Biometric Security Systems: Fingerprint and Speech Technology

research based, Ph.D. student paper,
the work should be presented by both authors

Filip Orság
orsag@fit.vutbr.cz

Martin Drahanský
drahan@fit.vutbr.cz

BUT, Faculty of Information Technology
Department of Intelligent Systems
Božetěchova 2
CZ – 612 66 Brno
Czech Republic

Abstract: This paper deals with the design of a biometric security system based upon the fingerprint and speech technology. In the first chapter there are the biometric security systems and a concept of an integration of the both technologies introduced. Then the fingerprint technology followed by the speech technology is shortly described. There are discussed some basic principles of each of the technologies.

Keywords: fingerprint, speaker, recognition, biometric, security

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. These attributes are unique for each person. Of those attributes, the fingerprint was the first one to be discovered and examined. Everyone's finger carries a unique pattern. This pattern consists of different loops, spirals and curves and is absolutely unique.

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 supposed 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* (fingerprint, face, iris, retina, palm and hand, face thermogramm, ETC.) and the second class includes *behavioural attributes* (e.g. voice, signature, movement characteristics (walk, lips or hands movement, key press, etc.)).

Design of Biometric Security System

Most biometric identification systems are two-piece systems, which consist of a special hardware and a processing hardware. The special hardware part consists of a sensor, which is connected to the processing hardware. The recognition and identification is performed on the processing hardware (usually a PC). These separate parts are hazardous for the security of the whole system. Figure 1 shows the danger of an attack. A solution to this may be a usage of some cryptographic information calculated from the biometric attributes, combined with a splitting of a private cryptographic key.

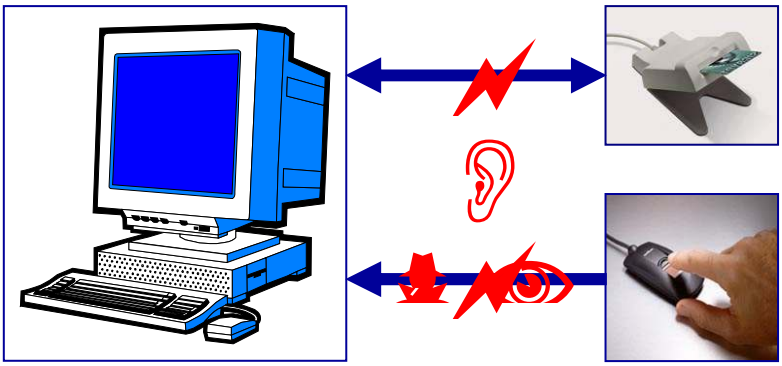

Fig. 1. Attack hazards to a biometric access control system

Fundamentally, the main goal is to split up the private cryptographic key among all used biometric technologies. Each of the biometric technologies should generate

limited amount of 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 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 – see the basic cryptographic rules (hash is one-way function, the encrypted information is indecipherable without having the key and the biometric keys used to the encryption are not stored).

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 the verification is performed only, then one biometric attribute is enough (i.e. fingerprint or voice). Upon 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 biometric cryptographic key. Finally, the hash function will be calculated upon this vector. The result of this calculation will be compared to the stored hash values.

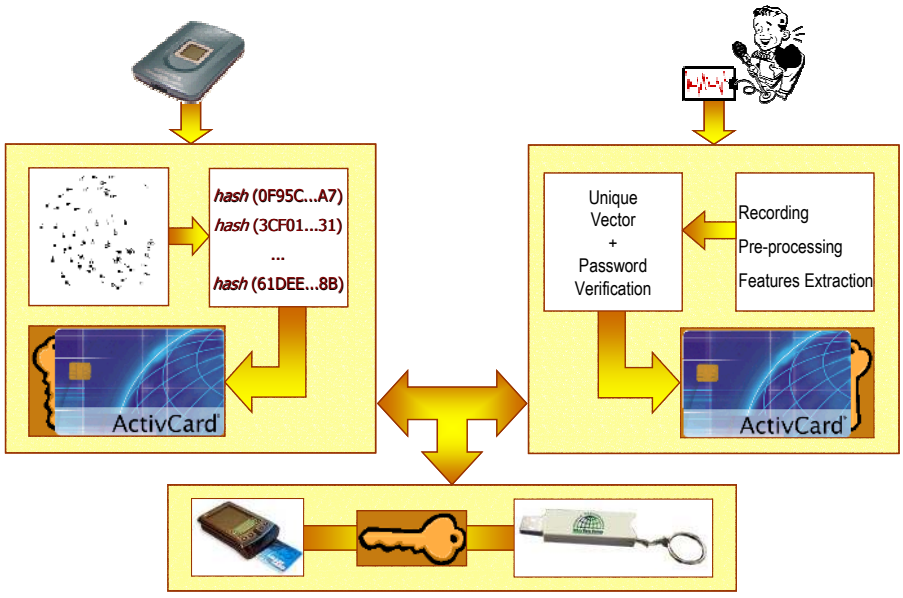

Fig. 2. Biometric security system – Architecture proposal

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 part of the whole cryptographic key. Obviously, the next part must be deciphered in the same way, just using another biometric technology. As soon as all parts of the private cryptographic key are deciphered successfully, it is possible to merge them into a single key and use this key to encipher/decipher some data. Then, this key must be deleted from a memory, as no private key is allowed to be saved anywhere. The proposed system architecture is shown in the Figure 2, where the fingerprint and voice technologies are used to ensure the security.

It is possible to use the entire private cryptographic key instead of its parts, but the distributed ownership (one part for each biometric attribute) is a better solution. Possibility of a cryptographic key misuse decreases with a growing number of the used biometric attributes. A great number of the biometric attributes may cause an impossibility of the entire private cryptographic key reconstruction. Reason for this is instability of the biometric attributes. One of them may change within a time, so that none of all stored subsets (biometric vectors) matches the stored hash values. It is clear that the biometric features are varying. To ensure the reproducibility of the features, more subsets will be selected from this set of biometric vector. The probability of finding the same subset next time is higher, then. Besides that, some rough raster will be used to minimize the variability. Unpleasant effect of this problem may be reduced slightly by an increase of a certificate revocation rate.

Fingerprint recognition

The first thing to describe is the principle of fingerprint recognition, i.e. extracting the minutiae from the fingerprint. It should be said that all fingerprints could be divided into 5 classes. These classes are shown in Figure 3.

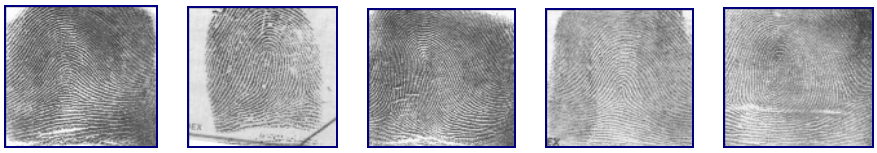

Fig. 3. Fingerprint classes: Arch, Left Loop, Right Loop, Tended Arch, Whorl

The whole process of fingerprint analysis (the method of minutiae comparison) consists of the following six steps – see Figure 3:

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 tolerate 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 equalization is performed, the Gabor filters are used – they improve 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 domain (FFT → Ikonomopoulos filter → IFFT).

3. *Performance of the image preprocessing.* It is a preparatory step for minutiae extraction and classification. 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 five classes. The classification is a difficult process for the machine as well as for the human, because for some fingerprints 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 into one of five classes.
5. *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*. In this step some improvements have been done. When the detection and extraction phase is finished, the minutiae are tested once more. If they lie on the edge of the fingerprint, they are deleted. The second test checks the papillary line continuity (partially done in step 3) – difference between line ending and bifurcation. And the last improvement includes more accurate scale for gradient of the minutia. Now it is possible to detect the degree of the bias of the papillary line more accurately and compute the gradient of this minutia.
6. *Verification.* It is the comparison of two minutiae sets. The efficiency of the minutiae comparison algorithms strongly depends on the reliability of minutiae obtaining process and external comparison process. For the minutiae comparison, we use the Ratha method that tolerates e.g. rotation, translation and other changes in the fingerprint.

Speaker recognition

The speaker recognition part consists usually of four steps: a recording, a signal pre-processing, a feature extraction and recognition.

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.

