need an algorithm with a low level of complexity because the data bases used in practice have millions of fingerprints. To reduce the search time and complexity, we first propose to classify the fingerprints, and then, to identify the input fingerprints only in one subset of the data base.

To choose the right subset the fingerprint is matched at a coarse level to one of the existing types. After that, it is matched at a finer level to all the fingerprints of the subset. The FBI in the United States recognize eight different types of patterns. For example, we have an input fingerprint and we want to identify it in a data base with 15000 entries. We will take the minim number of minutiae points, 40. If no classification is made we have to do at least $40 \times 15000 = 600000$ operations. But, if we use a classification with eight types (each subset has the same number of fingerprints $15000/8 = 1875$) we will have at least $(8+1875) \times 40 = 75320$ calculations. This is because we will first compare the input fingerprint with each group and after that it will be compared with each element of the chosen group [10]

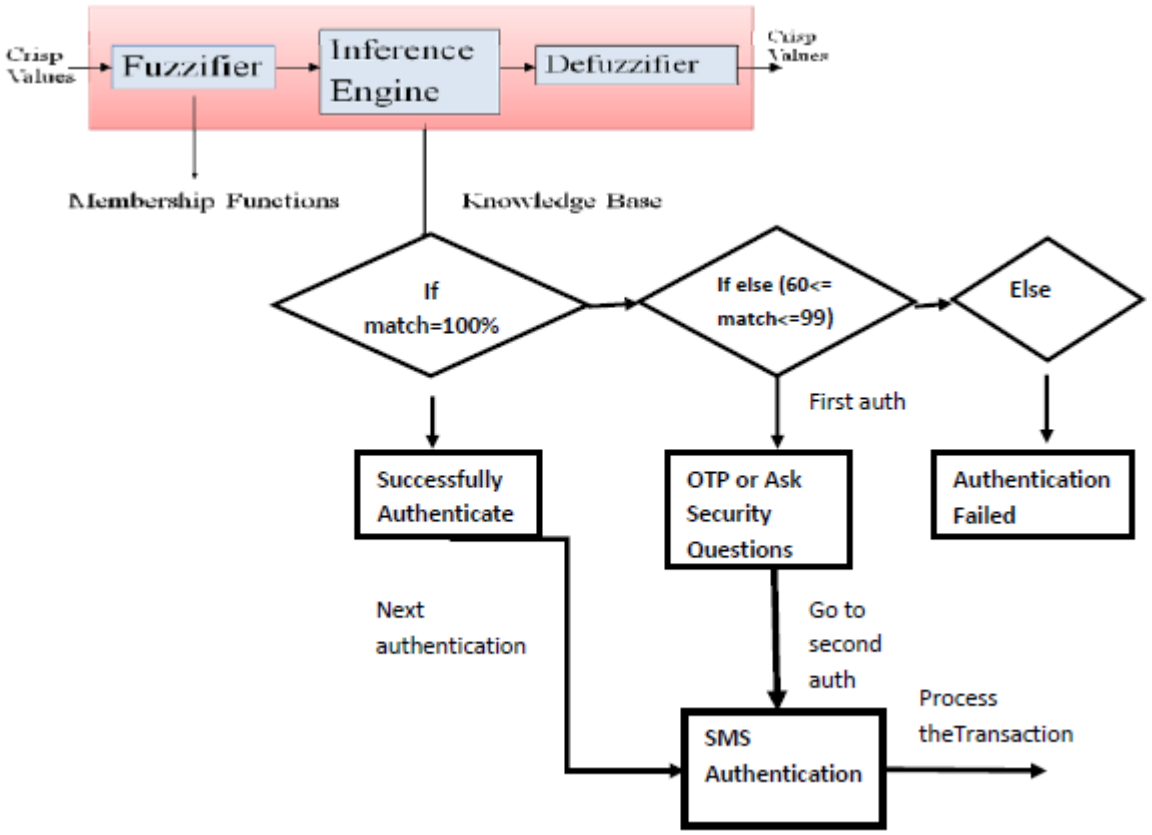


Figure 7: Fuzzy logic process

As we can see, the calculations are reduced to only 12,5%. The classification of the fingerprints is preferred to have more than three types of subsets. This is because a higher accuracy is achieved. Such a classification, also, helps to reduce the number of calculations with a higher percentage. Fuzzy control provides a formal methodology for representing, manipulating and implementing human's heuristic knowledge about how to control a system. In a fuzzy logic controller, the expert knowledge is of the form.

