

*Proceedings International Conference on the
Biometrics: Fraud Prevention, Enhanced Service, Las
Vegas, Nevada, USA, 1997, pp. 270-286*

IMAGE ANALYSIS AND PATTERN RECOGNITION IN BIOMETRIC TECHNOLOGIES

**J. Soldek¹⁾, V. Shmerko¹⁾, Phil Phillips²⁾, G. Kukharev¹⁾,
W. Rogers³⁾, and S. Yanushkevich¹⁾**

¹⁾ Institute of Computer Science & Information Systems, Technical University of Szczecin
Zolnierska St. 49, Szczecin 71210, Poland, Fax: (**4891)4876439, Email: shmerko@dedal.man.szczecin.pl,
szmerko.ii.dyda@beta.ii.tuniv.szczecin.pl

²⁾ IEE C3 Committee, Netherlaw 1, North Berwick, United Kingdom, Fax: (**44) 017-1250-1290, Email:
phil4CCML@aol.com

³⁾ Biometric Digest, St. Louis, Missouri, P.O. Box 510047, MO 63151-0047, USA
Tel: (**314)892-8632, Fax: (**314)487-5198, Email: wrogers@anet-stl.com,
WWW: <http://www.anet-stl.com/~wrogers>, <http://www.anet-stl.com/~wrogers/biomtrics/biodigest.ht>

Abstract. *Many biometric methods are closely connected with methods of pattern recognition and image analysis. The realization of a number of biometric technologies requires using the last achievements in this area. Some elements of technology based on some methods of image analysis are demonstrated by the example of iris person identification. From a position of organizing the educational process, laboratory works in the area of biometric technologies allow stimulating students' inquisitiveness in studying methods and algorithms for image processing and pattern recognition.*

Key words: *biometric technologies, biometric authentication, image processing, education*

1. Introduction

Biometric and biomedical informatics are the fast developing scientific direction, studying the processes of creation, transmission, reception, storage, processing, displaying and interpretation of information in all the channels of functional and signal systems of living objects which are known to biological and medical science and practice. Modern natural sciences at present sharply need in the updating of scientific picture of the world, and the essential contribution in this process can be made by the biometric and biomedical methods.

Only some more simple (statistical) forms of biometric and biomedical information have found their application when person identification, and raised interest for these methods of identification can be caused by new possibilities of information technologies.

So, exclusively new and not explored possibilities for verification of living objects can be expected in eniology. A concept of electromagnetic is intensively investigated at present. New results have been obtained in fractal analysis, using which an attempt was taken to explain some paradoxical phenomena such as morphogenetic field, distant cells communications, anomalously high sensitivity of organism to near-zero frequency perturbations, regulation processes critical dependence on the fractal features of noisy environment, etc. [Polo]. Perhaps,

each of these phenomena can be applied in future to identify a person, and these methods may replace instead the traditional ones such as fingerprinting, handwriting, signature verification etc.

Biometric Technologies (BTs) in modern (commercial) condition actively applies for an independent place in complex hierarchy of information technologies. The terms to determine the borders of this place have been formed: *biometric industry, biometric products, biometric projects, biometric approach and methods, biometric devices (scanners, ID cards, etc) and systems* and so on [BioD], [BioT], [BioR]. This is, of course, not very correct from the position of designers of such system, however, on the other hand, it proves intensive commercial applications BTs. It is obviously, that BTs are closely connected with problems of information security [Phil], including criminology [Diat].

In this paper we consider BTs from the position of using the image processing and pattern recognition methods, or *high-level vision*. Vision is a complex process that includes many interacting components involved, for example, with the analysis of color, depth, shape, motion, texture of objects, and with the use of visual information for recognition, extraction of shape properties, classification, locomotion, and manipulation. The significant part of modern directions of BTs is implemented based on classical and modern approaches which are very well established for various engineering applications (robot engineering, radiolocation, map drawing, document recognition and understanding, etc.)

At the same time, to realize BTs, it is required to take into account many rather specific requirements, for example, a character of timing stability of attributes, statistical sufficiency of these attributes, increasing the reliability of object identification. That part of these problems can be decided and frequently is decided based on enough simple approaches, say, by a combination of BTs and traditional methods.

The main goals of this paper are: (i) to show close connection BTs with methods of image processing and pattern recognition, to pay attention the experts to it a heavily developing direction, and (ii) to analyse BTs from the academic point of view, i.e. as object of study in educational establishments.

The paper organized in following way. In the first section we present the main directions of modern BTs which are using in practice. The practical applications are considered in details in the second section of the paper. In the third section we concentrate our attention on methods and algorithms of image processing and pattern recognition which are using in BTs. Finally, in the last section of the presenting paper we discuss as an example eye's identification technology.

2. Modern directions of Biometric Technologies

Nowadays term BTs means: *voice and speech recognition, dynamic signature and handwriting capture, eyes (iris and retinal) identification, hand geometry, fingerprint (palm print) identification, face recognition and keystroke dynamics* (Fig.1) [BioD], [BioT], [BioR],[Shme].

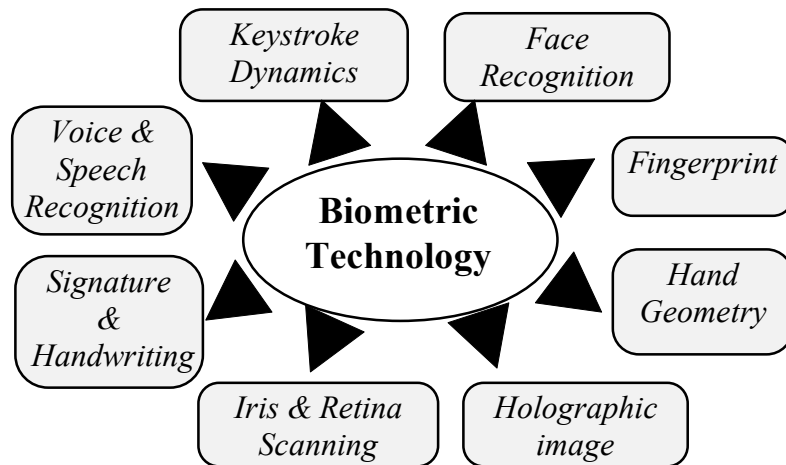


Fig.1. Main directions of modern BTs

In a number of cases, *thermal imaging* of a living objects is also used. Possibly, it should be classified as a separate direction of BTs.

It is quite clear from Fig.1 the modern view of BTs. It is necessary make some remarks only.

It is doesn't mean, that BTs includes this direction only. We say about the direction rich are used now in many practical applications. It is well known about many others investigation in biometrics, but these methods can be called as *laboratory's BTs methods and approaches*. We

don't discuss their in this paper, but many experts predict development of not-touch methods BTs, i.e. methods which allow identifying the person on distance.

Stability is the main criterion of the BTs. It is mean that we must good understand during what period the biometric attributes of an object will not be changed essentially. For instance, it is known that the signature and handwriting of a person are changed during a day and strongly depend on psychologic factors. The similar remark can be made on keystroke dynamics identification, for the same time it is necessary to add, that a number of other rather specific factors, for example, increasing of a professional skirling level, is here added. From the position of stability, steady interest to methods of fingerprint and eyes identification is clear. These methods of BTs have a number of unique properties, which allow using them during practically all life of the person.

Character of using the BTs methods is another criterion of a choice the BTs. For example, a number of the financial applications are characterized by short BTs devices life time and high extensively. It imposes a number of other requirements for choice and use of BTs methods:

(i) Whether it meets the requirements of a particular application. For example, for super smart cards, the signature and face identification are considered as good combination.

(ii) Whether it is possible to realize the chosen BTs by using identical mathematical and algorithmic methods. For example, signature and face identification methods have little in common.

3. Practical applications

The areas of BTs application is dynamically extend. It is possible to explain partially by that problems of information safety became priority for the present stage of IT development. The hopes on BTs are in many respects justified and their use frequently gives good results.

The modern BTs applications mainly concentrate in the following areas: *medical, law and order, banking and finance, immigration control, visual and voice communications, access control* (Fig.2). No doubt, everybody in his (her) life already met various biometric devices, which called in another way. Let us consider the applications and features of realizing some BTs in details.

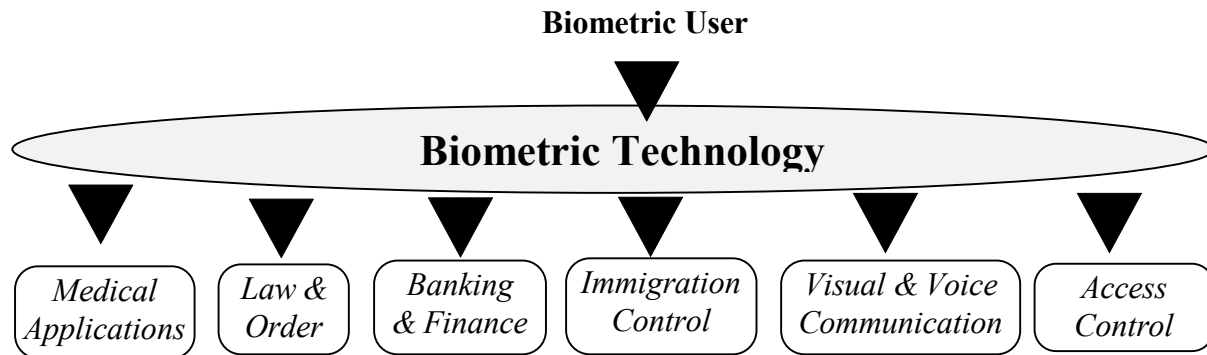


Fig.2. Main modern BT applications

3.1. Signature and handwriting authentication

Nowadays the automatic investigation of handwritten objects (for example, there are handwritten text, signature, short letter, notes) has been widely used: to confirm the document authenticity in the financial sphere; to solve the expert problems in criminology; to diagnose the physical and psychic state of patients in medicine; to make the psychological individual analysis in psychology and others.

This area of BTs is enough explored by specialists in graphology, psychology and medicine, and modern systems apply often the results obtained by in criminology. However, many revered approaches are differed essentially from the classic ones.

Computer analysis of handwriting signature and handwriting is very interesting research area. Most of the work done in this area has made use of real-time input (i.e., handwriting objects are input to the computer by means of light pen, table, and so on), so that the time sequence of strokes in the signature and handwriting is known. Little has been done on the analysis of these objects that is input to the computer by scanning and digitizing of source documents.

Automatic reading of unknown signature and handwriting is difficult problem. Signature and handwriting varies greatly, even for a single individual. It is hard to segment unknown signature and handwriting words into letters or strokes. This becomes much easier, although it is still quite nontrivial, when the words are known (the case of the signature of known person).

The task of handwriting objects verification is to determine whether a given signature or handwriting is genuine or forgery. In many papers consider the problem of detecting free-hand forgeries, where the forger made no attempt to simulate or trace a genuine signature. In the latter case, the forged handwriting object has the proper shape, but differs from genuine object in the quality of the strokes. Free-hand forgeries, on the other hand, differ from a genuine signature with respect to the values of various size and shape features.

The modelling of handwriting objects is a highly nontrivial task, since even genuine signatures and handwriting can be quite variable in size and shape, and template matching is not a viable approach to verification. Certain features of these objects are, however, believed to be relatively invariant for a given writer. These include ratios of small letter height to signature width, of tall letter height to small letter height, distances between letters, and so on. To measure these features, it is necessary to segment the signature at least partially - in particular, to determine the small and tall letter heights, and positions of the letters.

Before all, it should be noted, that the ways to solve the problems of authentication signature and handwriting are different. It is connected with the fact that the problem of signature verification is always solved in the conditions of indefinite information. Therefore in graphology frequently take the additional information by other ways, including chemical methods. It is

obvious, that there is no such opportunity for commercial (non-professional) applications, and it stimulates researchers for searching new, non-standard decisions.

The problem of handwriting verification requires other approach, as it is possible to gather from the letter, slip or address on the document, as a rule, enough for acceptance of the reliable decision.

It should be noted, that there is the large difference between professional and commercial versions of such the systems.

The design of a signature and handwriting verification system generally requires the solution of next types of problems: *data acquisition, pre-processing, feature extraction, comparison process, and performance evolution*

Personal signatures are easy forged because their verification is usually limited to a visual image comparison. The essence of signature verification in some cases is that the comparison is not made look but between the way in which they have been written. The type of information which is gathered from the signature writing process in order to carry out verification varies between systems, but the data captured usually includes the time taken to write the signature, the speed at which it is written, the number of times the pen is lifted from the paper and the points in time at which this occurs.

Therefore in a number of causes the design of such systems means the automatization the methods which have good investigated and widely used in police applications. The typical example is considered in [Pena]. A dynamic signature verification system which analyzes signatures dynamically by considering their shape, time, domain characteristics, such as speed and acceleration, and force domain characteristics, i.e. applied pressure, is presented there. Experimental results demonstrate 92% authentic signature detection accuracy and 100% forgery signature detection accuracy.

The following below technology is investigated in many papers. A signature is obtained as a sequence of x,y-coordinates of pen-tip movement and writing pressure. The features of a signature are derived from the coordinates and the writing pressure and are decomposed into two principal features, shape and motion. Various approaches are used below.

In [Lee] were proposed on-line dynamic signature verification system with a database of more than 10 000 signatures. Authors extracted a 42-parameter feature set at first, and advanced to set of 49 normalized features that tolerate inconsistencies in genuine signatures while retaining the power to discriminate against forgeries. Authors studied algorithms for selecting and perhaps orthogonalizing features in accordance with the availability of training data and the level of system complexity. For decision making authors studied several classifiers types. For example, one of the classifiers yielded 2,5% equal error rate and, more importantly, an asymptotic performance of 7% false acceptance rate at zero false rejection rate, was robust to the speed of genuine signatures, and used only 15 parameter features.

Let us give some results which allow discussing about approaches to solve the problem. So, Neural networks (NNs) were proposed in [Huan] for signature verification. Experiments have showed that average 90% test samples can be correctly classified on a data set of over 3000 signature images.

The main point of the approaches supported in [Huan] is the following. Geometric features of input signature image are simultaneously examine under several scales by a NN classifier. An overall match rating is generated by combining the outputs at each scale. Artificially generated genuine and forgery samples from enrolment reference signatures are used to train the NN, which allow definite training control and at the same time significantly reduce the number of enrolment samples required to achieve good performance.

