**Biometric Security Systems**

A COURSE PROJECT REPORT

By

# UMESH CHANDRA(RA2011003011224)

# ARLA VENU GOPAL(RA2011003011200)

# MELAM SIVA RAM(RA2011003011208)

# DHANUSH (RA2011003011215) PRANEETH(RA2011003011226)

Under the guidance of

## Mr.VINOTH N.A.S

*In partial fulfilment for the Course*

of

18CSE357T - BOMETRICS

in computer science



**FACULTY OF ENGINEERING AND TECHNOLOGY**

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**Kattankulathur, Chenpalpattu District**

NOVEMBER 2022

# SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

**(Under Section 3 of UGC Act, 1956)**

## BONAFIDE CERTIFICATE

Certified that this mini project report " **Biometric Security Systems**" is the bonafide work of

**Venu gopal(RA2011003011200)**

**Siva ram(RA2011003011208),**

### Dhanush(RA2011003011215),

### Umesh chandra(RA2011003011224),

**and**

**Praneeth(RA2011003011226)** who carried out the project work under my supervision.

**SIGNATURE**

**Mr.VINOTH N.A.S**

**Asst. proffessor**

SRM Institute of Science and Technology

### ACKNOWLEDGEMENT

We express our heartfelt thanks to our honorable **Vice Chancellor**

**Dr. C. MUTHAMIZHCHELVAN**, for being the beacon in all our endeavors.

We would like to express my warmth of gratitude to our **Registrar**

**Dr. S. Ponnusamy,** for his encouragement

We express our profound gratitude to our **Dean (College of Engineering and Technology) Dr. T. V.Gopal,** for bringing out novelty in all executions.

We would like to express my heartfelt thanks to Chairperson, School

of Computing **Dr. Revathi Venkataraman,** for imparting confidence to complete my course project.

We are highly thankful to our my Course project Faculty VINOTH N.A.S**, Ass. proffessor , Biometrics department,** for his/her assistance, timely suggestion and guidance throughout the duration of this course project.

We extend my gratitude to our **HoD Mrs. PUSHPALATHA,**

**,**

**HOD OF CSE DEPARTMENT** and my Departmental colleagues for their Support.

Finally, we thank our parents and friends near and dear ones who

directly and indirectly contributed to the successful completion of our project. Above all, I thank the almighty for showering his blessings on me to complete my Course project.

***Biometric Security Systems***

### Abstract

This paper describes the design of a Biometric Security System. At the beginning we introduce some biometrical attributes, especially the fingerprints, and we discuss their advantages and disadvantages when used in Biometric Security Systems. On example of the well understood fingerprint method we try to estimate the upper limit for the amount of available information on a fingerprint. Next part describes the architecture of such Biometric Se- curity System focused on fingerprint and speaker recognition. A qualified draft of the design is shown in this chapter. Finally the last chapter outlines the transformation of a biometric information key from fingerprint and the comparison of this key. Performance estimations of the whole system are introduced too.

**Keywords:** biometrics, fingerprint, voice, speech, verification, identification, PKI, key generation

#### 1 Introduction

Reliable person identification is necessary due to the growing importance of the information technology and the necessity of the protection and access restriction. The identification or verification might serve for a purpose of an access grant. Everyone successfully identified and accepted may acquire certain privileges. In the lawsuit, the identification is very important as the best evidence. However, these are not the only domains, in which the identification may be used. The range of the use is much wider. The person identification/verification is not the only part of the biometry. The biometry includes all systems that make the interface between a computer system and a human.

There are a lot of attributes that could be used for identification purposes. A number of such attributes hold as unique for each person. Of those attributes, probably the fingerprint was the first one to be examined in more systematic manner. Everyone’s finger forms of a unique pattern of different loops, spirals and curves of very high but still finite diversity. Fingerprint-recognition-based IT security has reached great importance as a mean of admitting information and services. Other attributes, which are unique for each human, include *face features*, *eye iris* and *retina features*, *palm* and *hand geometry*, *ear shape*, *DNA*, *odour* and *hand writing feature*. Some methods using these features are still under development, but they require new devices and technologies for detecting the deviations. The communication purposes include *speech recognition* , *speech generation*, *special input devices* and also *character recognition* (the OCR applications). These make it easier to operate a machine due to the natural way of the communication. The speech based methods are not common yet, but they are sup- posed to be very important as soon as the reliable identification methods will be developed. Advantages of the speech technology are an easiness of the sample acquisition (there has to be only a single microphone to get the needed data) and a willingness of the people to provide the system with a speech sample.