IF (a set o f conditions are satisfied) THEN (a set o f consequences are inferred)

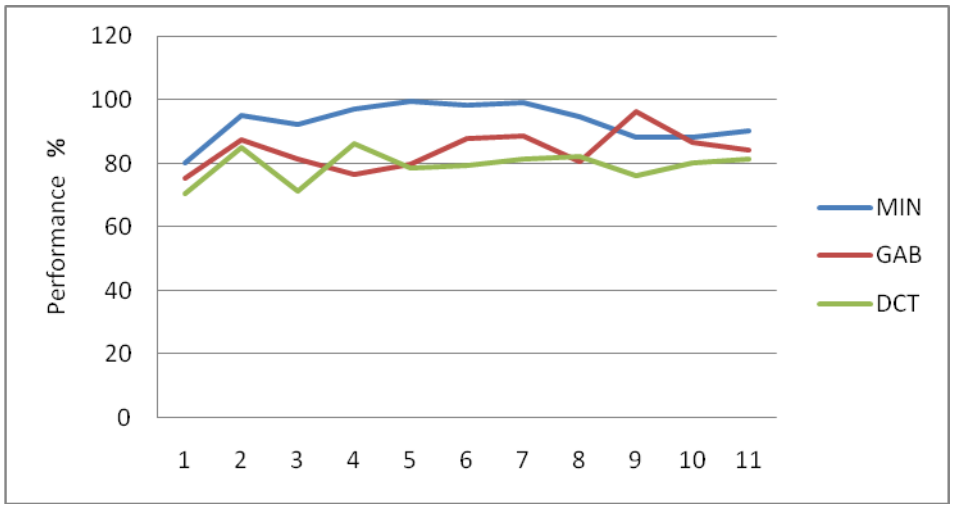
where the antecedents and the consequences of the rules are associated with fuzzy concepts (linguistic terms). The most known systems are: Mamdani, Tsukamoto, Sugeno and Larsen which work with crisp data as inputs. A Mamdani type model which works with interval inputs.

In this paper we use a version of Fuzzy Logic Control (FLC) system in fingerprints identification. This version is characterized by:

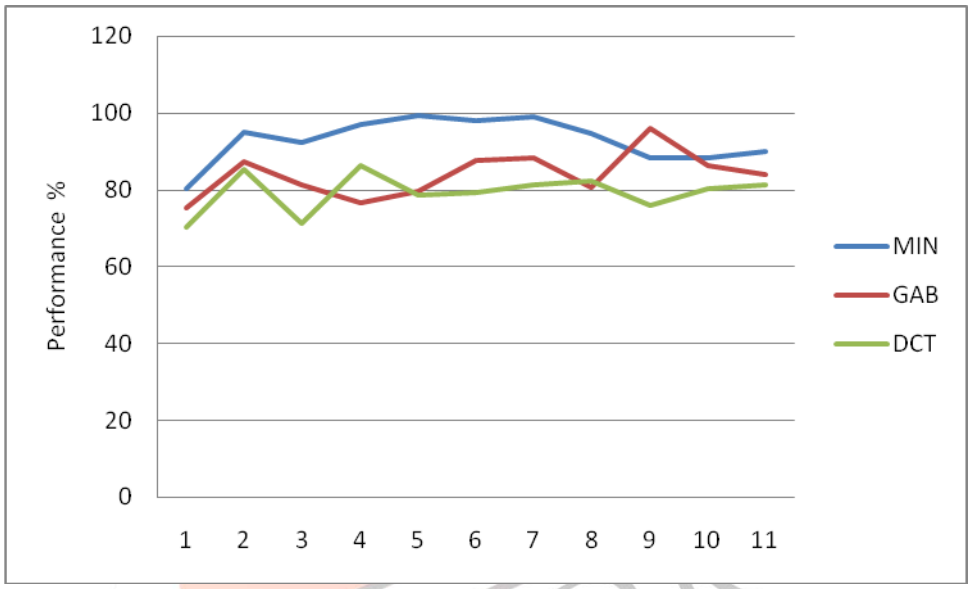
• the linguistic terms (or values), that are represented by trapezoidal fuzzy numbers
• Lukasiewicz implication, which is used to represent the rules
• the crisp control action of a rule, computed by Middle-of-Maxima method
• the overall crisp control actions, computed by discrete Center-of-Gravity.

