2009 International Conference on Machine Learning and Computing
IPCSIT vol.3 (2011) © (2011) IACSIT Press, Singapore

A Biometrics Based Secure Communication Scheme for Bluetooth Environment

Mostafa Akhavan-E-saffar [+]

ICT Msc of, Iran university of Science and Technology Islamic Azad University of Tabas

Abstract. A novel personnel authentication and verification system for devices communicating through Bluetooth protocol has been proposed in this paper. Unlike existing verification systems which provide password or a PIN as a key, the system uses biometrics features as a key. In the implementation of the scheme, ridges and bifurcation based parameters are derived to generate a 128 bit Bluetooth pairing PIN In this paper a unique translational and rotational invariant feature set has been developed. These extracted feature data, unlike traditional systems which include the extracted data into payload, is used for device connection by generating the 128 bit PIN the system performance is analyzed using the pairing PIN for inter-sample and intra-sample recognition To validate the stability of the system the performance is analyzed with external samples which are not a part of the internal database .

Keywords: Bluetooth, fingerprint,pairing, Authentication,biometric

1. Introduction

The offices of yesterday were a mesh of wired cables which often resulted in confusion with the exponential growth in peripheral devices. With so many devices like fax machines, printers, desktops, laptops, landline phones, the hazard and the clutter associated with the cables could not be overlooked . Bluetooth as a wireless network protocol provides a low-cost solution, for a wireless and cable free work area. Most of the electronic devices which are widely and commonly at workplaces, home and commercial establishments are Bluetooth enabled. the Bluetooth devices when connecting to each other follow the Bluetooth protocol where two devices share a common pairing key. the pairing keys chosen are based on choice of the user and are easy to be hacked and use by impostors, which can lead to serious security issues in places where high level of security is required. Biometric features provide the capability of a secure authentication because of the uniqueness associated with them. Among the extractable and collectible features, fingerprints have acquired widespread acceptance because of the ease associated with their collectibility and uniqueness. Other biometrics features are also widely used, but have certain disadvantages associated with them . A system which can combine the wireless connectivity of the Bluetooth with the user-specific advantage of biometrics can provide a solution for scenarios, where high level security is required. Suppose, a user enters a high security wireless area and he/she wants to access the database of the system. If he/she happens to be a legitimate user, he/she can pair with the database master device and become a part of the whole set-up. As opposed to the other valid and established systems, the system will use the biometric data to generate the pairing key between the two devices. Thus the devices connected are not only permitting a legal user, also the slave device can be synchronized as per the user logging in, into the system .

2. BIOMETRICS AND BLUETOOTH

2.1. Biometrics

Biometrics is the SCIence of identification of an individual based on the measurements of his physical

[+] Tel:+(98 ,09133567433);Fax:+(98,03534221270);
E-mail address:(akhavansaffar@gmail.com)

characteristics.Biometrics authentication or, simply biometrics refers to establishing identity based on the physical and behavioral characteristics (also known as traits or identifiers) of an individual such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc [Jain 2004].the behavioral features include speaker recognition, keystrokes and signature dynamics.the physical characteristics are iris scan, fingerprint recognition, hand geometry, retinal scan, DNA etc .[12]

2.2. Use of Biometrics

A large number of systems require reliable personal recognition to either confirm or determine the identity of the individual who require service.Only legitimate users should access the services rendered by these systems.for example, usage of cell phones, ATM, access to secure areas should be restricted to only authorized people.Biometrics systems are pattern recognition systems which can be utilized in two ways .In a one-to-one comparison between an individual and a stored biometrics, and in a one-to-many comparison between an individual and multiple biometrics on a database. Biometrics has certain salient features which makes it useful for authentication .Some of these salient features are:

- Universality: Every person has characteristics.
- Distinctiveness :No two persons have the same characteristics.
- Permanence: the characteristics do not change over a period of time.
- Collectibility: the characteristics can be measured quantitatively.

A generic biometrics system is described in figure 1

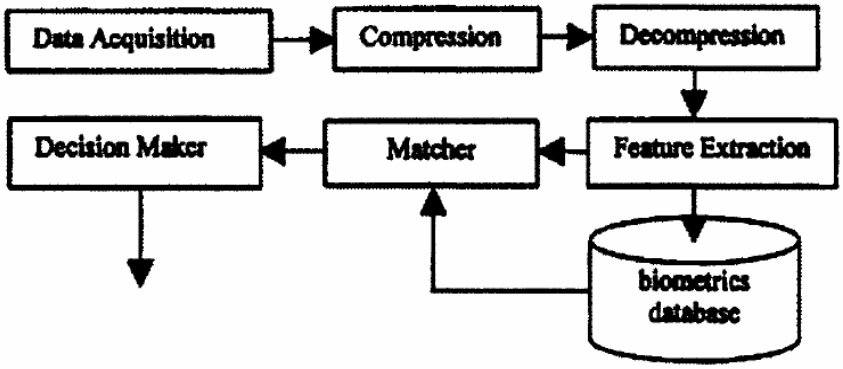

Figure1: generic biometrics system

In this system, data is acquired using a device, like scanner, voice recorder, etc. the acquired data is used to extract quantifiable features .Some of the features like minutiae of fingerprints, unique vessel pattern of the iris, length of the fingers in hand geometry, etc are used for extractable features.the extracted data is compared with the database and depending on the result of a match or a mismatch, authentication or identification is performed Encryption required: Access to the service is possible only after the link has entered encrypted mode.[9,10]

2.2.1 Types of Biometrics

As was discussed earlier, there are several biometrics features which can be utilized for biometrics systems:

Fingerprint: Fingerprints are the most widely used biometrics systems.Fingerprints are widely used by FBI for secure authentication.

Voice Recognition:A popular methodology for implementing voice recognition would involve recording a user's voice over a given system and then comparing them with a database.Voice recognition systems have 1 to 2% False Acceptance Rate FAR [Woodword 2003] and are not robust on their own, but can be combined with other systems to provide lower FAR.