The biometric attributes could be divided into two classes. The first class includes *physical attributes* (finger- print, face, iris, retina, palm and hand, face thermogramm, etc.) and the second class includes *behavioural attrib- utes* (e.g. voice, signature, movement characteristics (walk, lips or hands movement, key press, etc.)). Some of them are shown in the Figure 1.

It has been quite a long time since the first Biometric Systems were introduced and until now they have not be- come widely used. Such a tendency is usual in case of all new, not well-tested and unverified principles and technologies, among which the Biometric Systems could be included. This holds true especially in case of the security systems. Though the popularity of the Biometric Systems is not at a high level yet, they are supposed to be very important in a short time. What could make them popular then? Why should they play a main role in the security systems?

1

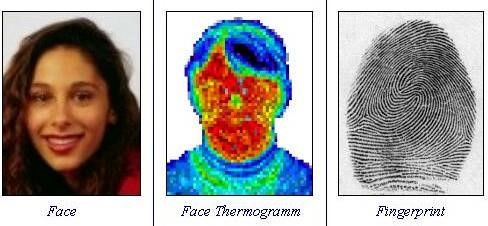
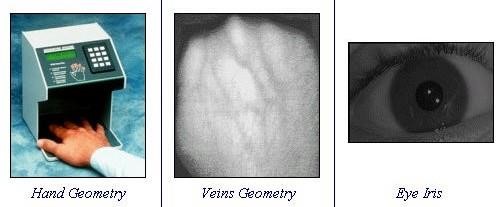
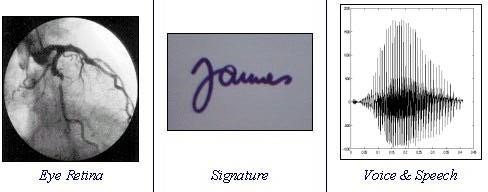


Figure 1: Some physical and behavioural biometrical attributes

#### 2 Design of Biometric Security System

First of all we would like to mention that this proposal does not describe an improvement of current biometrical systems, but should introduce more a new approach, using common biometrical technology, combined with cryptography. Most biometric identification systems are two-piece systems, which consist of a special sensor hardware and a processing hardware. The sensor is mostly connected to the processing hardware by discrete signal lines and the recognition and identification is performed on the processing hardware (usually a PC). These physical separation of components is hazardous for the security of the whole system and has its origin in the fact that the manufactures of biometric sensors and of computational hardware are often different companies. It is obvious that the integration of software into an intelligent hardware is the best solution (e.g. fingerprint sensor integrated on a smart card or in the USB-flash-disc). Another solution to this may be a usage of some crypto- graphic information calculated from the biometric attributes, combined with sequential enciphering of a private cryptographic key.

Fundamentally, the main goal is to encipher the private cryptographic key with all used biometric technologies. Each of the biometric technologies should generate limited amount of information vectors, which will be then considered as the biometric cryptographic keys. Then, a hash function should be calculated for each of these keys. This hash may be stored on storage (on a smart card, a USB token, a server, etc). An advantage of this will be that the storage will not contain any secret information, since the features of the biometric attributes will not be stored.

Every part of private cryptographic key will be encrypted with all biometric vectors generated during the en- cryption phase from the given biometric attribute (e.g. fingerprint, voiceprint). The whole information – i.e. hashes and encrypted values of the appropriate part of the cryptographic key – will be saved in the database. This database may be unlimited in access, because it does not contain any secret information. The encryption biometric key is stored during the procedure only in the volatile RAM.