PERFORMANCE EVOLUTION:

We demonstrated that incorporating the mixed fingerprint authentication in the online online transaction system improves the system performance. In the first test, the single fingerprint was applied. Each fingerprint image in the data set was directly matched against the other fingerprint images in the database. In the second test, the mixed fingerprint authentication method was applied to each fingerprint image in the data set. Then, the verification was conducted on the mixed fingerprint images. The receiver operating curves (ROC) resulting from these two tests are shown in Fig. 12. From these experimental results, we can observe that the performance of the fingerprint verification system is significantly improved when our mixed fingerprint is applied to the input fingerprint images. The proposed approach enhance the single fingerprint algorithm In particular, the enhancement algorithm substantially reduced the false reject rate while maintaining the same false accept rate.



a) Single Fingerprint



b) Mixed Fingerprint

Variations in the orientations and frequencies of ridges between fingerprint images can result in visually unrealistic mixed fingerprint images. This issue can be mitigated if the two fingerprints to be mixed are carefully chosen using a compatibility measure. In this paper, the compatibility between fingerprints is computed using nonminutiae features, viz., orientation fields and frequency maps of fingerprint ridges. The orientation and frequency images are computed from the pre-aligned continuous component of a fingerprint using the technique Then, Yager and Amin's approach is used to compute the compatibility measure. To compute the compatibility between two fingerprint images, their orientation fields and frequency maps are first estimated. The performance of the proposed approach to generate virtual identities was tested using the fingerprint dataset from the West Virginia University (WVU) multimodal biometric database. A subset of 300 images corresponding to 150 fingers (two impressions per finger) was used. For each finger in the WVU dataset, one impression was used as the probe image and the other was added to the gallery resulting in a probe set *P* and gallery set *G* each containing 150 fingerprints.

In the following experiments, the VeriFinger SDK was used to generate the normalized fingerprint images and the matching scores. Also, an open source Matlab implementation based on Hong et al.'s approach was used to compute the orientation and frequency maps of the fingerprints. In order to establish the baseline performance, the images in *P* were matched against those in *G*. This resulted in a rank-1 accuracy of 100% and an Equal Error Rate (EER) of 0%.

The RSA cryptosystem is the de facto standard for public-key encryption and signature worldwide. It is implemented in the most popular security products and protocols in use today, and can be seen as one of the basis for secure communication in the Internet. Its underlying function and properties have been extensively studied by mathematicians and security professionals for more than a quarter of a century. While a number of attacks have been devised during this period, exploiting special properties of the RSA function as well as details in particular implementations, it has stood up well over the years and its security has never been put into doubt. No devastating attack has ever been found and most problems appear to be the result of misuse of the system, bad choice of parameters or flaws in implementations. In fact, years of research have probably increased the trust the security

community has on RSA, and we have every reason to believe that it will remain the most used public-key algorithm for years to come.

CONCLUSIONS

We performed three different feature extraction methods for fingerprint authentication and reported the results on their security compromise. Our results indicate that Minutiae's have the best performance to provides secured m-commerce. In this work, the design approach for a Biometric Mechanism for enhanced Security of Online Transaction on Android system has been proposed. Here run time fingerprint would be captured for mobile transaction; it is not stored already in the mobile device so it provides more security and not stolen by third party. We also generating a virtual identity by mixing two distinct fingerprints were explored, by overlapping the components of each fingerprint. In this work, the possibility of experiments fingerprint dataset show that the mixed fingerprint representing a new identity can potentially be used for authentication and the proposed method can be utilized to generate a database of virtual identities from a fixed.This gives the better level of security mechanism for m-commerce system.

References:

[1] Mangala Belkhede*, Veena Gulhane**, Dr. Preeti Bajaj*** "Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach" ISBN 978-89-5519-163-9,Feb. 19~22, 2012 ICACT2012
[2] Fahad Al-harby, Rami Qahwaji, and Mumtaz Kamala "Secure Biometrics Authentication: A brief review of the Literature"
[3] Uday Rajanna Ali Erol George Bebis" A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion" Springer-Verlag London Limited 2009
[4]Yager N, Amin A (2004) Fingerprint classification: a review.Pattern Anal Appl 7:77–93
[5] Yager N, Amin A (2004) Fingerprint verification based on minutiae features: a review. Pattern Anal Appl 7:94–113
[6] T. Ahonen, A. Hadid and M. Pietik ¨ ainen, "Face recognition with local binary patterns", European Conference on Computer Vision,Prague, 469–481, 2004.
[7] John Daugman "New Methods in Iris Recognition" VOL. 37, NO. 5, OCTOBER 2007
[8] Kawagoe M, Tojo A (1984) "Fingerprint pattern classification". Pattern Recognit 17(3):295–303
[9] Dr. Manish Manoria,Ajit Kumar Shrivastava,Satyendra Singh Thakur,,Debu Sinha.(2011)" Exploring the Prospect of Secure Biometric Cryptosystem using RSA for Blind Authentication".
[10] System I. Iancu, N. Constantinescu, M. Colhon "Fingerprints Identification using a Fuzzy Logic" ISSN 1841-9836, E-ISSN 1841-9844 Vol. V (2010), No. 4, pp. 525-531
[11] Dr Suresh Sankaranarayanan, "Biometric Security Mechanism in mobile Payment", Published by the IEEE Computer Society, 2010.
[12] Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik (2008) "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications"