Stručni članak

Biometrics Identification Process: A Multimodal Approach

Željka Požgaj
Faculty of Economics and Business
Trg. J. F. Kennedy-a 6, Zagreb, Croatia
zpozgaj@efzg.hr

Marko Miloš
Baruna Trenka 16, Zagreb, Croaita
xyzmarmi@yahoo.com

Summary

Rapid progress of biometric technology and its expanded application brings new possibilities in identification process. First biometric identification systems were organized as unimodal systems. It means that process of identification was based on single unique individuals' physical or behavioral traits. Although most biometric systems deployed in real-world applications are still unimodal, multimodal biometric systems represent an emerging trend that attempts to increase the level of security by using more than one biometric trait for identification or authentication.

The paper presents basic characteristics of biometric identification process, discusses various scenarios that are possible in multimodal biometric systems, and analyzes the levels of fusions in biometric systems, modes of operation, security requirements.

Key words: biometrics, identification process, multimodal biometric system

Introduction

The word *biometrics*, an acronym of Greek origin can be literally translated as “the measure of life” (Chirillo et al. 2003). It refers to identification techniques that rely on individuals' measurable physiological (anthropological) or behavioral traits that can be automatically checked. Physiological biometric traits are: fingerprint, hand and finger geometry, vessel pattern, iris and retina pattern, face geometry, facial pattern etc., while behavioral traits reflect individuals’ behavior regarding performing of certain actions. They are: gait, keystroke, signature, voice etc.

The implementation of biometric traits in identification process reaches as far as the 2nd century BC The Chinese recognized that every person has their own, unique bodily traits and started to use fingerprints in signing important documents (Požgaj, 2002.). As a form of identification, biometric traits have been applied up till today. The development of information and Internet technologies in the past two decades has had a great impact on the development and implementation of biometric identification systems. The development of information technologies has influenced the development of specific hardware and software especially adapted to biometric needs, the identification process itself by enabling digitalization of biometric sample, automation of sample comparison and with it the duration of the identification process (by shortening it). The Internet and its technologies are the basis of digital economy. There are new ways of running business (e-business), new ways of making business transactions (e-transactions), new ways of performing everyday activities. New forms of communication are being developed, awareness of value of certain resources like information is rising. Along with the positive changes brought by the new technologies, there are also some negative side effects. The security issue becomes ever more significant in business field as well as in other spheres of everyday life. New forms of protection are being explored that will provide additional security measures in comparison with the existing models. In that context multimodal biometric identification systems are being developed. The first multimodal systems appeared in 1998 (Bearman, 2006), but their full implementation is yet to follow.

From the point of view of security, multimodal systems represent a form of improvement for the identification process in a unimodal system. Unimodal systems are based on a single biometric (physiological or behavioral) trait used in identification and verification process, whereas in multimodal systems more biometric traits participate in an identification process. To be able to speak about specific qualities of multimodal systems it is necessary to become familiar with the qualities of unimodal systems since they represent a genetic pattern of biometric identification systems.

It is an undeniable fact that biometric identification is becoming a generally accepted form of identification. Issues most often arising from implementation of biometric identification systems refer to the choice of biometric system (unimodal or multimodal), choice of biometric trait (or traits) an identification system would be based on, implementation simplicity, implementation costs, system reliability, etc. However, the choice of a particular biometric technology for implementation largely depends on the type of application and the level of security required. This paper concentrates, as the title itself suggests, on multimodal approach to biometric identification process.

Following the introduction, the second chapter discusses basic characteristics of biometric identification/verification process connected to specific qualities of unimodal and multimodal systems. The third chapter deals with specific qualities of multimodal systems. The discussed qualities refer to scenarios of sample creation, operation modes, types of data fusion as well as certain difficulties in an identification process. Implementation of biometric identification systems is dealt with in the fourth chapter. The fifth chapter is the conclusion.

Basic characteristics of biometric identification/verification process

Basic identification/verification model includes two processes: enrolment and verification (authentication) (Požgaj et al. 2007.).

Enrolment process covers the following steps:

- Taking the initial (identifying) sample
- Transforming the sample to template
- Storing the template (into a database or on a smart card).

In taking the first sample, the person is identified through classical method of identification (identity card) in order to confirm their identity. A biometric trait (initial sample) is taken according to selected methods and characteristics of the identification equipment, transformed to a digital template and stored in a database, on a local reading device or on a smart card.

Verification process can be repeated in every further attempt of identification. It covers:

- Identification process (taking a new biometric sample)
- Verification of the taken and stored template
- Approval or rejection for further actions.

Next time when someone wants to identify themselves they have to pass the identifying process again. The goal of verification is to confirm authentication. Process of verification is successfully completed if the template of the newly scanned part of a person's body corresponds with the stored template. Depending on the result of verification, further activities are either granted or denied.

The described model points at the generic activities typical for the biometric identification system. What separates unimodal from multimodal systems is the way in which the activities are performed. Differences in number of biometric traits from which an initial sample is created are obvious as early as the enrolment process (in unimodal systems one trait is present, in multimodal two or more). The procedure of creating a template itself also differs. In unimodal systems template is created via simple transformation of sample to template, whereas in multimodal systems a template is created following one of the possible scenarios typical of multimodal systems. The matching procedure is identical in both systems. The comparison process is based on sequential searching of the biometric sample database (1: n matching) or on comparison of the initial sample stored on a mobile carrier like smart card and the newly created one (1:1 matching). Verification is a process of confirming the authentication of the person being identified. It is successful if the comparison shows that the newly created sample and the stored sample match (1:1 matching).

Specific qualities of multimodal identification systems

The identification process in multimodal systems depends on multimodality. Since it is a system where identification is based on more than one biometric trait, there are certain scenarios for the final sample creation, fusion, results of matching and reaching a decision.

Possible scenarios for sample creation

As it was said earlier, identifying template in a multimodal system is formaed based on two or more single samples. The way in which a biometric sample is created is determined based on the chosen biometric technology. Regardless of the scenario according to which the data are collected in order to create a sample, the same scenario has to be applied when creating an initial template and the template created whenever identification is attempted. There are four possible scenarios (Ross et al., 2007):

- Single biometric trait, multiple sensors
- Single biometric trait, multiple classifiers
- Single biometric trait, multiple units
- Multiple biometric traits

The Single biometric trait, multiple sensor scenario means that the identification data are collected by scanning a single biometric trait with multiple sensors. A template is created by compressing the collected data. If the chosen biometric trait is hand, it is possible to create a template based on data collected by scanning hand geometry and data collected by scanning blood vessels of the hand (palmprint).

The Single biometric trait, multiple classifiers scenario means that the rough data of a single biometric trait are collected during single scanning. The data are then processed with multiple algorythms. If the biometric trait in question is a fingerprint, the desired template is created by applying minutiae-based and texture-based algorythms.

The Single biometric trait, multiple units scenario means that the biometric sample is created based on more than one biometric unit of the chosen biometric trait. If identification is based on a fingerprint, the final template can comprise fingerprints of more fingers (of all ten of them, of index and ring finger, of five fingers on the left hand, etc.).

The Multiple biometric traits scenario means that the final biometric template comprises of two or more samples of various biometric traits (fingerprint and face traits, fingerprint, face and voice traits, etc.).

Modes of operation

Besides the template creation process itself, in multimodal systems time sequence in which a person is identified is also significant. There are two types of procedures: synchronous and asynchronous. In a synchronous procedure a person is identified simultaneously. Fingerprinting is carried out at the moment of identification by using more than one sensor. It is possible to scan a fingerprint when scanning hand geometry. When an asynchronous procedure is applied, a person is identified sequentially using two or more devices. A person can be identified upon entering the working premises by palmprint and voice trait. It is also possible to combine both synchronous and asynchronous procedures in an identification process.

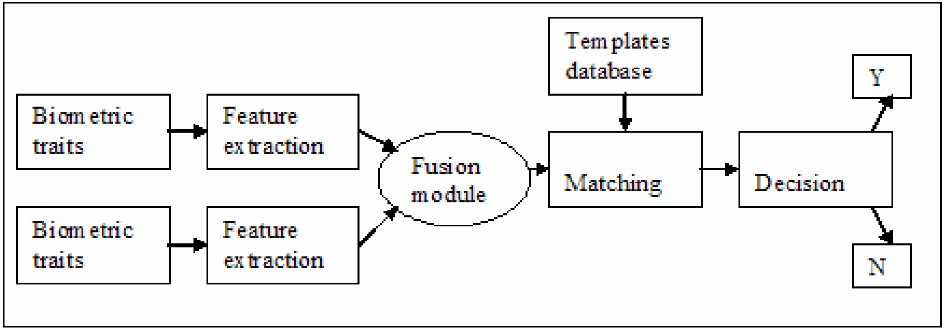
Multimodal system can operate in one of three different modes: serial mode, parallel mode or hierarchical mode (Ross et al., 2006.). In a serial mode the processing of biometric information takes place sequentially. If an identification system involves two biometric traits, a person is first identified based on the first trait (e.g. a fingerprint). In case the identity of a person is authenticated by processing the data collected according to the first trait, further identification is not necessary. If the identity is not authenticated, a person is identified using the following trait (e.g. face geometry). In this way time necessary for identification is reduced, which is extremely important when you have a situation where identification of a great number of users in the shortest time possible is required (for example upon coming to work). If a biometric system functions in a parallel mode, each ID subsystem processes its data independently at the same time and the processed data is combined using an appropriate fusion scheme. Most multimodal systems operate in a parallel mode as their primary goal is to reduce error rates of a biometric system despite reducing the recognition time. If an identification system operates in a hierarchical mode (tree-like architecture) it combines the advantages of both serial and parallel mode. Ross points out the cascade mode. It operates in serial mode but in such a way that the matching process based on the first biometric trait produces the top n matches whereas the second trait determines the identity of the user based on the n retrieved matches. It is possible to choose the order of biometric traits in which identification is carried out.

Data fusion

In multimodal systems data fusion occurs. Fusion can take place prior to or after the matching (Jain et. al., 2007.). Prior to matching fusion can occur either at sensor or feature level.

At sensor level, fusion is carried out at the rough data level. The data refer to the same biometric trait and are collected through one sensor or more compatible sensors. At feature level, fusion is preceded by creation of two (or more) independent feature templates (biometric vectors in Jain et al.). Fusion creates a single new template (vector). It represents a person's identity. Next follows the matching procedure in which a single new template is compared with templates stored in the database. The final decision depends on the results of matching.

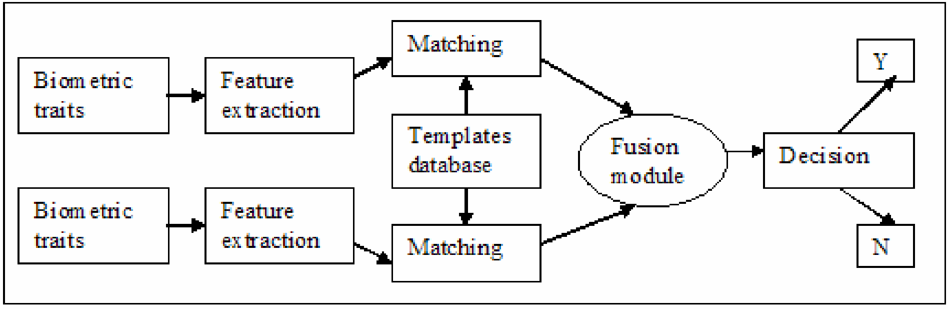
Figure 1.: Fusion at the feature extraction level



Source: Jain K. Anil, Ross Arun, Prabhakar Salil: An Introduction to Biometric Recognition. Modified by authors.

After the matching level, fusion can occur at match score level or decision level. During fusion at match score level (Fig. 2), for each biometric trait features are extracted and an input feature template is created. Matching is carried out in a way that every input feature template is compared with templates from the database. Matching scores are combined using the weighed averaging technique in order to authenticate the veracity of the claimed identity. According to the results a final decision is made.

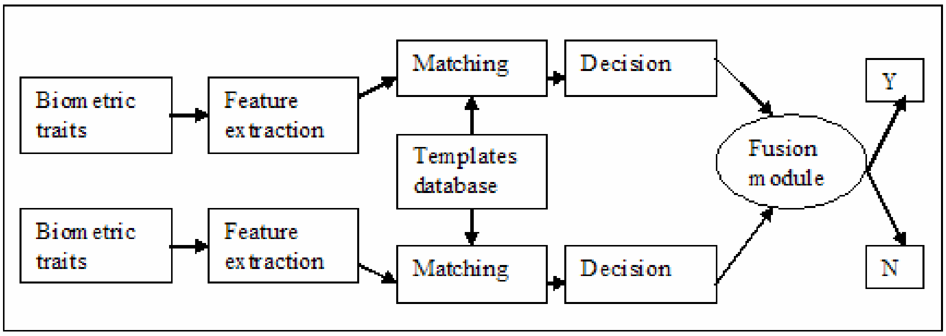
Figure 2.: Fusion at the matching score level



Source: Jain K. Anil, Ross Arun, Prabhakar Salil: An Introduction to Biometric Recognition. Modified by authors.

During fusion at decision level (Fig. 3), each segment of a multimodal system carries out its own identification process during which an input feature template is created and then compared with the templates from the database resulting in a recognition decision. At the end of the procedure single recognition decisions are combined and the identity of the person in question is either authenticated or not.

Figure 3.: Fusion at the decision level



Source: Jain K. Anil, Ross Arun, Prabhakar Salil: An Introduction to Biometric Recognition. Modified by authors.

Difficulties in identification process

Each identification system has certain limitations. In biometric systems these limitations most often refer to (Jain et.al., 2007), (Ross et al., 2006):

- Noise in sensed data
- Intra-class variation
- Inter-class similarities
- Non-universality
- Spoof attack

Noise in sensed data occurs when, for certain reasons, the chosen biometric trait cannot be used in identification. The reasons can be a dirty finger, husky voice, injured hand, but also the dirt on or damage of the sensors.

Intra-class variation and inter-class similarities are possible when the set rules of behavior are not followed in providing an identifying sample (position of finger, hand or face in regard with the sensor i.e. camera). Because of the finger movement or facial mimic it can happen that the created template does not match the real biometric traits of a person that is being identified. This can lead to false results of the verification process and the access can be enabled to an unauthorized person or denied to an authorized person.

Although it is stated that biometric identification methods are universal for everyone, non-universality occurs when certain people due to some physical handicap, illness, etc. cannot be identified through certain biometric traits. According to (Jain et al., 2007.) 4 per cent of the population may have poor quality fingerprint ridges and cannot be identified based on their fingerprints.

Spoof attack is present in all identification systems. In a biometric system the attacker tries to penetrate the system by imitating or forging biometric traits of the person he is posing as.

The described problems (except spoof attack which is possible in all systems) are especially noticeable in unimodal identification systems. The implementation of multimodal systems helps avoid or diminish these problems. So if a person cannot be identified through a certain biometric trait (noise in sensed data or non-universality), other traits in the system can be used for identification (cascade mode identification).The same applies to the case when one of the collected samples cannot be used for comparison (intra-class variation and inter-class similarities). Each spoof attack based on imitation or forging of biometric sample has less chance of success in multimodal systems than in unimodal systems because the identification process is more complex and the system is more reliable.

Reliability is a very important issue in multimodal systems. There are three different metrics to rate accuracy of biometric technology and they are manifested as (Bearman, 2006.), (Požgaj et al., 2003):

- False match (imposter breaks in),
- False non-match (correct user locked out),
- Failure to enrol (user cannot register in system).

False Match Rate (FMR) or rate of false acceptance (FAR) represents the probability that particular user’s verification template will be incorrectly judged to be a match for a different user’s enrolment template. False Non-Match Rate (FNMR) or false rejection rate (FRR) represents the probability that a user’s verification template will be incorrectly judged not to match that same user’s enrolment template. Failure to Enrol (FTE) Rate represents the probability that a particular user will be unable to enrol in a biometric system due to insufficiently distinctive biometric sample(s).

These three metrics are strongly related. If FMR decreases or makes system less suitable to importers, legitimate users will be rejected (FNMR) and vice versa. The values of FMR or FAR and FNMR or FRR can form curves whose intersect is called Equal Error Rate (EER) or the crossover accuracy of the system. This is the rate at which the FAR is equal to the FRR. In general, the greater value of the crossover accuracy, the greater inherent accuracy of the biometric. According to the Biometric Consulting Group investigation the greater crossover accuracy is present in retinal scanning (1:10,000,000+), then iris scanning (1:131,000), fingerprints and hand geometry (1:500), signature and voice dynamics (1:50) (Požgaj, 2002.).

The reliability issue in multimodal systems is very complex and although in the end it is expressed with FTE, FAR and FRR, the reliability of the system is influenced by user’s behaviour during identification process but also the traits of biometric technology represented through number of biometric traits used in identification, scenario of data collection, fusion and the decision-making process.