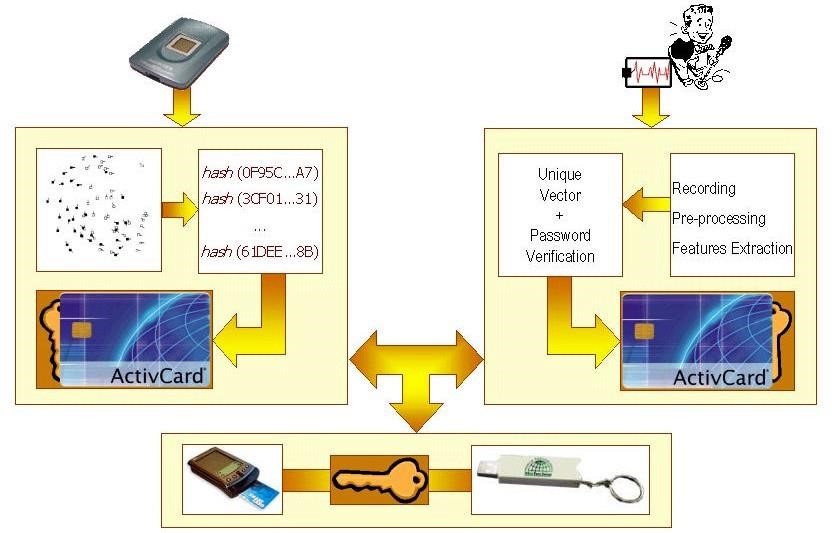


Figure 2: Biometric Security System – Architecture proposal

The comparison (verification) will be done via the hash values. When a user is about to log in, he/she claims his/her identity and then provides some biometric information to be authenticated. If only the verification is performed, then the usage of one biometric attribute is enough (i.e. fingerprint or voice). Out of this biometric attribute, certain set of features will be acquired. From this set, a subset of vectors will be generated, and this subset will be considered as the biometric cryptographic key. Finally, the hash function will be calculated from this vector. The result of this calculation will be compared to the stored hash values.

If a usage of the private cryptographic key is needed, the biometric attribute features will be acquired and the hash functions will be calculated upon these features. The hash value will be compared to the stored hash values. If a hash value matches, then the biometric vector, from which the hash value was calculated, is said to be the right vector to decipher corresponding round of the cryptographic key. Obviously, the next round must be deci- phered in the same way, just using another biometric technology. As soon as all rounds of the private crypto- graphic key are deciphered successfully, it is possible to use this key to encipher/decipher some data. In the end, this key must be deleted from a memory (RAM), as no private key is allowed to be saved anywhere. The pro- posed system architecture is shown in the Figure 3, where the fingerprint and voice technologies are used to ensure the security.

##### Advantages of the Biometric Security Systems

*Reliability and uniqueness:* The Biometric Security Systems are supposed to be very reliable. Reason for this is the relative very high uniqueness of some features used in the process of authentication in the Biometric Security System. These features are *physical attributes* and *behavioural attributes.*

*Security:* The Biometric Security Systems are very secure and the protected devices and services are only hardly to be misused due to the biometric protection. The biometric features can be acquired only from the authorised individual. E.g. it is only possible to get the fingerprint in case the authorised human is at the place of identifica- tion.

*Scalability:* The individual biometric systems may be connected together in a multilevel authentication system. This may include the standard login, voice login, fingerprint login etc. These stages of the login increase the security of the whole system. Should one of them fail or be cheated the others are able to negotiate the possibility of the break through.

##### Disadvantages and Limits

*Exactingness:* Some of the features are very exacting to acquire. These features may be very exact and unique but they are difficult to acquire (e.g. DNA analysis).

*Difficult implementation:* It is very complicated to implement very reliable Biometric Security System. Nowa- days teams of developers and researchers are working on the secure and reliable implementation of the Biometric Security System.

*Cooperation unwillingness:* Some humans are not happy with acquiring their biometric features. Results of the public inquiry being gone ahead recently shown that the most people dislike scanning their retinas. It is clear that it would be very useful to develop a reliable technology based upon the speech processing. The most of us are ready to let the machine analyse our voices rather than anything other.

*Inconstancy:* For example the human voice is not constant during the whole life. Let us emphasise the changes of the voice by the teenagers. But aside should not stay the influence of the illnesses or psychological condition of a human. This may be the greatest difficulty. Similar questions arise around the non-proved long life constancy of other attributes or the mathematical prove of their uniqueness.

*Fraud*: Some of biometrical attributes are quite simply illegal acquirable, e.g. fingerprint from glass or face im- age from some photo of the genuine user of the biometrical system. In the worst case the impostor can steal the whole biometrical information career (e.g. finger, eye, etc.). Such impostor could use this copied or stolen biometrical information career to defraud (attack) the biometrical system. In this case only the liveliness recog- nition could help, i.e. test whether the biometrical information career lives. The cooperation of genuine user with some impostor (under threat) cannot be precluded. This is a general problem for all biometrical systems.

Pros and cons discussed above are only the main of all, of which you can find out, but these should enable you to get the picture of the technologies of the Biometric Security Systems.

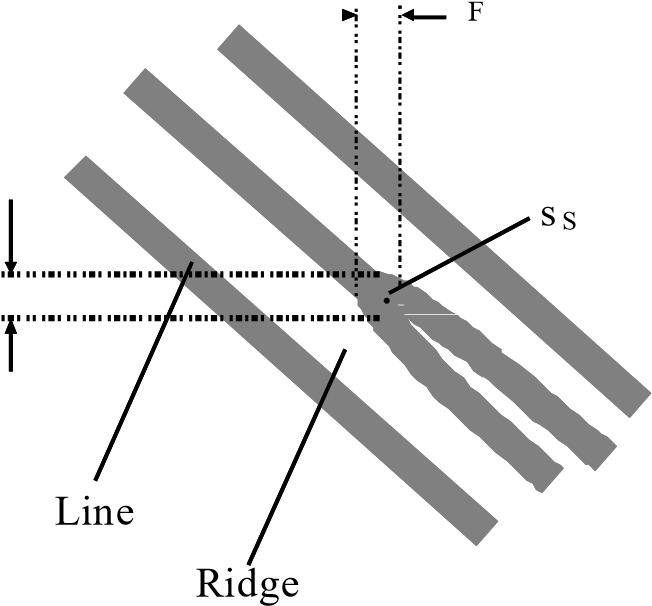
3

##### The Information Entropy of Biometric Attributes (Fingerprint as an Example)

Here we will introduce the general question, is there enough usable information hidden in a biometric pattern and are such information suitable for cryptographic purposes? First, it is a well established and straightaway fact that every random information can be used as a cryptographic key data as long as it is unpredictable and un- guessable (e.g. one time pad). As an example for a random information source we discuss the scan of a finger- print. The data acquisition of such fingerprint is an old traditional technique exploiting the visible structure of papillary lines and their discontinuity. In the common fingerprint systems usually the information about the po- sition of line ending or line bifurcation is converted into the *x*-*y* coordinates of so called minutia. Beside this, some additional information about the type of minutia and the corresponding line direction (gradient) is used to create an information vector consisting of digitized values.

For our rough estimation of an upper limit of available information on a fingerprint we start with the definition of a typical dimension of a minutia. We denote this size by *s F* (see Fig. 3).

**s**



s F

Figure 3: Bifurcation into two papillary lines in the corresponding biological resolution *s F* and the final reduc- tion to the resolution of the sensor *s S*

During the recognition procedure only such minutiae can be discover, if they are clear resolved from the “back- ground signal” (other papillary lines, ridges or other minutiae). With other words there must be at least a small area *F* surrounding the minutia *M* (see Fig. 4). We call the eight elementary cells *A* around the minutia *M* anti- minutiae and *A* gets for simplicity the same scale *s F* .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | A | A | A |  |
|  | A | M | A |  |
|  | A | A | A |  |
|  |  | M |  | M |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Figure 4: The definition of minutia *M* and the anti-minutiae area around *M*.

In our simple estimation we will define the biological dimension of a minutia as a square area of 0,33 *mm*  0,33 *mm* ( *s F* 0,33 *mm* ). We define the same scale also for anti-minutia. The space resolution of the fingerprint sen-

sor is of course much higher. The relation between the minimal resolvable scales *s F* and *s S* reads *s F* *s S* , where *s S* means the minimal resolvable scale with the sensor. The typical resolution of today’s sensors is

600 *dpi* which corresponds to *s S* = 0,043 *mm*.

4

In our model two close adjacent minutiae are separated by at least one anti-minutia *A* and their centers of gravity have a distance of approximately 2*s F* 0,66 *mm* (see Fig. 4). On a 1 *mm*2 square, which is a matrix of 3*s* 3*s* , maximal 4 minutiae can be placed without two minutiae

*F F*

touch each other. If we consider a rectangular fingerprint of the typical dimension of 10 *mm*  15 *mm,* which corresponds to a matrix 31*s F* 46*s F* , the maximal number of minutiae is 368. An example for a 5*s F* 7*s F*

matrix is given in the Fig. 5. A consideration whether a meaningful minutiae pattern is chosen here is not in the focus our discussion because we are interested just on the maximal density number of resolved minutiae.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| M |  | M |  | M |
|  |  |  |  |  |
| M |  | M |  | M |
|  |  |  |  |  |
| M |  | M |  | M |
|  |  |  |  |  |
| M |  | M |  | **M** |

Figure 5: Maximal density of minutiae on an array of a dimension 5*s F* 7*s F* . The next added minutia de- creases the total number of minutiae because the adjacent minutiae grow together

The final information about a minutia *mi* is reduced by the algorithm to a *x*-*y* coordinates (a point vector *ri* with the resolution of the sensor), the type *ti* of minutia (ending or bifurcation of a papillary line) and the direction *gi* of the corresponding line (gradient). We calculate the gradient in an array of 5*s F* 5*s F* which corresponds to the angular resolution of 22,5° and to the number of 16 values of gradients [1]. The only important information of minutiae position is their relative distance and the angle. This is given by the difference of point vectors. The Figure 6 shows an example for three minutiae.

