P3057/2000

ISSN 0239-8044

1
2000

Techniki Komputerowe

BIULETYN INFORMACYJNY

INSTYTUT MASZYN MATEMATYCZNYCH
WARSZAWA 2000

P3057/2000

Techniki Komputerowe

BIULETYN INFORMACYJNY

Rok XXXV, Nr 1, 2000

INSTYTUT MASZYN MATEMATYCZNYCH
WARSZAWA 2000

Wydaje:

INSTYTUT MASZYN MATEMATYCZNYCH
UL. KRZYWICKIEGO 34
02-798 WARSZAWA
TEL. 621.84.41, TLX 81.78.80, FAX 629.92.70
E-MAIL: imasmat@imm.org.pl
INTERNET: http://www.imm.org.pl

Copyright © by Instytut Maszyn Matematycznych, Warszawa 2000

Druk: Zakład Poligrafii Ośrodka Przetwarzania Informacji, al. Niepodległości 186

PD 165/03

W listopadzie 2000 r. w Instytucie Maszyn Matematycznych odbyła się ogólnokrajowa konferencja *Metody biometryczne w stystemach identyfikacji i kontroli dostępu*. Niniejszy numer Biuletynu poświęcony jest problematyce podjętej na tej konferencji. Aby ułatwić Czytelnikom zapoznanie się z wygłoszonymi referatami, prezentujemy je w formie aktykułów. Dziękujemy Autorom za dodatkowy trud w ich opracowaniu.

Wszystkie artykuły zostały zrecenzowane przez pracowników naukowych Politechniki Śląskiej.

Redakcja

Warszawa, listopad 2000 r.

TECHNIKI KOMPUTEROWE

Rok XXXIV Nr 1 2000

Spis treści

Str.

Techniki biometryczne. V. Shmerko, Phil Philips, W. Rogers, M. Perkowski, S. Yanushkevich 7

Zastosowanie sieci neuronowych do systemów rozpoznawania twarzy. G. Ososkov, A. Stadnik 31

System modyfikacji kodu elektronicznego podpisu. Agnieszka Janaszek, Andrzej W. Mitas 39

Zastosowanie funkcji rejestru liniowego do osobistej ochrony danych w transmisji informacji. Andrzej Mitas 55

Rejestracja i analiza sygnału akustycznego czynności jelit. Jerzy Sawicki, Adam Podhorski 63

Metody biometryczne w systemach identyfikacji i weryfikacji – techniki, zastosowania, aktualny stan rozwoju. Jan Ryżko, Jerzy Sławiński 71

V. SHMERKO[1], PHIL PHILLIPS[2], W. ROGERS[3],
M. PERKOWSKI[4], S. YANUSHKEVICH[1]
[1)] INSTITUTE OF COMPUTER SCIENCE & INFORMATION SYSTEMS, TECHNICAL UNIVERSITY OF SZCZECIN
[2)] IEE C3 COMMITTEE, NETHERLAW 1, NORTH BERWICK, UNITED KINGDOM
[3)] BIOMETRIC DIGEST, ST.LOUIS, MISSOURI, USA
[4)] FACULTY OF ELECTRICAL ENG., PORTLAND STATE UNIV., PORTLAND, OR, USA

Techniki biometryczne
Biometric technologies

Streszczenie

Wiele metod biometrycznych łączy się ściśle z rozpoznawaniem i analizą obrazów. Referat ten podaje aktualny przegląd rozwoju metod, opracowanych w wielu dziedzinach biometrycznego przetwarzania danych. Niektóre elementy techniki opartej na metodach analizy obrazu zademonstrowane są na przykładzie identyfikacji tęczówki. Z punktu widzenia procesu nauczania, prace laboratoryjne w dziedzinie technik biometrycznych pozwalają stymulować zainteresowanie studentów badaniem metod i algorytmów przetwarzania i rozpoznawania obrazów.

Abstract

Many biometric methods are closely related to methods of pattern recognition and image analysis. The paper gives an overview of many state-of-the-art. methods developed in many spheres of biometric data processing. Some elements of technology based on methods of image analysis are demonstrated by the example of iris person identification. From a position of 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.

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 cause, 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].

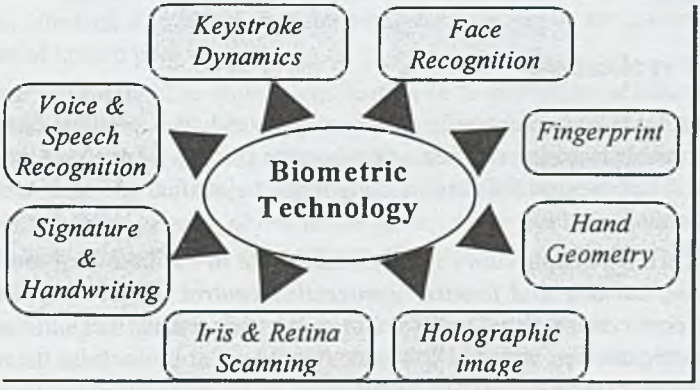


Fig.1. Main directions of modern BTs

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.

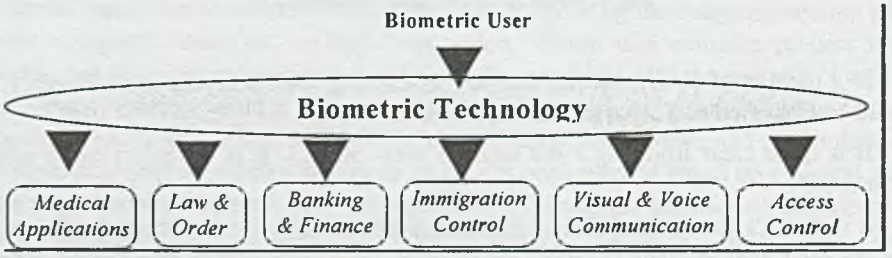


Fig.2. Main modern BT applications

3.1. Signature and handwriting authentification

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 rations 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 sped 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 $5*10^3$ links. The expenditures on the learning phase is $4*10^6$ 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.

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.

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 investigated methods of image processing and patter recognition.

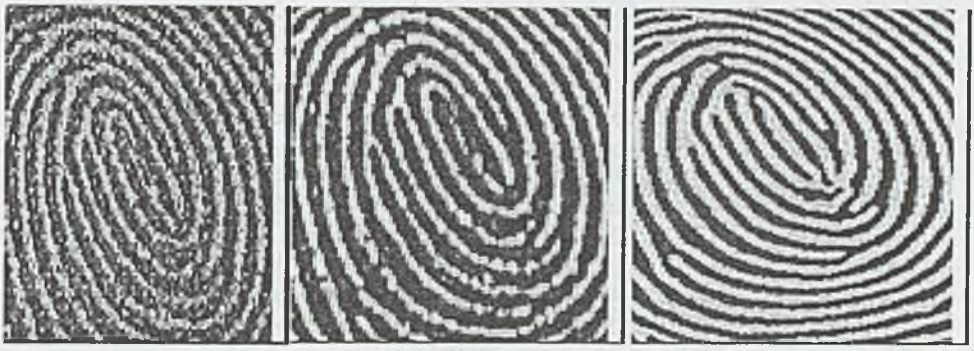


Fig. 4. Illustration of the image processing of fingerprint: input fingerprint: *terminations, bifurcations, trifurcations and undetermined,* and the task is automatically find and extract these feature.

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, resent 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.

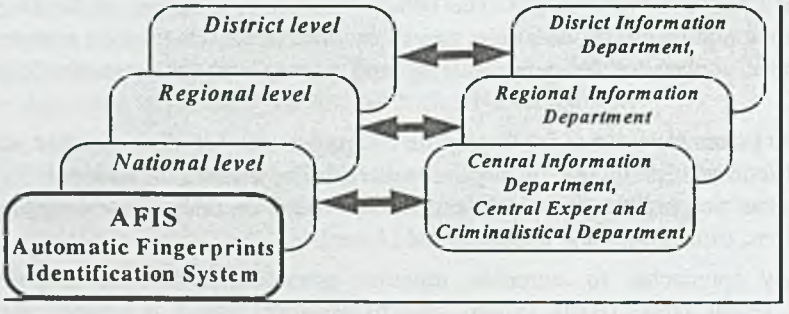


Fig.5. A three levels hierarchical model of its AFIS and representing by reflecting onto fingerprint information flows

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. 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 advertizing, „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 life 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 nonlinear 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.

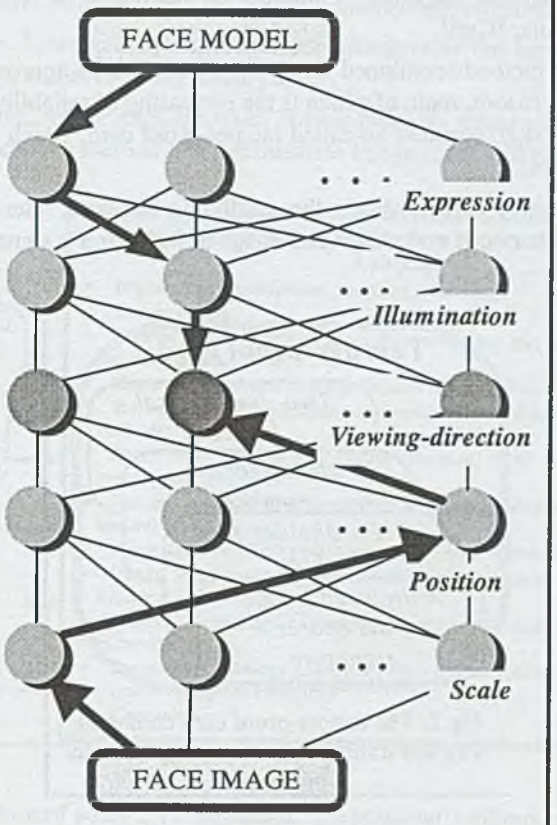


Fig.6. Technology of face image recognition

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).