Iris Recognition: Iris Recognition based models are unique, invariant and have higher confidence than fingerprints.However iris recognition was not widely used so far because of the patent issues.the patents on iris recognition technology have expired recently and they are supposed to become more popular.

Face: Face recognition are often used for verification, as required in picture IDs[Shen 1999], as an easy

means of identification for the eyes of humans.Also two twins may have same features.

Hand Geometry: Hand geometry means the measurement of human hand geometry and is used by measuring the size of human fingers, knuckles etc. it can be combined with other biometric projects.it is not exclusive like finger printing and retinal eye scan. the figure2 provide a survey of the various biometric features in use.

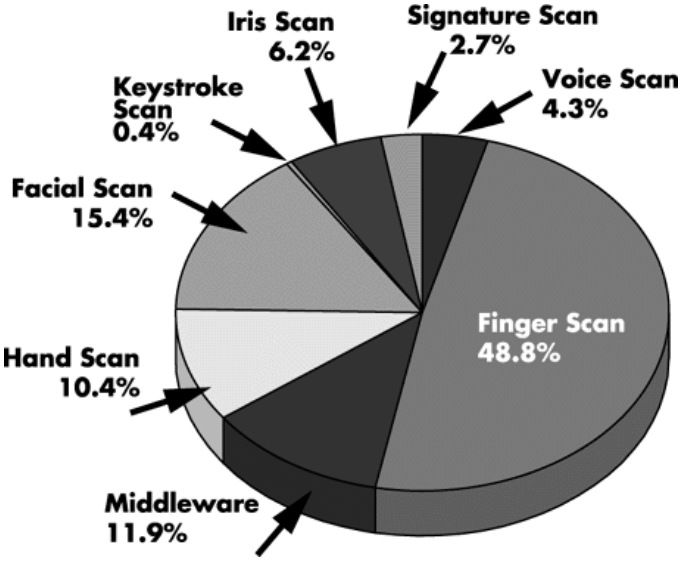

Figure2: comparative commercial usage[6]

2.2.2 Why fingerprints for our scheme

Fingerprints based biometrics authentications have been used extensively for authentication and verification.FBI has been using fingerprint based authentication for a long time.One of the reasons for the widespread use of fingerprints is their uniqueness.This is primarily because of the ease of collection and highly unique structure of the fingerprint.Fingerprints can be easily classified based on their minutiae and ridges.Also, fingerprint based systems can be used for user authentication in many systems such as personal laptops, enterprise systems, etc., due to their high accuracy (lower false accept and reject rates relative to voice and face-based solutions) and lower cost (relative to techniques such as iris recognition)

3. BLUETOOTH

Bluetooth data transmit on the unlicensed 2.4GHz ISM band. ISM band stands for industrial, scientific, and medical radio bands. It defines and reserves radio frequency for industrial, scientific, and medical purposes [2]. Bluetooth uses a frequency-hopping scheme in order to minimize the interferences with other technologies and applications such as 802.11, microwave ovens, cordless phones, etc.The connection range of off-the-shelf Bluetooth devices vary from 10 meters to 100 meters. Each Bluetooth device has a globally unique 48bit MAC address. The first 24 bits of the Bluetooth address is vendor specific. Forexample 0:14:9A:C9:20:10

3.1. Bluetooth Securoty

The primary emphasis of the Bluetooth security architecture involves link and network service protection. To do this, Bluetooth security mechanisms enforce authentication based on shared secret exchange, separable authorization for trusted versus untrusted connecting devices, and communication encryption. In this chapter the procedures that allow devices to exchange link keys, authenticate, establish secure sessions, and gain authorization to access network services are briefly summarized.A short description of the Bluetooth security algorithms is given at the end.[1]

3.2. Security Modes

Three security modes are described in the Bluetooth specification. They are defined as follows.

- Mode 1: No security. A device will not initiate any security at all.
- Mode 2: Service-level security. A channel on L2CAP level is first established without any security

procedures. Depending on which applications are running, different security requirements can be set for each one of the applications.

- Mode 3:Link-level security. Before establishing a channel on L2CAP the device initiates security procedures for a secure connection. This is the built-in security mechanism and it is not aware of service- or application-layer security.

For security mode 2, settings per device basis and per service basis are made. Two databases are used, one to hold device information and one to hold service information.The service database contains the security configuration as provided by the application software. The device database holds information regarding past sessions with other devices [3]

Two trust levels are specified: trusted and untrusted. Trusted devices are paired and that are marked as trusted in the device database. This level has unrestricted 15 access to all services. Untrusted devices are unknown or are paired but not marked in the database as trusted. This level has restricted access to services. Untrusted devices must be authorized to access a service if authorization is required (see below).A new device is always regarded as untrusted [4].Three levels of service security are defined so that the requirements for authorization,authentication, and encryption can be set independently. For example, services can be set to require authorization and authentication, require authentication only,and set to be open to all devices. The three attributes that determine the level ofsecurity are as follows [5].

- Authorization required:Access to the application is granted automatically to trusted devices and onlyafter an authorization procedure granted to untrusted devices. Authorization always includes authentication.
- Authentication required: The remote device must be authenticated before being allowed to connect to the local service.
- Encryption required: Access to the service is possible only after the link has entered encrypted mode.[2,3]

3.3. Key Management

The Bluetooth security architecture is based on symmetric key cryptography where two Bluetooth devices share a common link key for authentication and encryption. Figure 1 shows the Bluetooth key structure.and his description in table 1

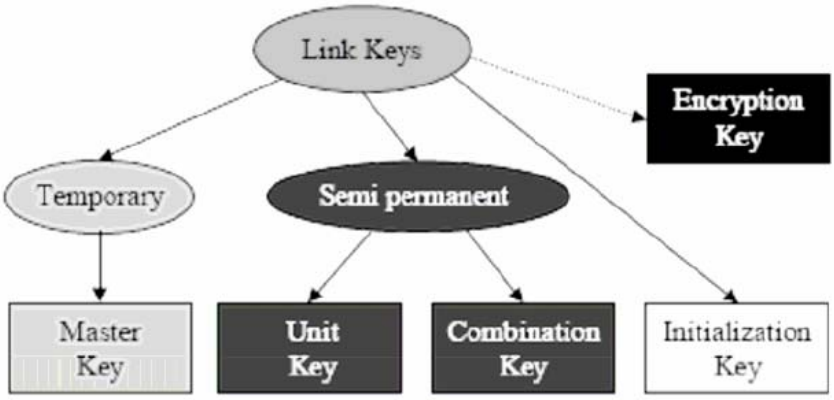

Figure1:Bluetooth Key Structure

Table 1:Bluetooth Keys

Key name	descriptions
Initialization Key	The initialization key (Kinit) is the first key being generated in the pairing process. It is used to derive combination or unit keys later on in the pairing process. Once a combination or a unit key is derived, the initialization key will be discarded. Note that the strength of this key relies solely on a 4 to 16bytes PIN
Combination or unit keys	Combination keys (Kab) and unit keys (Ka) are semi-permanent in the sense that devices store them permanently unless they are being updated through the link key update procedures or the broadcast encryption scheme. These keys can be reused in multiple sessions by the devices that share them.

Master key	The Bluetooth specification defines shared master keys to allow piconet masters to encrypt broadcast traffic.
Encryption Key	Encryption keys (Kc) are derived from the current link keys and are automatically updated each time the devices enter encryption mode. KC is used to generate a cipher stream KCipher that in turn will be XORed with payloads.

Four hash functions are used in pairing, authentication, and encryption. The heart of all four functions is the SAFER+ block cipher.table 2.shows the hash functions

Table 2:Bluetooth security function

function name	descriptions
E22	The Bluetooth design uses E22 to generate initialization keys (Kinit)
E21	Bluetooth design uses E21 to generate unit keys
E1	The Bluetooth design uses E1 to generate authentication responses
E3	to generate the ciphering key Kc ,which is used by system E0 to generate key streams for encrypting message payloads in encryption

3.4. Pairing

Before two Bluetooth devices can establish a connection and send data to each other, they have to go through a pairing procedure, which is essentially a process for creating a common key for authentication and encryption between two Bluetooth devices.Figure 2 [3] show a simplified pairing .

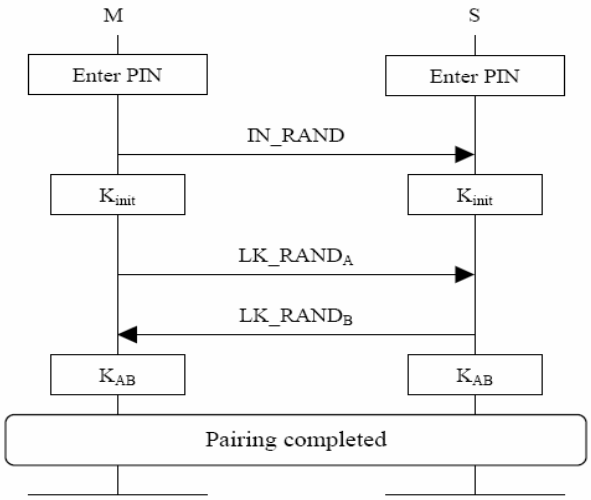

Figure2:A simplified Bluetooth pairing protocol

3.5. Authentication

Bluetooth security architecture uses a challenge-response authentication scheme. Figure 3 show a simplified authentication.[3]

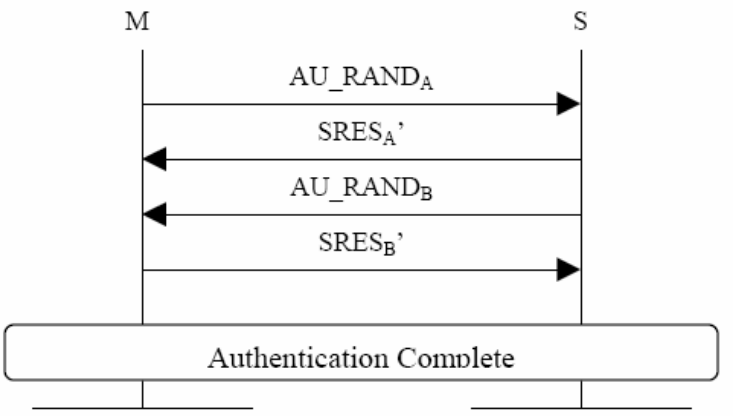

Figure3:A simplified Bluetooth pairing protocol

4. PROPOSED BIOMETRICS BASED SYSTEM

the most important part was to convert the data obtained from the fingerprint into 128 bits, which is the size of the encryption key in the Bluetooth payload. This issue involves data compression with a loss of information. e scanned fingerprint image is 260X300 78,OOO pixels with 4 bits/pixel representation, i.e., 16 gray levels, which is 312kb. Hence direct compression is very difficult and it is necessary to reduce raw data features to informative features like minutiae, ridges, bifurcations.

4.1. system description

The raw data from the fingerprint was obtained by taking multiple scans of the same finger using an optical fingerprint scanner .

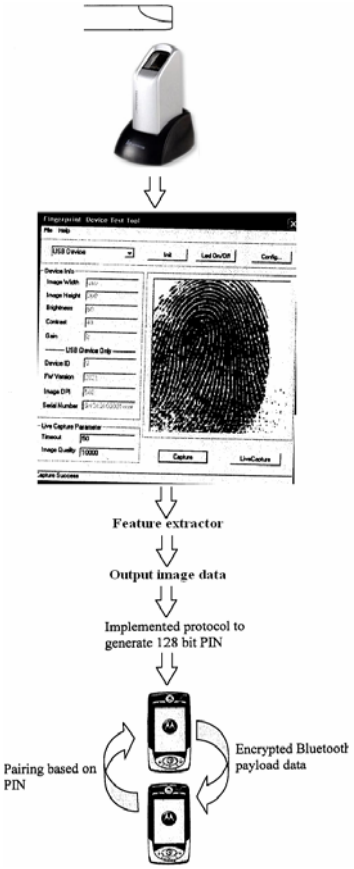

Figure6:Impelemented Syste, set-up

Along with the output image containing the marked minutiae points, the feature extractor also generates a file which contains the number and the location of the fingerprints in the input sample[14].