***g***

***1***

***m***

***3***



***3***

***g***

***2***

***m***

***2***

***r***

***3***

***r***

***2***

***g***

***1***

***r***

***m***

***1***

Figure 6: The information which characterises the minutiae: vectors *ri* , the colours give the type of minutia

and *gi* is the gradient vector. The relative positions are given by the vector difference, e.g.: *r*2  *r*1 and *r*3  *r*1

The estimation of number of information from a set of *M* minutiae is now quite easy, from the two possible types of minutia we obtain a factor of 2*M*. The gradients contribute with the factor of 16*M-1*, because one of the gradients has per definition the trivial angle of 0°. The number of possible, non redundant, difference vectors in a raster of 230  350 points (this corresponds to the resolution of approx. 600 *dpi*) is 80.500. For the encoding of such number of relative vectors we need approx. 17 bits1 (80.500 217), for the minutia type we need one bit and for the gradient four bits.

1 Of course there is a small reduction of phase space for the number of vectors, because each additional minutia reduce the possible surface by an area between 4 *s* 2 and 9*s* 2 . In our estimation we are neglecting this fact.

*F F*

5

The common fingerprint systems are using a set of 12 minutiae (FBI standard). Our estimation yields in this case the following maximal number of available information:

217 121 212 16121 2214

This number we define as the ideal upper limit of available information. A string of 214 bits characterises unam- biguously the topology of 12 minutiae. Of course, such huge resolution (600 *dpi*) decreases dramatically the ability for the correct recognition during the matching phase. In order to achieve a higher process reliability and performance we introduced a new additional step into the standard recognition procedure which makes the algo- rithm more robust against the systematic effects[[1]](#footnote-1). The price for this is the reduction of the maximal available information to a number between approximately 2170 and 2125. Although this number is big, it is still negligible to an amount of data necessary for a generation of an asymmetric key. On the other hand this number is big enough for a use as a symmetric key and has a much higher information entropy as the usually used passwords or PINs.

#### 3 Fingerprint Recognition

We describe here the principle of fingerprint recognition, i.e. extracting the minutiae from the fingerprint. Fin- gerprints can be divided into few general classes. These classes are shown in Fig. 7.



Figure 7: Fingerprint classes: (upper row) *Arch*, *Tended Arch, Loop, Central Pocket Loop;* (lower row) *Double*

*Loop, Double Loop, Whorl, special Whorl (accidental)*

The whole process of fingerprint analysis (the classical method of minutiae comparison) consists of the follow- ing six steps – see Figure 8:

1. *Getting the input fingerprint image.* The quality of acquired image is important for the performance of automatic identification. It is desirable to use fingerprint scanner of high quality that is capable to toler- ate different skin types, finger injures and dryness or dampness of the finger surface.
2. *Performance of the algorithms for image quality improvement.* Image quality improvement is used to recover the real furrow & ridge structures from a damaged image. At first the histogram of fingerprint image is obtained, then the histogram equalisation is performed, the Gabor filters are used – they im- prove the clearness of ridge & furrow structures in recovered areas and so prepare image for minutiae extraction algorithm. Then the directional array is found in the image using filtering in frequency do- main (FFT  Ikonomopoulos filter  IFFT).
3. *Performance of the image pre-processing.* It is a preparatory step for minutiae extraction and classifica- tion. Thresholding by RAT scheme (*Regional Average Thresholding*) and thinning (*by Emyroglu*) is performed in this step.
4. *Fingerprint classification.* In this step the fingerprint is assigned to one of some defined classes. The classification is a difficult process for the machine as well as for the human, because for some finger- prints it is very complicated to unambiguously choose the particular class. At first the Karhunen-Loève transformation is applied on the directional array obtained from the step 2. Then the PNN classifier (*Probabilistic Neural Network* ) is applied, which assigns the fingerprint the class.