In [Sabo] proposed a formalism for signature representation based on visual perception. A signature image of 512x128 pixels is centred onto a grid of rectangular retinas which are excited by a local portion of the signature image. Each retina has a local perception of the entire scene.

The methods of fuzzy logic and evolutionary programming are also often used to solve the problem of signature and handwriting verification [Xuhu], [Zhou]. There are known the papers which reported about very good results of off-line signature verification system based on fuzzy logic.

Let us consider generally one of possible approaches to handwriting verification, what is used in criminology practice. At the first step, as a rule, features' set is formed. that reflects the distinctive feature of handwriting and not depends on the text content. Such features are often described as handwriting feature vector. The Hough transform is a standard technique for finding features such as lines in images. Typical, edges or other features are mapped into a partitioned parameter or Hough space as individual votes. The target image features are detected as peaks in the Hough space.

At the second stage of investigation, a decision (for example, about identity of text writers) is made. Here, handwriting feature vectors corresponding to the different text fragment are compared.

There are well known approaches to make a decision: vector data analysis and preliminary transforms the high-dimensional vector data to the one-dimensional. Latter is performed by either convolution operation or distance calculation between vectors using metric. The weight Euclid distance is used as distinction measure of handwriting feature vectors.

The main requirements at the system design are to make a decision with guarantee authenticity and to supply the refusal from unreliable situation. The decision making approach based on the modification of Bayes statistical procedure. NN can be efficiently used at the first step. Let us consider the results of [Koch] as an example. NN contains about $5 \cdot 10^3$ links. The expenditures on the learning phase is $4 \cdot 10^6$ teaching cycles. The NN had been tested on the control set having such size like the teaching set. It is proved that the accuracy 91,3% - 93,3% was achieved.

An example of realization of once more original idea is the results represented in [Cui]. The hand movement is tightly coupled with spatial recognition (hand shape). The system uses the multiclass, multidimensional discriminant analysis to automatically select the most discriminating features for gesture classification. Authors propose a recursive partition approximator to do classification. The framework has been tested to recognize 28 different signatures. The experimental results show that the system can achieve a 93,1% recognition rate for test sequences that have not been used in the training phase.

Two different approaches have been taken to capture the signature dynamics: an active pen and sensitive tablet. For example, a document can be sent by the email, authorised by a signature which do not have graphic form. This signature includes parameters of pressure, the number of times the pen was lifted from the paper and so on. It is an easy means of security.

Another requirements are taken into account in signature and handwriting person verification systems when making criminological researches and expertise.

The process of an authentic signature addition to the database consists of the following steps: scanning of binary signature image from a document, building mathematical model, and placing it as a separate record in the database.

Afterwards the model is extracted by some key (for example, by client account number), and the reproduction program restores the original view of a signature to the screen. The examined signature is also scanned and displayed on the screen. Thus, a bank clerk has a opportunity during some seconds to access to original client signature and to compare it with the current image.

To be noted, the information stored in such way is insufficient to match criminological expertise, which required from 6 to 20 original objects (depending on signature complexity).

The transformation of scanned image consist of following stages: image thinning, image representation as a graph, shape smoothing, graph minimization, and shape compression.

Some approaches to work out professional signature and handwriting identification systems were reported in [ShmY], [ShmK], [Abla]. Such systems are characterized by that they meet the requirements accepted for criminology.

It also should be pay an attention for papers [Amma], [Plam] and [Lee], where very optimistic results were achieved.

The experts-graphologists have accumulated rather large experience in handwriting and signature authentication, what now begins to be used in various commercial applications. We pay our attention only for one factor of the given BTs direction, namely the timing instability of the given form of biometric information. It is well-known, that handwriting and signature of a person strongly correlates with his mood and feeling. As one of paradoxical examples, we consider a few Napoleon the Emperor's signatures made at the most significant shocks in his (and Europe!) life (Fig.3) [Morg]. On the other hand, this signatures illustrate not only graphical features, so, their processing allow obtaining the quite significant characteristic such as signature dynamics.

It was stressed in the beginning of this section that commercial systems use often the experience of policy. However, the classic approaches are also mainly not automatized. At the best it is possible to speak about automation some stages of signature and handwriting verification. In it easily to be convinced when visiting the appropriate division of police.

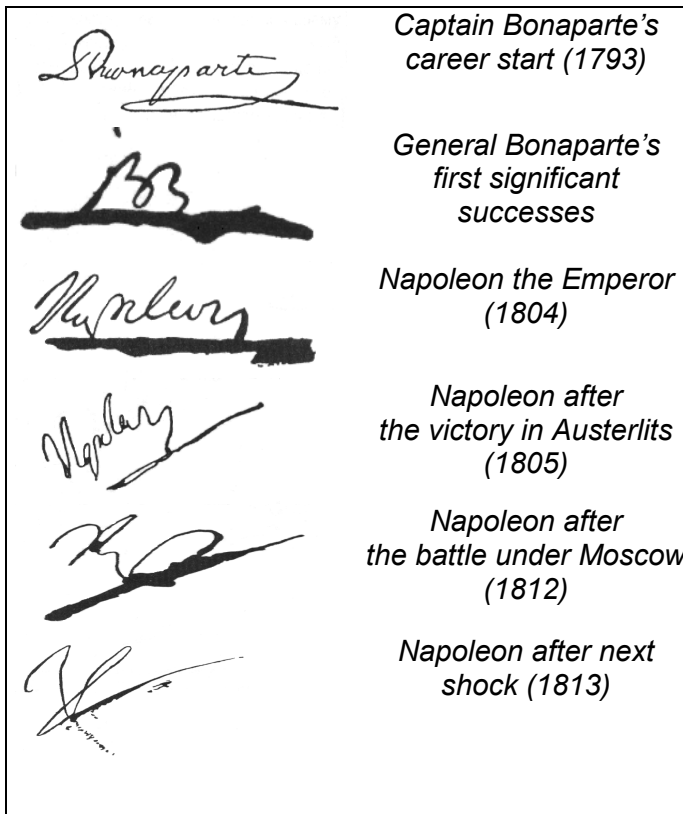


Fig.3. Change of the signature of Napoleon after some historical events on an during 20 years

3.2. Keystroke Dynamics

Everybody has their own typing rhythm and it is this rhythm that keystroke dynamics utilises.

The process of typing the personal identification number (PIN) can be broken down into quantifiable components, such as latency time, keypress force, keypress duration and keypress displacement which can be evaluated and used to verify the identity of a person. the keypress pattern is called the PIN signature. As the PIN signature is like the written signature that differs slightly with every execution, a neural-fuzzy application is devised to verify the PIN signature input against the reference profile [Tee]. Like signature dynamics, keystroke dynamics are difficult to reproduce.

Note, that to investigate the keystroke dynamics, the methods of visual interpretation for the process are widely used. It allows not only simplifying the analysis, but further using the well

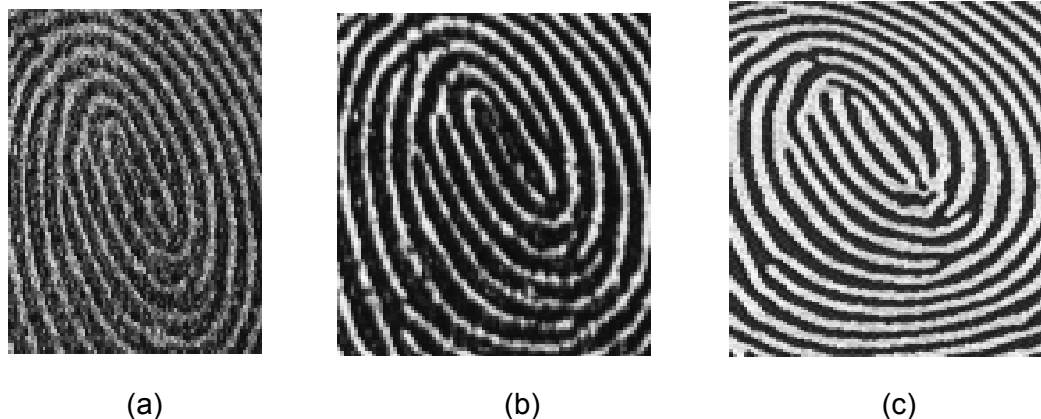


Fig.4. Illustration of the image processing of fingerprint: input fingerprint (a) - result of some steps of preprocessing (b) - fingerprint image for extraction features (c). At the last fingerprint image can see *terminations, bifurcations, trifurcations and undetermined*, and the task is automatically find and extract these feature

investigated methods of image processing and pattern recognition.

3.3. Fingerprint authentication

The application which most people are familiar with in this area are Automatic Fingerprint Identification Systems (AFIS) as used by police forces across the world (PRINT-PAK-ORION Systems, MORPHO Systems, NEC Systems, COGENT Systems, and others). BTs have in this direction rather deep historical roots (from the mid 1880) and enough experience accumulated in criminology [Chap].

The problem of automation of this activity is solved during last decades, and rather impressive results were achieved. The numerous other applications of the fingerprint authentication products are, as a rule, special cases of AFIS. Therefore it is expediently to consider a place of image processing and pattern recognition methods in such systems.

Most automatic systems for fingerprint comparison are based on *minutiae* matching (local discontinuities in the fingerprint pattern). The American National Standards Institute has proposed a minutiae classification based on four classes: *terminations, bifurcations, trifurcations and undetermined* [Amer].

Many approaches to automatic minutiae extraction have been proposed, for instance, recent papers [Hali], [Maio], [Mech]. However always is realized next technology: *<Input fingerprint image> <Improvement of legibility and smoothing out> <Outlining> <Binarization> <Thinning> <Extraction of minutiae>*.

It is typical for the fingerprint image that the finger is usually not printed uniformly: one part of it is extremely light and other part dark, so methods based on global threshold finding fail. There are also other causes to make necessary the pre-processing of fingerprint image.

Thus, for example, a NN based on self organizing feature maps is proposed for fingerprint classification [Hali]. The author's results show that a NN that is trained with a sufficiently large and representative set of samples can be used as an indexing mechanism for a fingerprint database, so that it does not need to be retrained for each fingerprint added to the database.

NN are often applied to compress fingerprint images. The following technology is used: by learning with self-supervision, NN finds near-optimal clustering from image data and builds a compression codebook in the weight connections.

Since the majority of the commercial applications are the simplified and partial solutions of professional AFISs, it is meaningful to consider AFIS in more detail.

The theoretical basis of a modern AFIS is illustrated in Fig.5. The AFIS is structurally represented by number levels hierarchical model reflecting an existing structure of dactylography information flows in police. The example of such system - national AFIS] - is represented below in Fig.7 [Gord], [Zavg].

The nodes of the national level are included the electronic archives of dactylocards of common use (about 1500 000). The nodes of the regional level are held an electronic archives of common use with fingerprints from the places of crime commitment (10 000-40 000). In each node of the district level is held particular electronic archives of fingerprints (about 13 000).

There is a large amount of the fingerprint information (more than 500 000) on the hard medium (paper, film) in expert-and-criminalistic divisions. Such form of information does not suitable for identification by AFIS, it should be transformed into special electronic format. To converse the existed and newly entering dactylographic information into electronic format.

Inputted fingerprint information consists of a descriptive part and fingerprints images.

After processing fingerprints input, this information is transformed into electronic format and also an additional code characteristic is formed. This code is a result of automatic image processing and it namely uses in next search operations. It is allowed editing (translation) of fingerprint information.

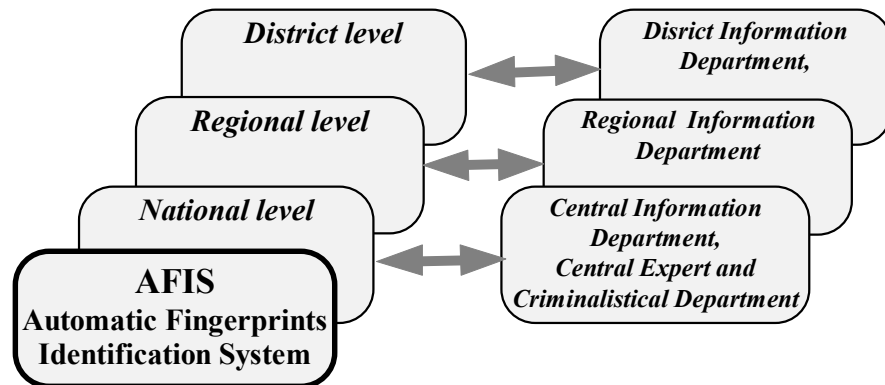


Fig.5. A three levels hierarchical model of AFIS and its representing by reflecting onto fingerprint information flows

All inputted (edited) information is personalized, so any time it can be ascertained who namely inputted (edited) information. This is necessary for exception of abuses and estimation the quality of operators work at input of fingerprint information.

3.4. Eyes identification

Traditionally use two ways to identify the eyes. These ways differ in accordance with the zones of eye, from which the attributes are obtained: (i) the blood vessels on the retina, and (ii) iris. These systems are most secure biometrics and require to apply rather complex methods of image processing (further we demonstrate elements of this technology). The iris identification systems looks promising for the future, as allows to use standard means (telechamber and processor), whereas retina systems require special and expensive devices (retina scanning devices).

Many papers are concentrated on radial basis function feed-forward NN. Their authors affirm that such NN are more assimilated for the given type of objects.

One of problems is an iris localization for a head-mounted eye tracker. The tracker must gaze direction to be measured by supplying simultaneous views of a subjects eye and of the world from a head-mounted camera. Finding gaze direction relative to the head requires accurate and robust measurement of the iris outline under a wide range of lighting conditions, in the presence of highlights, and when the iris is in an extreme position.

Some approaches for eyes identification are referred more in detail in [Absa], [Herp].

3.5. Face identification

Facial recognition is also a convenient means of identification because, as it is often said in advertising, „you don't have a worry about losing your ATM card or forgetting your PIN (personal identification number) - you always have your face with you”.

Researchers in computer vision and pattern recognition have worked on automatic techniques for recognizing human faces for the last 20 years.

In facial recognition system computers perform three classical tasks: *verification* (the system attempts to match a live face with a specific reference digital image), *recognition* (the system try to match a live face with any saved faces in a central computer database), and *locating* the face within the image.

One of the problems is face recognition under varying pose. Sometimes use the next technology: (i) representation of faces with templates from multiple model views that cover different poses from the viewing sphere, (ii) recognition of a novel view, the recognizer locates the eyes and nose features, uses these locations to geometrically register the input model views, (iii) using the correlation on model templates to find the best match in the database of base of people.

One of the very important steps of this process is determination the best facial features to discriminate the features of one face from those of another (sometimes this process called *eigenfaces*). Typically, a sample of only 40 -50 eigenfaces.

Human face detection is another interest problem considered in many papers. An edge-enhancing preprocessor and some separately trained backpropagation NN are often applied for this problem. Many authors report about good results on using the NN at the first stage of face recognition: determines general properties of the input, such as whether the facial image contains glasses or a beard.

This direction attracts the serious attention of specialists last years. It is connected with that many problems have not been solved yet in this direction. The technology of face image recognition can be explained with the illustration on Fig.6. The idea consists in search of conformity (on determined criteria) face model to face image. This idea is realized with staircase procedures of processing (from above downwards to face image and from below upwards to face model). The set of the factors influences for search of an optimum way, which comes to an end by identification or recognition. The major factors are specified on Fig.6: expression, illumination and so on.

So, in [Ezza] the image - based model is build using example views of the face, by passing the need for any three-dimensional computer graphics models. A learning network is trained to associate each of the example images with a set of pose and expression parameters. In [Folt] a wavelet decomposition technique or morphological non-linear filtering is used to enhance intrinsic features of a face, reduce the influence of rotation in depth, changes in facial expression, glasses and lighting conditions. In [Yoko] the method to detect human face regions precisely, without imposing any constraints on the face size, position or features (glasses, beard, and so on), employs a genetic algorithm. The proposed method detects the edges in input image, and it searches elliptical regions.

Some new ideas are explained in [Yase].

Interesting results have been achieved by our colleagues fro East European countries, however, unfortunately, the most part of the publications is submitted in Russian at national conferences. We would like mention the paper [Kova] in this area.

It is necessary to emphasize, that using the tomography methods allow solving many problems of face recognition. However these methods requires large computational cost.

It is the not complete list of original ideas in this area. Visual communication is another application of the BT. Now this direction has been extensively studied, especially in the

psychology literature. It should be noted that face recognition - one of few investigated directions BTs. The commercial applications of such systems are known, however they work at a number rather strong restrictions.

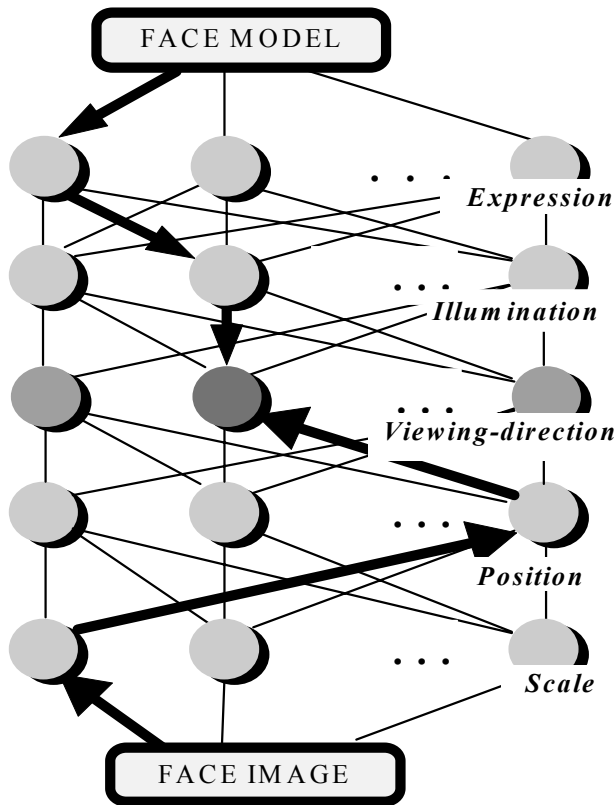


Fig.6. Technology of face image recognition

3.6. Complex methods of authentication

At present, a number of systems for verifying a person identity have been developed that rely on a single, intricate identifying feature such as fingerprint or the eye retina. As a rule, such systems generally uses details which complicate sensing and necessitate a certain amount of direct interaction with users. So, to explore new techniques that reduce the amount of interaction required and minimize the possibility of deception is advantageous. Developing a non-contact (i.e., without physical contact) biometric identification system with quickly determining or verifying the person identity with a low error probability is very important. The low error probability is achieved by fusing coarse features remotely acquired from face, hand, and voice. These individual features provide inadequate error performance, however, information obtained by fusing or combing the features in a feature space enables reliable identity determination. The applying of coarse features reduces the computing power required for feature extraction, simplifies the remote sensing requirements

and minimizes human interaction with the system. Such simultaneous using of multiple features from multiple sensors lessens the possibility of deception. Recently, a number of papers to develop such approach, occurred, in particular [Carl].

The complex methods combined the traditional and BTs approaches and methods are used for many reasons, main of which is the increasing of reliability of identification. As an example we shall consider so-called tamper-proof card, which is a good example of such combination.

The tamper-proof cards include the cardholder's photo, identification number, a two-dimensional bar code and a digitized image of the bearer's signature (Fig.7).

The cards are created when clients enroll in the system. Applicants place their index fingers, one at the time, on an optical reader, which scans them to create images for database. While the scans are taking place, the client's photograph is taken with a digital camera. Next, the client signs a digitizer tablet, which captures the signature electronically. After the fingerprints are scanned, the files are transmitted to a server, where all client fingerprint images are stored in a database.

Use complex methods always causes questions of validity of the decisions, i.e. assumes the decisions of a problem of comparison of a level of privacy of various methods. However, as a rule, use of many methods of protection does not raise a level of safety.

4. Methods of image processing and pattern recognition in BTs

The analysis shows, that the overwhelming part of BTs is realized by using image processing and pattern recognition methods and algorithms. As the most evident example, we consider here the following BTs: hand geometry, signature and handwriting, face recognition finger and palm print, iris and retina scanning. To solve the problem, in this or that form the following main methods were used: *digitization, compression, enhancement, restoration, reconstruction, segmentation, feature measurement, scene analysis, image representation, models, design methodology, clustering* (Fig.8).

Note, that the distance BTs require to use additionally the tomography methods, however it is not the subject of the present paper.

Typically, a number samples are taken at time (speech, signature) and processed in accordance with a chosen method. An intermediate image is formed as result.

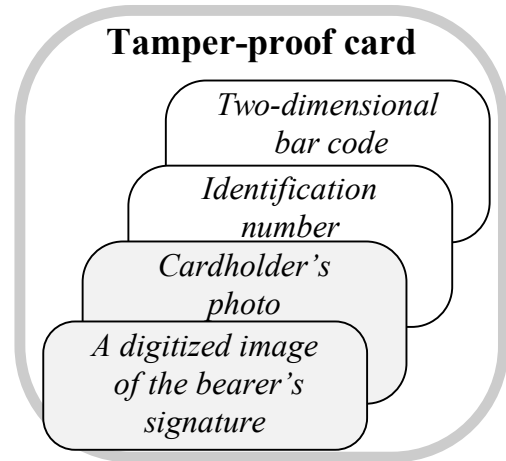
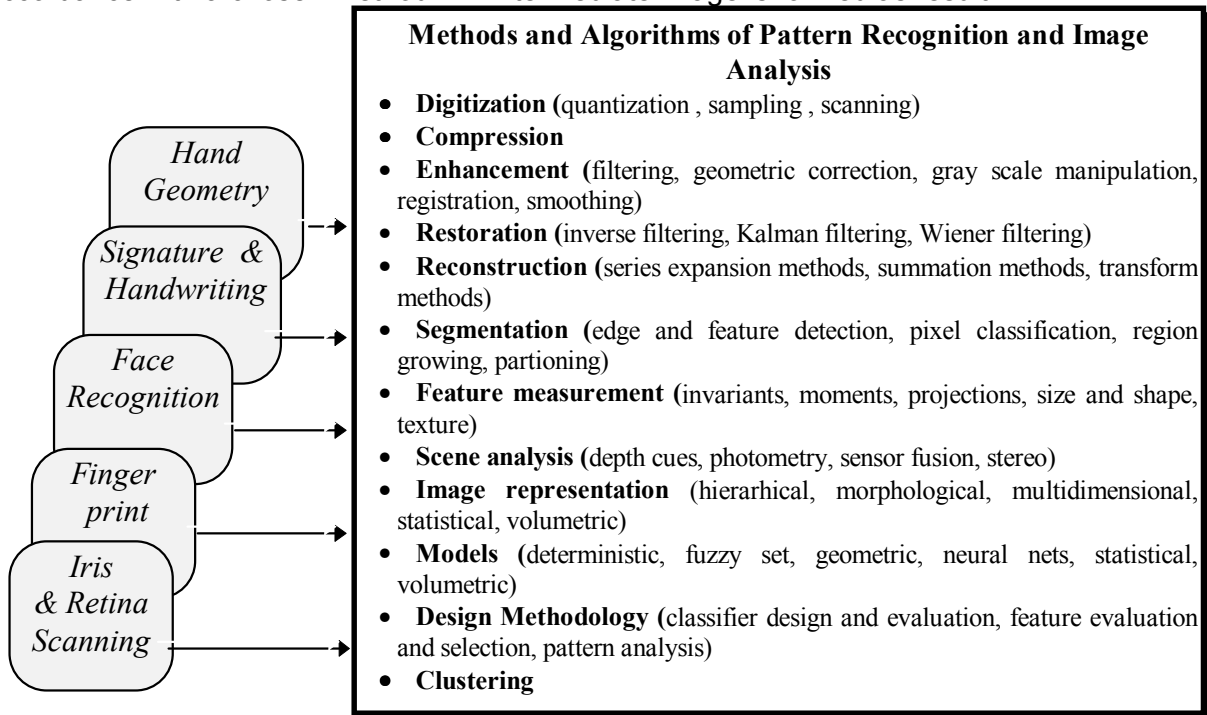


Fig.7. The tamper-proof card combines BTs and traditional person identification approaches



- Methods and Algorithms of Pattern Recognition and Image Analysis**
- **Digitization** (quantization , sampling , scanning)
 - **Compression**
 - **Enhancement** (filtering, geometric correction, gray scale manipulation, registration, smoothing)
 - **Restoration** (inverse filtering, Kalman filtering, Wiener filtering)
 - **Reconstruction** (series expansion methods, summation methods, transform methods)
 - **Segmentation** (edge and feature detection, pixel classification, region growing, partitioning)
 - **Feature measurement** (invariants, moments, projections, size and shape, texture)
 - **Scene analysis** (depth cues, photometry, sensor fusion, stereo)
 - **Image representation** (hierarhical, morphological, multidimensional, statistical, volumetric)
 - **Models** (deterministic, fuzzy set, geometric, neural nets, statistical, volumetric)
 - **Design Methodology** (classifier design and evaluation, feature evaluation and selection, pattern analysis)
 - **Clustering**

Fig. 8. Implementation of some BTs requires to use practically all modern achievements in image processing and pattern recognition

It is interesting to compare storage requirements for these templates for various BTs (Fig.9). We have used many various sources and also our own research results. So, for instance, we report here resent results of the authors of [Cheu].

The number varies between nine bytes to more than one thousand. It is feasible to store the large numbers of templates in standard memory media.

It should be said some words on compression methods for biometric information. For instance, instead of storing an actual image of the fingerprint as the template, most verification devices store a code which relates to the location of the minutiae points on the fingerprint.

It should be said some words on compression methods for biometric information. For instance, instead of storing an actual image of the fingerprint as the template, most verification devices store a code which relates to the location of the minutiae points on the fingerprint. The template cannot be used to recreate an image of the fingerprint so it is of no use to law enforcement agencies. the templates range in size from 25 to 2000 bytes so can be stored as a bar code, on a magnetic stripe card, smart card or on a central database connected to the owner by a PIN.

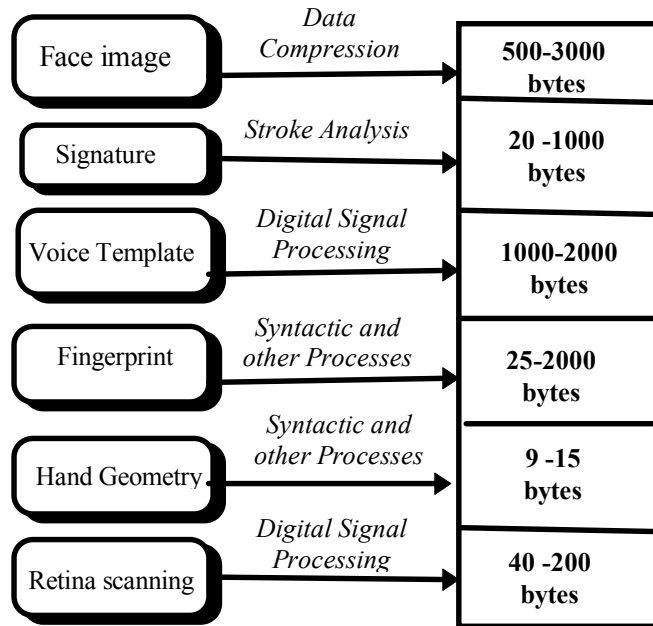


Fig.9. Space requirements for various biometric data storage

To identify a person based on retina scanning technology, it is enough to process 200-300 pixels of the image and then to compress the results by traditional way. From 40 to 200 bytes are enough to store one image.

4. Eyes identification technology from academic point of view

BTs is a very interesting area from educational point of view. First, it is important to acquaint the students with this modern direction of information safety. Secondly, studying the BTs requires rather extensive theoretical and practical knowledge from adjacent scientific directions and, at last, thirdly, studying the BTs from the methodical point of view can be considered as good mean to stimulate curiosity of the students.

In this section we demonstrate some elementary methods used effectively to allocate attributes from the image of an eye

(iris) (Fig.10). The choice of iris as object for biometric information is explained by a number of reasons, in particular: there is no necessity to use special equipment and software; the identification of iris is referred to a number of methods with raised level of information safety.

This section describes the fragment of laboratory work for students specialized in *Banking Information Technologies* at the Institute of Computer Science & Information Systems, Technical University of Szczecin (Poland). Note, that students do this laboratory work on *Banking Information Systems*, after the courses on *Image Processing*, *Artificial Intelligence* and *Information Security*.

The laboratory work is built basing on the software package MATLAB, a platform IBM/PC 586.

The main point of the experiment is to allocate attributes meeting the requirements (i) stability of statistical estimations for identification process, (ii) independence of turns of the object, and (iii) independence of scale (the last two points are the main features when comparing the features of initial object with its features with ones from data basis).

In laboratory task the students study two approaches: (i) allocation of attributes in object after its transformation into polar and polar-logarithmic systems of coordinates, and (ii) allocation of spectral attributes.

We shall state only part of laboratory work - iris transformation into polar and polar-logarithmic systems of coordinates. The theoretical bases of this part are stated in work [Kuch]. We shall be limited only by some comments to intermediate results of technology of identification.

Distinction of two ways of segmentation of the object image is well appreciably in polar system of coordinates, that is illustrated by Fig.11-13. In the first case the scanning is performed from a conditionally found centre of an eye without preliminary preparation (Fig.12). Thus non-character attributes belong to the pupil on the eye are dominated. In the second case, a pupil of an eye is excluded from the processing, and the unique own attributes are observed in the polar system of coordinates (Fig.13).

Note, that transformation of the initial image to polar and polar-logarithmic systems of coordinates basically eliminates problems of displacement and scaling during comparison with reference images (attributes).

We give an opportunity for students to be convinced of it during doing their exercises. In this connection expediently to result some themes of the abstracts and individual tasks of the students, in particular:

Statistical sufficiency of reliable identification of the person on eyes (fingerprints, signature, handwriting, speech),

Comparison of efficiency biometric methods (on criteria of compression of the information, volume of computing and hardware expenses, speed of identification),

Comparison of methods of identification in temporary and spectral areas.

5. Open Problems

As any other rather new area of human activity, BTs have not today a system approach to design systems to realize BTs technology. For example, techniques and criterion of a choice of particular BTs for the purposes of applications have not been developed. It stimulates interest of many experts to the given subject area. NCSA (National Computer Security Association, USA) will perform various biometric projects on behalf of its corporate members as well as CBDS (Commercial Biometric Developers Consortium, USA) members. NCSA is likely to do research on biometric product effectiveness, to develop methodology to test and certify biometric products. For the same time, large experience of designing AFIS has been accumulated. The most simple engineering solutions of AFIS are widely used in banking, financial and access control.

The important factor to influence onto using other BTs is the developing of effective marketing strategies. BTs application is connected with the decision of many new problems, in particular, legal & social problems, alerts to ethical use, privacy considerations, industry standards, biometric & internet security and others (Fig.14).

On estimations of the experts many problems require non-traditional approaches. However frequently the life much accelerates the decision ethical and social problems, connected to wide by use BTs-systems, for example, national safety, terrorism, immigrations' problem, large losses of financial institutions and etc. The numerous examples of the decision of these problems are resulted in [BioD], [BioT], [BioR].

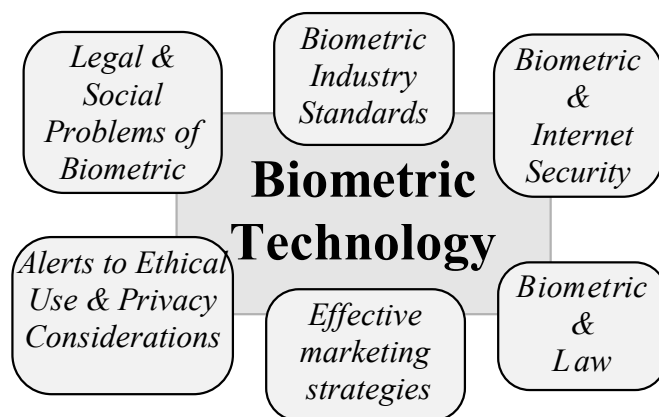


Fig. 14. The future of BTs is connected with solution of many not only engineering problems

6. Conclusion and comments

The modern practical applications BTs make a *small part of our knowledge* about living objects. The distance methods of identification of the person are used at the moment in the elementary variants and presently are the subject for laboratory researches. Today is real such the forms of BTs as fingerprint, as voice and speech, signature and handwriting, eyes, hand geometry, face, keystroke dynamics and others . It means, that rather effectively it is possible to automate processes of identification of the person under these forms of the biometric information and to satisfy with the requirements of many practical applications.

Biometric products design requires knowledge of the modern achievement from many directions of human activity. The realization of any system BTs for commercial application requires *interdisciplinary researches*.

The overwhelming part BTs is closely connected to methods image processing and pattern recognition. It means that many experts of this area can use their knowledge and methods in BTs. BTs is one of areas, for which systems approaches to designing and creation BTs-systems are not developed. The main obstacles are absence of the standards, not enough experience of the existing BTs-systems (excepting fingerprints devices and systems). The effective use BTs requires to solve many social questions, connected to the law, etiquette and others.

Use of methods BTs in educational process gives many interesting effects, main of which is, that stimulates inquisitiveness of the students in study of methods image processing and pattern recognition. It is possible to expect increase of interest to BTs. This forecast is based that BTs effectively supplement traditional ways of identification of the person and in a number of cases it appear more preferable or effective

ACKNOWLEDGEMENT

The work was supported in part by Committee on Scientific Researches (Poland) and in part by the Informatization Foundation (Belarus), and in the frameworks of agreement on co-operation between Institute of Computer Science & Information Systems (Technical University of Szczecin, Poland) and State Economic University (Belarus). We are very grateful to many colleagues from Lab. *New IT in Economic & Management* (Economic University), Lab. *Pattern Recognition & Image Analysis* (University Informatics & Radioelectronics) (Belarus), Institute Computer Science & Information Systems (Technical University of Szczecin, Poland), Central Forensic Laboratory of the Police (Warsaw, Poland), *Institute of Problems on Criminology, Criminalistics and Forensic Expertise*, and *Laboratory of Prof.Dr.Revinsky* (Belarus), for fruitful discussions and possibility to get to know their results. Our thanks go to Polish and Belarussian students *G.Holowinski, T.Roszak, K.Malecki, D. Popel and A.Shakirin* for their help.