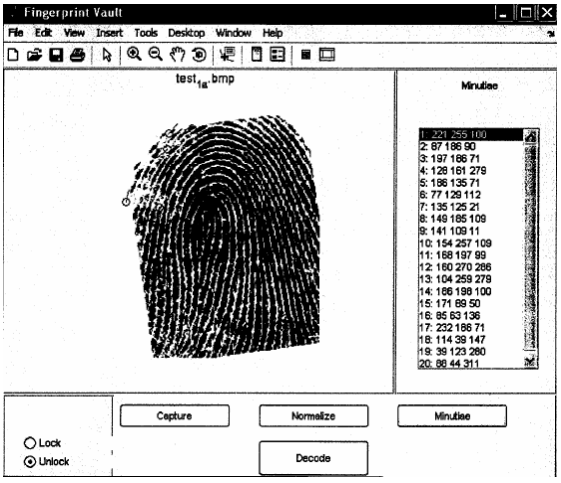

Figure7:Minutiae extraction

In the already normalized fingerprint image shown in the left pane, identified minutiae points. the right pane lists these points individually in the following format: minutia number, x-coordinate, y-coordinate, theta (angle) the following table is a tabular representation of the one of the fingerprints of the database the data obtained in the minutiae reading from the fingerprint has 4 fields[16]

Table 3 :The Output file format generated by the feature exteractor

X coordinate	Y coordinate	Angle	Type of minutiae	Random nimber
161	125	56	B	60
31	266	210	B	60
28	278	52	B	60
45	280	228	R	60
216	242	286	R	60

1)X co-ordinate- the first field.
2)Y-co-ordinate- the second field.
3)A, the angle the minutiae makes with respect to the origin
4)The type of the minutiae i.e., ridge type (R) or bifurcation (B).

4.2. Feasibility system

One of the early approaches which we adopted for achieving the goal was the use of Asus Bluetooth devices. Two Bluetooth adapters when connected over two different computer systems serve as a Bluetooth Piconet.

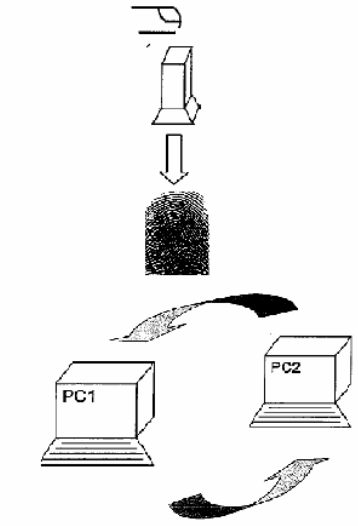

Figure 8 :the asus device set-up

Referring to Fig 8 the fingerprint from the finger is obtained by the scanner. the information obtained from the fingerprint was stored in first database system PC 1. PC2 had the stored information for the incoming fingerprints. the system did not convert the fingerprint data into Biometric PIN, which needs to be provided for Bluetooth protocol communication system Instead, it used the entire fingerprint data and plugged it into data field of the Bluetooth payload and then used its own algorithm for providing secure communication using that part of data field, and hence did not meet our stated objective [19]

4.3. the Implemented approach

This new method is based on rotation and translation invariant features of the fingerprint. the number of ridges and bifurcations of the fingerprints are invariant to the rotation and translation of the fingerprint the distance and the number of ridges and bifurcations is neither altered nor tempered when the fingerprint samples are utilized for extraction. the data extracted from these features are applied in study of biometric characteristics of False Acceptance Rate and False Rejection Rate . the first step involved in recognizing the features which would be independent of translation and rotation of the fingerprint. the uniqueness of the fingerprint is dependent on the ridges and bifurcations Total 6 parameters i.e., total number of minutiae, total

number of ridges, total number of bifurcations, maximum distance between minutiae, maximum distance between ridges and maximum distance between bifurcations of every person, were analyzed in the implemented approach. the samples chosen are the right hand thumb for every person. Total numbers of samples chosen are 10 per person. There are 11 people in the study. Therefore the total numbers of samples are 110. First step was to calculate the mean value of all the 6 parameters per person. the logic behind the thinking is that since the samples were collected from the same fingers the mean value should not vary too much for intra-person recognition. Table 4 shows a matrix which contains the information of all the 11 people with all the 6 parameters. the first column is the total number of minutiae, the second column is total number of ridges, the third column is the total number of bifurcations, the fourth column is the maximum distance between minutiae, the fifth column is the maximum distance between ridges, and the sixth column is maximum distance between bifurcations of every person .

Table 4:the value of the tempelates with their respective values

Template ↓	No. of Minutiae	No. of ridges	No. of Bifurcations	Distance Between minutiae	Distance Between ridges	Distance Between bifurcations
Template1	75	45	30	340	327	331
Template2	25	10	15	330	286	326
Template3	46	21	25	339	333	322
Template4	27	14	13	334	320	313
Template5	48	29	19	347	339	319
Template6	35	17	18	327	303	316
Template7	35	18	17	342	341	326
Template8	46	11	35	335	300	329
Template9	21	3	18	311	246	307
Template10	56	30	26	353	352	316
Template11	38	12	26	347	336	337

the next step involves calculating the difference of every fingerprint's 6 parameters with their corresponding parameters from the above mentioned matrix. the following computation was used to arrive at the results

$$\sum_{i=1}^{6} \frac{|X_i - T_{ij}|}{T_{ij} \ldots\ldots\ldots\ldots eq(1)}$$

X: incoming fingerprint file

T :Matrix corresponding to the fingerprint

i: parameter of the fingerprint

j: No of samples

As mentioned before, Tij contains the information about the average of all the six parameters obtained for every single person. Therefore the normalized distance between the same person's samples with its own template should be very small value. Since the fingerprints are a unique feature of a single person, these distances should also have the unique information about the person, i.e., they should be smallest for the same template. the next step involved in calculating the threshold values for all the samples. False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the functions of threshold values. FRR(False Rejection Rate) و FAR (False Acceptance Rate) .As was mentioned already the normalized distance for the same fingerprint samples with their own average, should be the least. the normalized distances were chosen as threshold values. For lower threshold values, only the lower distances should be accepted by the system and there will be a lot of false rejection. For higher threshold values, there will be a lot of false acceptance .In the further implementation, 100 more fingerprints were extracted from different people the 100 external fingerprints were registered in the system with the help of the 11 templates. the normalized distance of the external fingerprints was obtained with reference to the 11 templates the next step was to decide, whether to accept the fingerprint or to reject it. Threshold value was the parameter chosen for this decision. the samples

were analyzed for the randomly generated threshold values and then the total number of samples which were accepted and rejected on the basis of these threshold values.[20]