6

1. *Minutiae extraction.* Here we use the Emyroglu extractor, which extracts only three types of minutia from the fingerprint skeleton – *ridge ending*, *continuous line* and *bifurcation*. The gradient (papillary line direction) of this minutia is then computed.
2. *Verification.* It is the comparison of two minutiae sets. The efficiency of a minutiae comparison algo- rithms strongly depends on the reliability of minutiae obtaining process and external comparison proc- ess. For the minutiae comparison, we use the Ratha method that tolerates e.g. rotation and translation.

#### 4 Speaker Recognition

The speaker recognition part consists usually of four steps: a recording (4.1), a signal pre-processing (4.2), a feature extraction (4.3) and recognition (4.4).

##### Recording

The first step of the speaker recognition is the recording of the signal. This is usually done by a sound hardware which should be able to sample a sound with a sampling frequency at least of 11 *kHz* and a precision of 16 bits. A quality recording may affect the results of the recognition. In case of an insufficient hardware capabilities may be the recognition false.

##### Pre-processing

Next step in the speaker recognition process is the pre-processing of the input signal. It consists of some ele - mentary steps: pre-emphasis, framing, windowing and clipping of the non-speech frames, i.e. selecting of the speech frames.

*Pre-emphasis:* Is based on a very simple high-pass filter. This filter actually does not eliminate all the spectral parts below the cut-off frequency of the filter. It rather weakens the influence of the base voice frequency and strengthens the higher frequencies.

*Framing:* In this step a whole speech signal is divided into some shorter signal segments – frames. The length of the frames is usually about 10-20 *ms*. Sometimes, the frames may overlap each other, which shortens the step from the 10-20 *ms* to a smaller one (the precise length of the overlapping depends on the further processing).

*Windowing:* The frames acquired from the speech signal are multiplied by a rectangular window, which has a bad influence upon the spectrum of the signal. This is the reason, why each frame is multiplied by a nonrectan- gular window with a weaker influence upon the spectrum. Such a window may be a Hamming or Hann window.

*Clipping of the non-speech frames:* In this step the frames that are not usable for the further analysis are clipped out of the frame sequence. Usually only the first and the last speech frames are found and all the frames between them are supposed to be the speech frames. This usually works in case the utterance consists only of a single word. Otherwise this method fails. The clipping or the endpoint detection may be performed using a back- propagation neural network.

##### Feature extraction

The next step in the speaker recognition is the feature extraction. At this time, the proper frames have been ex- tracted from the signal and are ready to the further processing. A goal of this stage is to extract some typical features from them. There are a lot of various possibilities and it is not easy to choose the best of them. The most features base upon some parameters of the speech signal. These parameters may be e.g.: autocorrelation, energy, Zero Crossing Rate, Linear Prediction Coefficients, Mel-Frequency Spectral Coefficients, Mel-Frequency Cep- stral Coefficients.

These parameters are typical and well known in the filed of the (speech) signal processing. But they do not suf- fice for the speaker recognition. It is necessary to extract from the speech signal some other information that enable us to recognise the speaker reliably. Such features result from the typical above named parameters and it is not an easy task to choose the proper ones. The features must be unique and same every time a user would like to log in, i.e. after the analysis of the voice some features will be acquired and these must be same every time. But this is not easy to reach, especially in case of the speaker recognition.

7

##### Recognition

The recognition success (either a proper confirmation or a proper refusal) depends before all on the feature set chosen for this task. Then, even the worst recognition method would be able to perform the recognition properly. If a unique feature vector was extracted then the recognition process would transform to a simple comparison. But this scenario is not usual. The feature vector is not perfect, so that it is necessary to use some tools like the neural networks or hidden Markov models to recognise the speaker.

#### 5 Biometric Key Generation from the Fingerprint

As mentioned above, the encryption of a private cryptographic key is performed by symmetric keys obtained with different biometric technologies (e.g. fingerprint, voice). After the first encryption (e.g. symmetric key from fingerprint recognition), the resulted cipher can be newly enciphered with the next cryptographic key from an other biometric technology (e.g. voice recognition). Obviously it is possible to use several biometric technolo- gies simultaneously. This approach decreases significantly the risk coming from an unauthorised gathering of biometric information.

To have an example, a particular approach to fingerprint key generation is shown. At the beginning, the minutiae are extracted from the fingerprint (left part of Fig. 8). This minutiae extraction is done by a classical, well-known algorithm (see chapter 3). In the right part of Fig. 8, some transformations of the minutiae set are made, sche- matically explained by that figure. At first, the centre point of the fingerprint must be found, then the whole minutiae set is rotated and translated. Afterwards, the granularity (raster) of the fingerprint image is changed using certain special transformation. After these steps, certain minutiae set is available as an intermediate result, which can be named “an inaccurate set”. Then some subsets are selected from this “inaccurate set” and hashes are computed upon them. In fact, the input data of the hash functions forms the biometric cryptographic keys.