References

- Ablameyko S., and Shmerko V., Graphics Recognition and Handwriting Text Identification: Belarussian Results and International Co-Operation, *Proc. 3rd Int.Conf.on Applications of Computer Systems - ACS'96*, (J.Soldek Editor.), *Technical University of Szczecin, Poland*, 1997, pp.343-354
- Ammar M. Progress in Verification of Skillfully Simulated Handwritten Signatures, *Pattern Recognition and Artificial Intelligence*, vol. 5, 1993, pp. 337-351.
- Absaloms H., and Tomikawa T., A Study of Human Eyes' Detection by Window-pair Chasing, *Trans. Inst. Electr. Eng. (Japan)*, vol.116 - C, no.9, 1966, pp.1015-1028
- American National Standards, Fingerprint Identification - Data Format for Information Interchange, N.Y., 1986
- Biometric Digest™* (USA), Ed. William Rogers, 1996/1997
- Biometric Technology Today™* (UK), Ed. Emma Newham, 1995/1996
- Biometrics Report*, 1996 (UK)

- Carlson J.J., and others, Fusion of Multiple, Coarse Features from the Face, Hand and Voice for Realable Human Identity Determination. *Proc. SPIE (USA)*, vol.2755, 1996, pp.283-293
- Chapel C.E., Fingerprint - A Manual of Identification. N.Y., *Coward McCann*, 1971
- Cheushev V., Miller J., Thomson P., and Popel D., The Mathematical Model of Signatures for Compact Storage and Operative Personal Identification in Bank Systems, In.: *V.Shmerko and S.Yanushkevich (Eds.), Banking Information Systems, Technical University of Szczecin, Poland, 1997*,
- Clergeau-Tournemire Stephanie, and Plamondon Rejean, Integration of Lexical and Syntactical Knowledge in a Handwriting-Recognition System, *Mashine Vision and Applications, Springer-Verlag*, 8, 1995, pp.249-259
- Cui Y., and Weng J.J., Hand Sign Recognition from Intensity Image Sequences with Complex Backgrounds, *Proc.of the 2nd int. Conf. on Automatic Face and Gesture recognition, Killngton, USA*, 1996, pp.259-264
- Diatlov O., and Bocharova O., Criminalistic Estimation of Possibilities of Ascertainment of Forgery of Documents, which are Produced by Means of Assembling, In.: *V.Shmerko, and S.Yanushkevich (Eds.), Banking Information Systems, Technical University of Szczecin, Poland, 1997*, pp.
- Ezzat T., and Poggio T., Facial Analysis and Synthesis using Image-Based Models, *Proc.of the the 2nd Int. Conf. on Automatic Face and Gesture Recognition, Killngton, VT, USA*, 1996, pp.116-121
- Foltynowicz R., Automatic Face Recognition via Wavelets and Mathematical Morphology, *Proc. of the 13th Int. Conf. on Pattern Recognition*, vol.2,1966, pp.13-17
- Gordey D., Gotin A., Zavgorodnev S., Lopatenko O., and Revinsky V., Structural Organization and Operation Principles of the National Fingerprint Identification System (NAFIS) of Ministry of Internal Affairs, Republic of Belarus, In.: *V.Shmerko, and S.Yanushkevich (Eds.), Banking Information Systems, Technical University of Szczecin, Poland, 1997*, pp.
- Halici U., and Ongun G., Fingerprint Classification Through Self-Organizing Feature Maps Modified to Treat Uncertainties, *Proc. IEEE (USA)*, vol.84, no.10, 1996, pp.1497-1512
- Herpers R., and others, Context Based Detection of Keypoints and Features in Eye Regions, *Proc. of the 13th Int. Conf. on Pattern Recognition*, vol.2,1966, pp.23-28
- Huang Kai, and Yan Hong, Off-Line Signature Verification by a Neural Network Classifier, *Proc. of the 17th Australian Conf. on Neural Networks, Canberra*, 1966, pp.190-194
- Kochergov E., Decision Making System for Handwriting Person Identification Based on Neural Network, *This issue*
- Kovalev V., Diakova N., and Bondar Y. On Feature Selection for Face Image Recognition. *In this book*
- Kukharev G., Direct and Inverse Transformations of Spectra from Cartesian into Polar System of Coordinates, *This issue*
- Lee L. L., Berger T., and Aviczner E., Reliable On-Line Human Signature Verification Systems, *IEEE Trans, on Pattern Analysis and Machine Intelligence (USA)*, vol.18, no.6, 1996, pp.643-647
- Maio D., and Maltoni D., Direct Gray-Scale Minutiae Detection in Fingerprints, *IEEE Trans. on Pattern Analysis and Mashine Intelligence*, vol.19, no.1, 1997, pp.27-40
- Mechtre B.M., Fingerprint Image Analysis for Automatic Identification, *Mashine Vision and Applications*, vol.6, no.2-3, 1993, pp.124-139
- Morgenshtein I. Psycho graphology, *St.Petersburg, Publishing House by Vejerman*, 1903 (In Russian)
- Penagos J.D., Prabhakaran N., and Wunnava S.V., An Efficient Scheme for Dynamic Signature Verification, *IEEE SOUTHEASTCON'96, Tampa, FL, USA*, 1996, pp.451-457
- Phillips Phil, and Yanushkevich S., Modern Conceptions of Information Security In.: *V.Shmerko, and S.Yanushkevich (Eds.), Banking Information Systems, Technical University of Szczecin, Poland, 1997*
- Plamondon R., and Lorette G., Automatic Signature Verification and Writer Identification -The State of the Art, *Pattern Recognition*, 1989, vol.22, no.2, pp.107-131
- Polonnikov R., and Korotkov K. (Eds.) Biometric Informatics and Eniology, *St. Petersburg, 'Olga' Publishing House*, 1995 (In Russian)
- Saborian R., Genest G., and Preteux F., Pattern Spectrum as a Local Shape for Off-Line Signature Verification, *Proc. of the 13th Int. Conf. on Pattern Recognition*, vol.3,1966, pp.43-48
- Shmerko V., and Yanushkevich S. (Eds.), *Banking Information Systems*, Technical University of Szczecin, Poland, 1997

- Shmerko V., Experience of Designing and Using Signature and Handwriting Person Identification Systems, *The BCS Computer Security Specialist Group Annual Conference 9-10th March, London, UK, 1995, British Computer Society, London UK*
- Shmerko V., Kochergov E., Mikhaylenko S., and others, Systems for Personal Identification using Methods of Signature and Handwriting Verification. *Proc. of the 3-rd Int. Conf. on Pattern Recognition and Information Analysis (S. Ablameyko Ed.), Minsk, Belarus, vol. 3, 1995, pp.25-35.*
- Tee E.R., and Selvanathan N., Enhancing the Personal Identification Number Input as a Means of Identification Signature. *Malaysian J.Comput. Sci. (Malaysia), vol.9, no.1, 1996, pp.37-41*
- Xuhua Yang, and others, Selection of Features for Signature Verification Using the Genetic Algorithm, *Comp. Ind.Eng. (UK), vol.30, no.4, 1996, pp.1037-1045*
- Yaser Yacoob, and Larry S.Davis, Recognition Human Facial Expressions from Long Image Sequences Using Optical Flow. *IEEE Trans. on Pattern Analysis and Machine Intelligence, vol.18, no.6, 1996, pp.636-642*
- Yokoo Y., and Hagiwara M., Human Faces Detection Method Using Genetic Algorithm, *Proc. of 1996 IEEE Int.Conf. on Evolutionary Computation (Japan), 1996, pp.113-118*
- Zavgorodnev S., Kolyada A., Revinsky V., and Selyaninov M., Methodical and Algorithmic Principles of Base Technology of Fingerprints and Imprints Processing for National Fingerprint Identification System (NAFIS) of Republic of Belarus, In.: V.Shmerko and S.Yanushkevich (Eds.), *Banking Information Systems, Technical University of Szczecin, Poland, 1997*
- Zhou R.W., and Quack C., An Automatic Fuzzy Neural Network Driven Signature Verification System, *The IEEE Int. Conf. on Neural Networks, Washington, USA, vol.2, 1996, pp.1034-1039*