The normalized calculated distances generate some values which happen to be very small. These small values may be very close to one of the templates and the choice of threshold value groups the fingerprint with one or the other template. the iterations were run for each fingerprint and their threshold values, were calculated the next step lied in getting the data from the fingerprints into 128 bit. As was mentioned already mentioned that the PIN utilized in generation of the passkey for Bluetooth devices can be anything from 0-128 bit.

A simple approach was generated for utilizing the data obtained from the study, into a string of size of 128 bits or lesser the 6 parameters were concatenated into a string with the first 2 bytes being occupied with the number of minutiae the next 2 bytes with the number of bifurcations, the next 2 with the number of ridges. This data generated is similar to the one extracted in the previous studies.

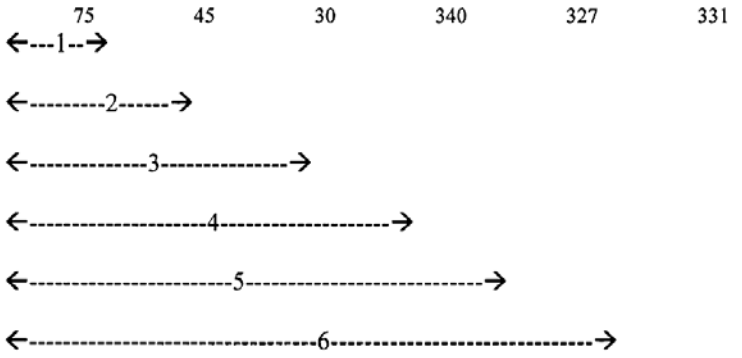

Figure 9:the data in the 128 bit fild

1) No. of Minutiae
2) No. of ridges
3)No. of bifurcations
4)Max distance between minutiae
5)Max distance between ridges
6) Max distance between bifurcations

In the assumed set up, the slave Bluetooth device searches for other Bluetooth device in its vicinity of 10 meters After finding the master device which, it needs to connect, the Bluetooth devices try to pair up with each other with PIN the 6 parameters from the incoming fingerprint file are concatenated as explained in the Fig. This will result in a PIN of size less than or equal to 128 bits. This PIN is entered into the slave device the Bluetooth protocol asks for the PIN on the Master device. From the master device, the 128 template string is entered into the device. If the PIN entered on the devices are found to be matched, then the devices are connected. the objective of the study was to convert the data from the fingerprint file into 128 bit PIN. the data thus obtained will have less than 128 bits and still has enough data space for appending more data.[21,22]

5. Results

The overall devised scheme as discussed was implemented through program written entirely in C language. the following sections will describe the step-by-step analysis of the whole scheme.

5.1. Database set-up

The 11 template constituting the database have been listed as per their order in the database. For all the 11 templates 10 prints of the same thumb were analyzed. the following Figure 10 shows the thumbprint which has the nearest value for its own subject.

5.2. study of Template 1

Reviews the template 1 and all its 10 fingerprints. it was observed during the study that the fingerprints of subject 1 were somewhat unique, since it did not get misclassified as any other fingerprint template. Also

none of its fingerprints were recognized as any other fingerprints. Thus we can state that it was an ideal example, since it was always correctly classified. the following Figure 11 contains all the 10 fingerprints of the template 1.

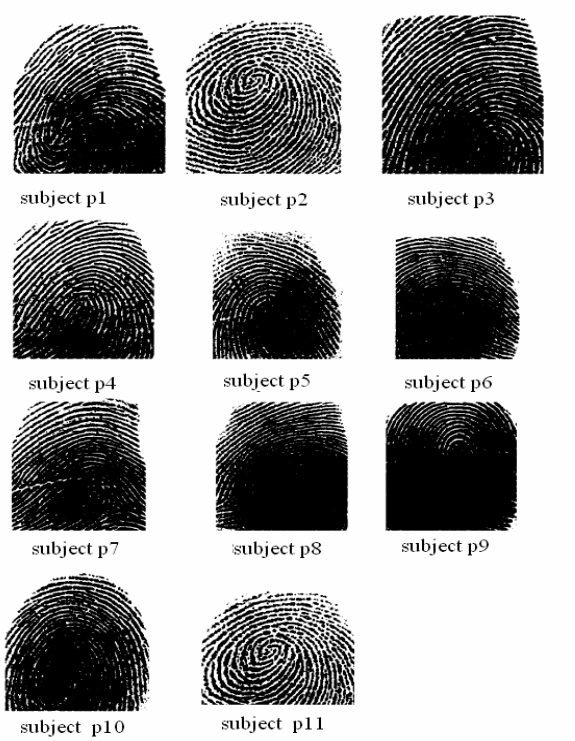

Figure 10 :all the 10 template of the study

Figure 11:all 10 fingerprints of template1

5.3. Correct Acceptance and Wrong Acceptance

One of the major considerations of this study has been to establish, which samples were correctly accepted and which samples were wrongly rejected, to justify the system functionality.