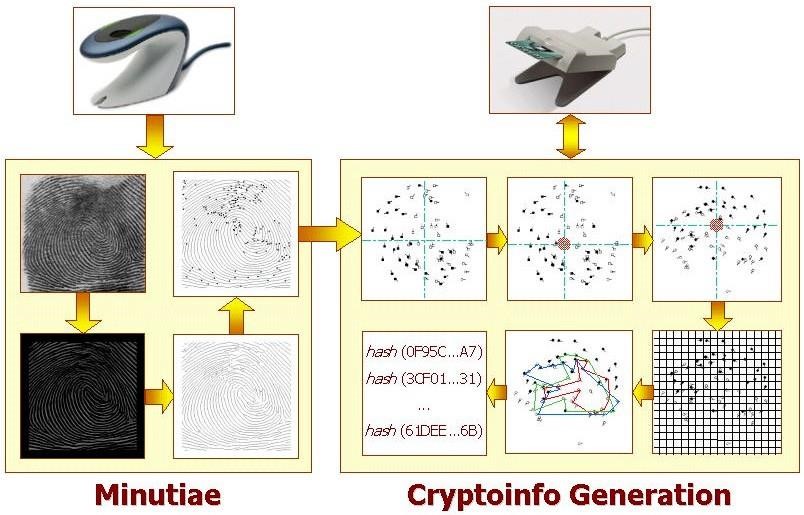


Figure 8: Generation of biometric cryptographic key

Figure 9 shows the comparison process. There are almost the same steps performed as in the generation phase, with a single exception of selecting only one minutiae set upon which the hash function is computed. This hash value is then compared with other hash values saved on the data carrier. If there is a match found, the temporary (in the CPU) corresponding biometric key can be used for the decryption of the private cryptographic key. Fi- nally, the (deciphered) private cryptographic key is now available in the RAM for the conventional crypto- graphic purposes. As soon as done, both keys are deleted from RAM.

8

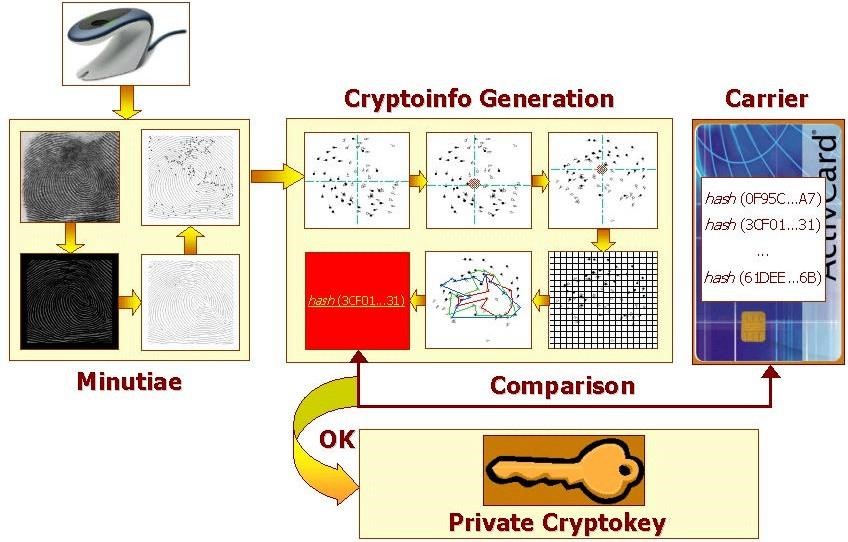


Figure 9: Decryption of private cryptographic key

##### Performance estimation

In this paper we present only the proposal of the biometric security system. This system is still under develop- ment, i.e. the performance of this system can be only estimated. Some parts are completed, i.e. some results are real.

In the following we give some typical numbers of processing time and storage place for the fingerprint recogni- tion. From the raw fingerprint an image quality improvement must be done. This pre-processing takes 1 second.

Minutiae extraction takes 0,35 second. The average size of fingerprint template is 650 bytes. This size doesn’t need to be optimised, because we use this template only for internal calculation and as an input for the next step. After that this template will be deleted.