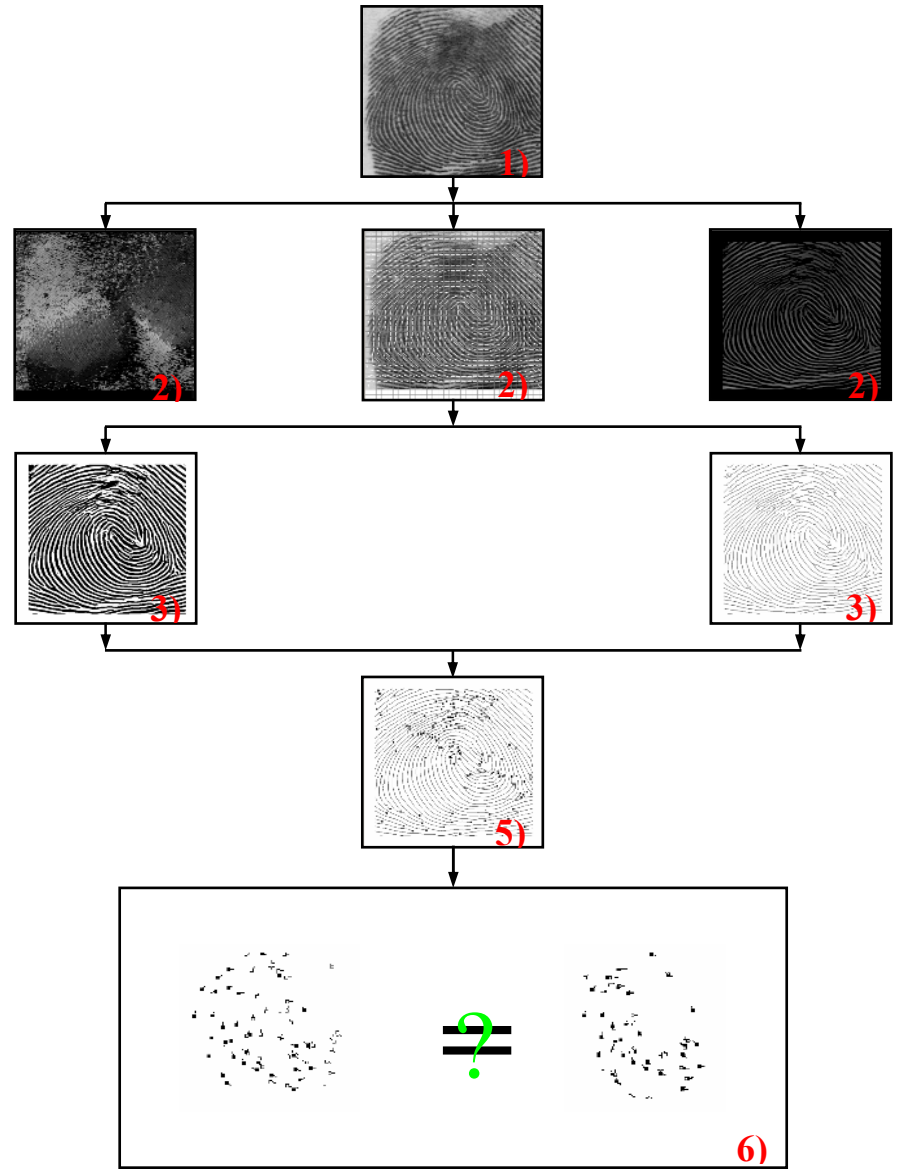

Fig. 4. Example of fingerprint analysis process (without classification)

Pre-processing

Next step in the speaker recognition process is the pre-processing of the input signal. It consists of some elementary steps 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 nonrectangular 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 extracted 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 (ZCR), Linear Prediction Coefficients (LPCs), Mel-Frequency Spectral Coefficients (MFSCs), Mel-Frequency Cesptral Coefficients (MFCCs), see [8], [9].

These parameters are typical and well known in the filed of the (speech) signal processing. But they do not suffice for the speaker recognition. It is necessary to extract form 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.

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 were 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.

Conclusion

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 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.

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 detect and extract always the same or nearly the same features. The features are changing with growth and age. Hence some rough rasterization (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 electronic world. The identification speed and accuracy will be the crucial factors. Therefore, the algorithms may be optimized 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 at 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.

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 Gesichtserkennungssysteme, 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] Jain, L.C., Halici, U., Hayashi, I., Lee, S.B., Tsutsui, S.: Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press LLC, 1999
[7] Nanavati, S., Thieme, M., Nanavati, R.: Biometrics: Identity Verification in a Networked World, John Wiley & Sons, 2002
[8] Huang, X., Acero, A., Hon, HW.: Spoken Language Processing, New Jersey, USA, Prentice Hall, 2001, ISBN 0-13-022616-5
[9] Gold, B., Morgan, N.: Speech and Audio Signal Processing, New York, USA, John Wiley & sons, inc., 2000, ISBN 0-471-35154-7