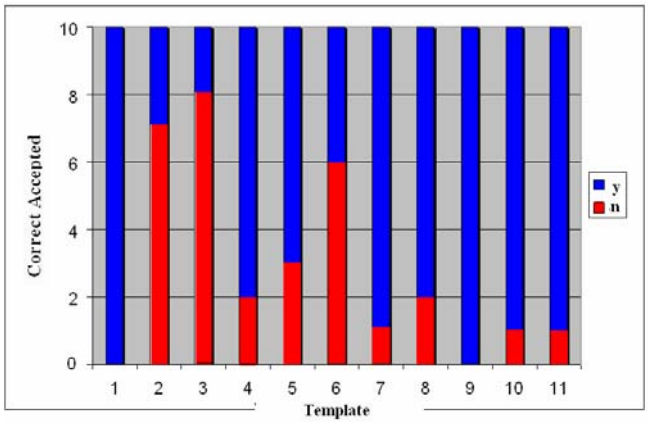

Figure 12 :Total correctly accepted sample

Referring to Figure 12, the horizontal axis indicates the template number and the vertical axis indicates the total number of samples of the template in consideration. the bar-graph shows which fingerprints were correctly accepted or wrongly accepted as indicated by the blue bar. it also shows which fingerprints were wrongly accepted as another template (red bar)

5.4. the Variation of the threshold values for the Samples

we analyses the effect of variation in the threshold value with respect to recognition value of samples .

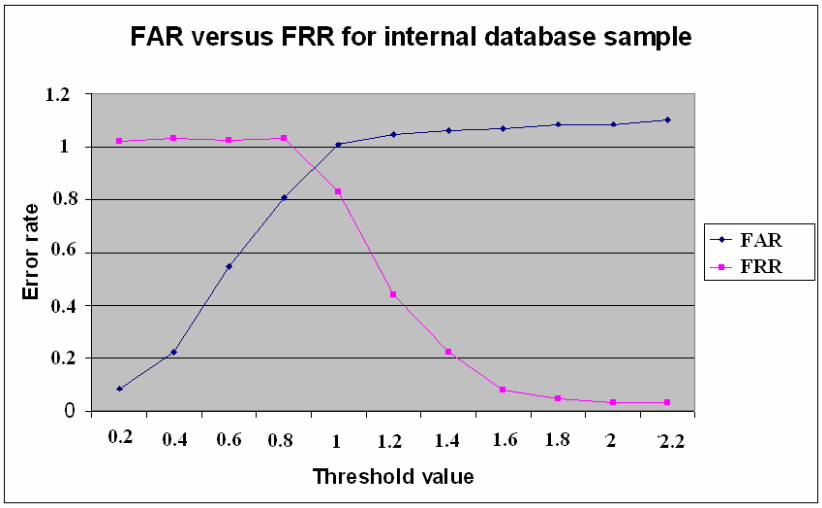

Figure 13 :FAR versus FRR for internal database sample

Figure 13 shows that initially FARis constant till the value of threshold 0.6, after that it starts decreasing from 0.85. The Equal Error Rate (EER) for the internal samples occurs at a value of 1.05.

5.5. Study of template 7

This section shows the template 7, all its fingerprints and we explain which one is being getting recognized as which one. The close observation of any sample suggests presence of the arches and the delta together in the fingerprint template. This can be suggested as one of the reasons why this fingerprint is being recognized as some other template. Also since both template 7 and template 6 have the same number of minutiae, most of the template 7 fingerprints (4 fingerprints) are recognized as fingerprint 6.

5.6. A discussion on high recognition and authentication/or template 1, 2 and 3

The results for High value of True Acceptances of subject 1 and high rate of False acceptance for subjects 2 and 3. Template 1 enlists 75 minutiae. All the other 10 templates have fewer than 75 minutiae. it can be suggested that for correct authentication a fingerprint with a large number of features has more probability for being correctly recognized. For fingerprint template 9, there are only 3 ridges, and 18 bifurcations on an average. The lower number of ridges or the absence of a large number of features, make it a unique finger print

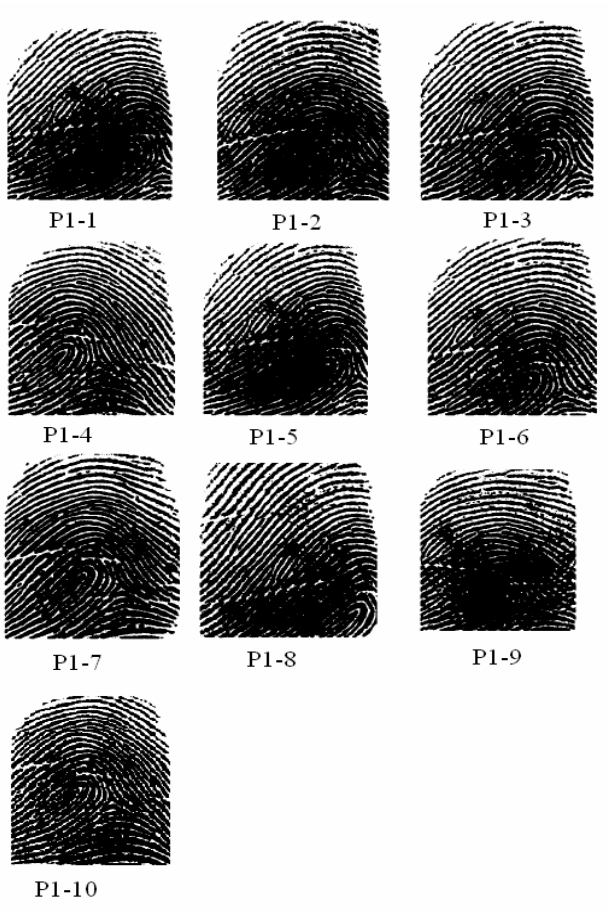

Figure14 :10 fingerprints of sample 7

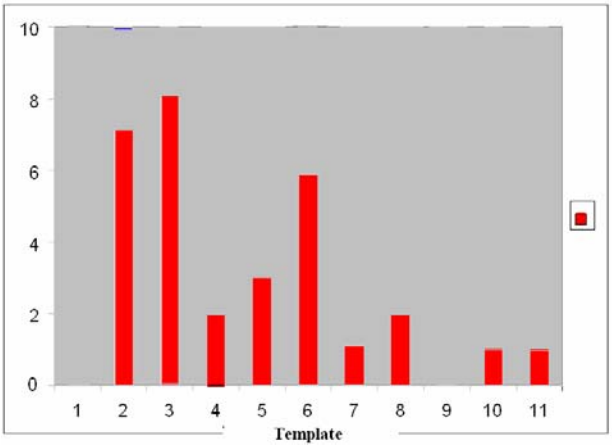

Figure15 :the wrongly recognized subjects

As can be seen in this table Figure 15, template 2 & 3 are wrongly recognizing many of the samples of the other subjects as their own. The X-axis refers to the subjects in the study the Y-axis refers to the total number of wrongly recognized fingerprints of the other fingerprints