During the registration a huge number of minutia subsets are calculated and results finally stored. This phase is very time consuming but it will be done only once. The typical number of found minutiae on one scan is around 50. From this set we extract 15 reliable minutiae which have to fulfil some quality requirements. Starting with 15 minutiae we create all possible subsets of 10 minutiae, it means 15possibilities, i.e. 3000 subsets. The selection

 

10 of one 10-minutiae-vector and the hash computation takes 0,1 second, i.e. the whole computation lasts 5 minutes. The approximate size of certificate with 3000 items is 400 *kB* (20 bits hash and 1024 bits enciphered crypto- graphic key).

The final performance of the system is not yet tested. The number of 15 reliable minutia is in the moment a compromise between the storage place, computational power and the acceptance and rejection rate and must be optimised. The limit of this proposal is of course given by a reasonable number of reliable minutiae. The number of possible subsets grows dramatically with the size of the minutiae set. For example when starting with 40 mi- nutiae about 847 million combination would have to be by calculated.

In the verification phase a significant smaller number of subsets have to be calculated. This depends on the fin- gerprint quality.

#### 6 Conclusions

Nowadays, a PIN code or a password is being used for the purposes of an authentication, which is the weakest point of the whole system. Biometry offers one reasonable solution. Biometry should be used instead of or addi- tional to the usage of passwords and PIN codes. A user will be authenticated by his/her biometric attributes and he/she will be either confirmed or refused. The confirmation or refusal depends on the acceptance of his/her biometric attributes. The biometrical key could play some role by replacement or improvement of traditional

9

PIN. Our biometrical key proposal could protect the system access on much higher level as PIN can do. Many people write their PIN on some paper or direct on smart card! Biometrical key or information cannot be written so easily somewhere and biometric can carry much more information entropy as PIN.

But the PIN and password replacement is not the only benefit of biometry. More might be got. Present biometric technology is not advanced enough to be used for the cryptographic purposes, because it is very difficult to de- tect and extract always the same or nearly the same features. The features are changing with growth and age. Hence some rough rasterization (granularity change; to avoid the position change of some feature) and subsets computation (to ensure the repeatability of some part of the features) is necessary.

Where to go on in the future? It is obvious that biometric systems will govern the security domain in future elec- tronic world. The identification speed and accuracy will be the crucial factors. Therefore, the algorithms may be optimised so that they can satisfy the strict conditions they will be exposed to during the regular service. The next possibility is to implement these algorithms under a smart card operation system and perform the fingerprint comparison directly on the smart card. It would increase the security and due to the impossibility of an attack of the communication among the computer, fingerprint scanner and smart card reader.

#### 7 Acknowledgements

The research has been done under support of FRVS project No. FR0835/2003/G1, GA CACR project No. 102/01/1485 and Research Intention No. CEZ: J22/98:262200012.

### References

1. Drahansky, M.: Fingerabdruckerkennung mittels neuronaler Netze, Diploma thesis, 2001
2. Smolik, L., Drahansky, M.: Exploitation of smart cards and human biometric attributes, CATE, 2001
3. Breitenstein, M.: Biometrische Authentifizierung – Übersicht und Evaluation verschiedener Gesichtserk- ennungssysteme, Technische Universität Clausthal, 2000
4. Emyroglu, Y.: Fingerprint Image Enhancement & Recognition; Yldyz Technical University, Turkey, 1997
5. Hong, L.: Automatic Personal Identification Using Fingerprints, Michigan State University, 1998
6. Ratha, N.K., Conell, J.H., Bolle, R.M.: Enhancing Security and Privacy in Biometrics-based Authentica- tion Systems, IBM Systems Journal, Vol. 40, No. 3, 2001
7. Jain, L.C., Halici, U., Hayashi, I., Lee, S.B., Tsutsui, S.: Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press LLC, 1999
8. Nanavati, S., Thieme, M., Nanavati, R.: Biometrics: Identity Verification in a Networked World, John Wiley & Sons, 2002
9. Innes, B.: Leichen sagen aus, Moewig-Verlag, 2003
10. Huang, X., Acero, A., Hon, HW.: Spoken Language Processing, New Jersey, USA, Prentice Hall, 2001
11. Gold, B., Morgan, N.: Speech and Audio Signal Processing, USA, John Wiley & sons, Inc., 2000

10

[View publication stats](https://www.researchgate.net/publication/312187756)

1. This will be discussed in one of our next papers.

   [↑](#footnote-ref-1)