Implementation of biometric systems

The advent of biometric systems has meant a great leap forward from the point of view of security issues compared to physical (key, plastic card) and logical forms of identification (password, PIN). Every day biometric systems are becoming more and more present. On a global level, a clear indicator that biometric technologies industry is becoming a respectable branch of information technologies industry are the predicted annual revenues for 2007 and 2010 stated in Annual Biometric Industry Revenues published by International Biometric Group. The predicted revenue for 2007 comes to around $3010.7 million and in 2010 it could go up to around $5749.2 million (Annual Biometric Industry Revenues, 2006).

There are three areas of implementation for biometric technologies (Jain et al., 2007.):

- Commercial applications
- Government applications
- Forensic applications

Forensic applications deal with a rather specific area of biometric identification and will not be discussed here.

In commercial applications mostly unimodal identification systems are used today. Reasons for that lie in a wide offer of unimodal identification devices based on various biometric traits, acceptable implementation costs, simplicity of use, users' good response to them … The main areas of implementation are:

- Physical access control which could ensure entrance to locations previously intended only for authorized persons (company premises, hotel rooms, schools, kindergartens, prisons …)
- Money transactions where identity control is needed (ATM, credit card payment …)
- Restriction in business activities where identity control is needed (access to particular business resources, access to confidential data …)
- Particular activities that become more secure if biometric identification is implemented (network transactions, logging on to computer, logging on to mobile …).

Comparing unimodal and multimodal systems one can come to conclusion that in multimodal systems the biometric identification technology is more expensive, the procedure of system implementation more complex, implementation forms more demanding, standardization and interoperability problems more clearly noticeable. Because of that, it is necessary to perform a detailed needs analysis when choosing a biometric technology and set certain priorities.

The basic criterion in government applications is increased security. That is why multimodal identification systems are recommended (and worldwide used) when it comes to applications that refer to national ID card, passport control, driver's licence, social security etc.

In Croatia, according to the information of the author, multimodal systems are still not used, but unimodal systems are ever more present. Unimodal systems are mostly used in physical access control with fingerprint as an identification trait.

Conclusion

The aim of this paper was to introduce biometric identification in general and multimodal approach in particular. Since the multimodal approach is in a way an upgrade to the unimodal approach, the paper is mostly based on comparison of the two. Specific qualities of the multimodal approach are represented via ways of collecting biometric samples and forming templates, modes of operation, fusion of relevant data within sensor module, feature module, matching module or decision module. By implementing multimodal systems it is possible to overcome the limitations of unimodal systems that in a way lessen the advantages of biometric identification systems. Multimodal systems are for now mainly used in government applications although it is to be expected that multimodal systems will find its way to commercial applications as well. Reasons for that are many and can be seen primarily in the need of higher security measures when performing business and everyday activities.

References

Bearman Nathan: Multimodal biometrics, http://www.securitysa.com (20.11.2006.)

Annual Biometric Industry Revenues, Biometric statistics in focus, http://www.sciencedirect.com (10.12.2006.)

Chirillo John, Scott Blaul: Implementing Biometric Security, Indianopilis, Willey, 2003.

Jain K. Anil, Ross Arun, Prabhakar Salil: An Introduction to Biometric Recognition, http://www.citer.wvu.edu (20.6.2007.).

Požgaj, Ž.: Biometrics and New Technology, Proceedings of 1st International Conference “An Enterprise Odyssey: Economics and Business in the New Millennium”, Graduate School of Economics & Business, Zagreb, June 27-29, 2002, 975-987

Požgaj Željka, Mateljan Vladimir: Some Sugestion about Biometrics' Technology Selection, Proceedings of the14th International Conference on Information and Intelligent System IIS 2003, Varaždin, September 24-26, 2003. 313-323

Požgaj Željka, Đuretek Ivor: Smart Card in Biometric Authentication, Proceedings of the18th International Conference on Information and Intelligent System IIS 2007, Varaždin, September 12-14, 2007. 319-325

Ross A. Arun, Nandakumar Karthik, Jain K. Anil: Handbook of Multibiometrics, NewYork, Springer, 2006

Ross Arun, Jain K. Anil: Multimodal biometrics: An overview, http://biometrics.cse.msu.edu (20.6.2007)