5.7. Study of 1 00 external samples

Another study included testing of 100 external samples with respect to the database. the system design allows co-operative users to be qualified as the authentic users Since theoretically the 100 external samples were not from the database, the probability of their resembling the database samples should be very small. the iterations were started from a value of zero threshold, to a maximum value for which all the samples were accepted the following graphs show the FAR and the FRR for the 100 external samples.

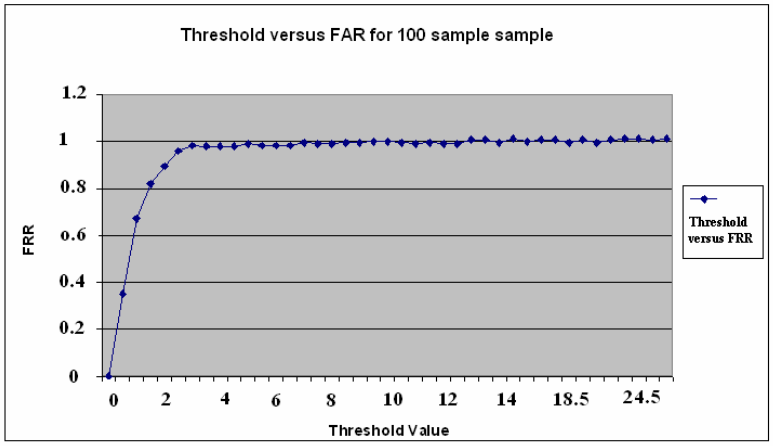

Figure16 :Threshold versus FAR for 100 sample

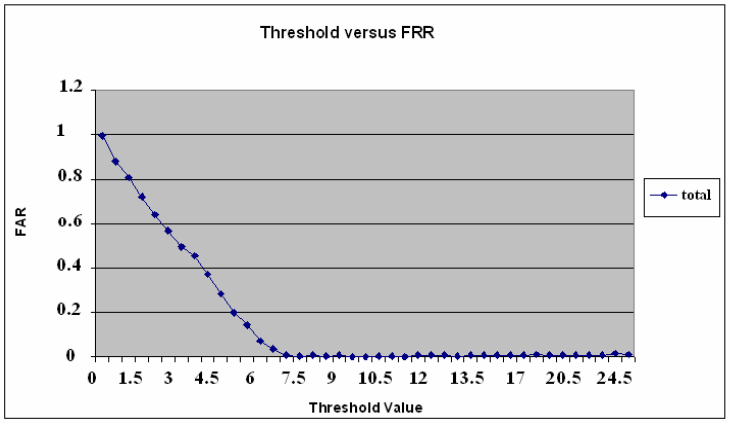

Figure 17 :Threshold versus FRR for 100 sample

As can be seen in the figures 16 and 17 the FAR and the FRR are complementary to each other With the increase in the threshold value the FAR decreases and the FRR increases. Figure18 shows the Equal Error Rate for the 100 external samples.

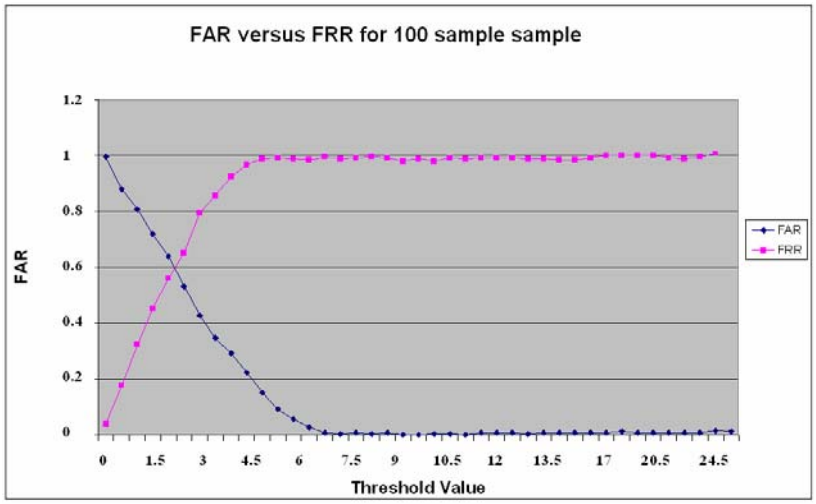

Figure 18 :Equal error rate for 100 external sample

As can be seen from the above for a threshold value of 2, the set-up allows the co- operative and hostile intruders equally to access the system.

6. Conclusions

the system successfully compressed and encrypted the data essential for Bluetooth Protocol communication. In order to evaluate the performance of the system for co-operative users and hostile

intruders experiments were carried out. Analysis of these experiments led to the study of the various constraints which were affecting the results.During the study, various possibilities of converting the unique biometric data into a feature vector were considered Based on various considerations a scheme was devised to compress the pixel data from a 260x300 (i.e. 78,000 pixels) . fingerprint image to 128 bits. From the analysis of the data obtained from the results, the following conclusions were drawn:

- For a threshold value of 1.05, the system had an equal error rate for FAR and FRR
- The fingerprints with greater no of extractable features have a better chance of being correctly recognized
- The fingerprints with lesser number of distinguished features have a higher rate of being recognized as a correct fingerprint.
- The uniqueness of the fingerprint i.e., non-identicality with other fingerprints may generate incorrect statistics.
- In cases where the data of one of the features, matches the data of another feature, of another fingerprint, it gets recognized as the other fingerprint.
- The inclusion of 1 00 external samples, representing hostile intruders, also did not affect the stability of the system .The system had an Equal Error Rate of 2 for external samples which was a low error rate as per a stable system.

Our suggested approach provides a unique approach where the Biometrics data is not appended into the Bluetooth payload Instead, it is utilized for pairing the Bluetooth devices and hence has the advantages over other systems where the data field is appended into the payload. For pairing between two devices a Bluetooth passkey or a PIN is entered into both the devices.

7. References

[1] Bluetooth SIG. Bluetooth Core Specification.

http://www.bluetooth.org/foundry/adopters/document/Core v2.0 EDR/en/1/Core v2.0 EDR.zip. [Accessed 8 September 2005].

[2] T. Muller. Bluetooth Security Achitecture.http://www.waterwood.com.cn/technology/bluetooth documents/SecuArch.pdf,1999.[Accessed 14 December 2007].

[3] Yaniv Shaked and Avishai Wool, Cracking the Bluetooth PIN, athttp://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/

[4] http://en.wikipedia.org/wiki/ Simple Password Exponential Key Exchange [Accessed 8 september 2007]

[5] http://en.wikipedia.org/wiki/Station-to-Station_protocol [Accessed 8 september 2007]

[6] Bellare, M.; Canetti, R.; Krawczyk, H. (1998), "A modular approach to the design and analysis of authentication and key exchange protocols", *Proceedings of the 30th Annual Symposium on the Theory of Computing*

[7] D. P. Jablon. Strong Password-Only Authenticated Key Exchange.http://www.jablon.org/jab96.pdf. [Accessed 6 Januari 2007].

[8] Bluetooth Pairing and Authentication Vulnerabilities , Protocol Design, Implementation, Dennis K. Nilsson, *Department of Computer Engineering,Chalmers University of Technology,* 2007

[9] Bluetooth Security Protocol Analysis, *The Faculty of the Department of Computer Science San Jose State University*, Chi Shing Lee ,May 2007

[10] Tom Karygiannis and Les Owens. “Wireless Network Security – 802.11,Bluetooth, and Handheld Devices”. *National Institute of Standards and Technology,Special Publication 8*00-48, Nov 2002.

[11] Levi, Cetinatas, Aydos, et al. “Relay Attacks on Bluetooth Authentication and Solution”. *Springer-Verlag Berlin Heidelberg*, 2004.

[12] Keijo M.J. Haataja. “Detailed descriptions of new proof-of-concept Bluetooth seuciryt analysis tools and new secrutiy attacks”. *Dept of Computer Science,University of Kuopio*, 2005.

[13] Jain, A.K.; Ross, A.; Pankanti, S.;- "Biometrics: a tool for information security. "- "Information Forensics and Security, *IEEE Transactions on" Volume 1, Issue 2, June 2006* Page(s):125 - 143

[14] Ani! KJain -"Biometric Recognition: How Do I Know Who You Are?"Signal Processing and Communications Applications Conference, 2004. *Proceedings of the IEEE 12th Publication Date:* 28-30 April 2004, page(s): 3- 5

[15] Biometric Technical Assessment http://bio-tech-inc.comIBio Tech Assessment.html

[16] Biometric Product Testing Final Report - National Physical Laboratory -http://www .cesg. gov. uk/ site/ast/biometrics/media/*Biometric TestReportpt* 1. pdf

[17] Patricia McDermott-Wells -"What is Bluetooth?" This paper appears in: "*Potentials,IEEE*", Date:Dec.2004-Jan.2005Volume:23,Issue:5page(s):33-35

[18] Yaniv Shaked and Avishai Wool-" Cracking the Bluetooth PIN" International Conference On Mobile Systems, Applications And Services Proceedings of the 3rd international conference on Mobile systems, applications, and services Seattle, Washington SESSION: Shake 'em, but don't crack 'em 2005 Pages: 39 – 50

[19] Biometric Product Testing Final Report - National Physical Laboratory - http://www.cesg. gov. ukl site/ast/biometrics/media/*Biometric TestReportpt* l.pdf

[20] Pauli Tikkanen, Seppo Puolitaival, Ilkka Kansala "Capabilities of Biometrics for Authentication in Wireless Devices" - Audio- and Video-Based Biometric Person Authentication" Volume 2688/2003 page 796-804.

[21] Li, H.; Mukesh Singhal-"A key establishment protocol for Bluetooth scatternets"Distributed Computing Systems Workshops, 2005. *25th IEEE International Conference on 6-10 June 200*5 Page(s):610 - 616

[22] T.CharIes Clancy, Negar Kiyavash and Dennis J.Lin, Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, Berkley, *California November* 2003 Page(s): 45 – 52

[23] Vivek Jain and Ramesh C. Joshi -"Integrating Bluetooth, Biometrics and Smartcards for Personal Identification and Verification" *Proceedings of National Symposium on Emerging Trends In Networking and Mobile Communication.*

[24] Hahnsang Kim; Dabbous, W.; Afifi, H.- " A bypassing security model for anonymous Bluetooth peers" Wireless Networks, *Communications and Mobile Computing, 2005 International Conference on* ,Volume 1, 13-16 June 2005 Page(s):310 - 315 voLl

[25] Adam Anthony -"An Investigation of Remote Authentication Schemes:The KeyScan Project"- http://www . wooster .edu/ cs/ seniors/2004/ adamAnthony .html

[26] Ray, M.; Meenen, P.; Adhami, R.;"A novel approach to fingerprint pore extraction" System Theory, 2005.SSST '05. *Proceedings of the Thirty-Seventh Southeastern Symposium on 20-22 March 2005* Page:282 - 286

[27] Poon, C.C.Y. Yuan- Ting Zhang Shu-Di Bao - Chinese Univ. of Hong Kong, Shatin, China: " *Communications Magazine, IEEE*" Date: April 2006 Volume: 44, Issue: 4 page(s): 73- 81