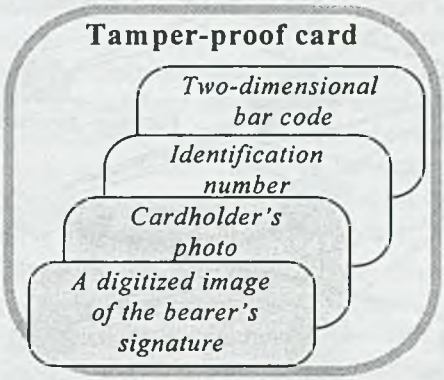


Fig.7. The tamper-proof card combines BTs and traditional person identification approaches

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.

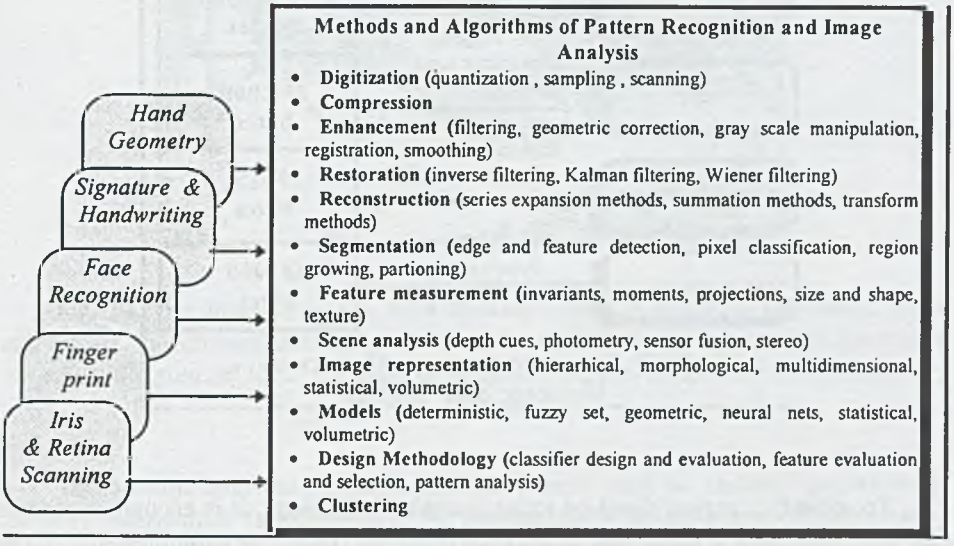


Fig. 8. Implementation of some BTs requires to use practically all modern achievements in image processing and pattern recognition

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.

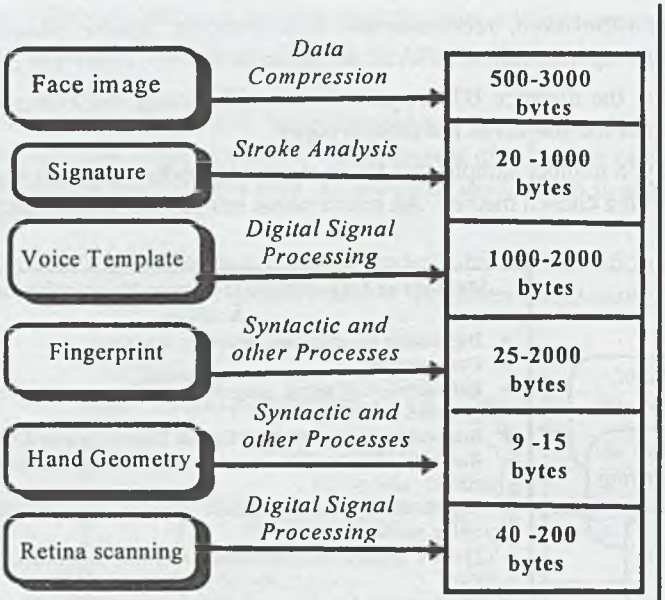


Fig.9. Space requirements for various biometric data storage

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.

5. 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 refereed to a number of methods with raised level of information safety.

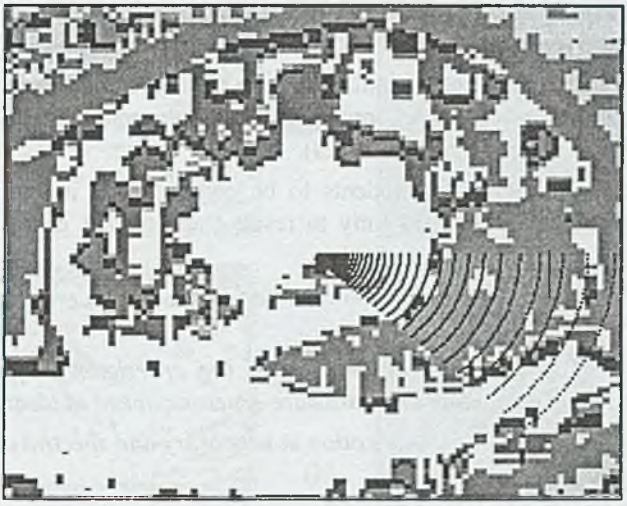


Fig. 10. The image of an eye; on a drawing, one of 8 sectors of the image, which are further transformed into other system of coordinates or into spectral domain is allocated; the glints of light on a pupil of an eye are precisely expressed in the image.

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.

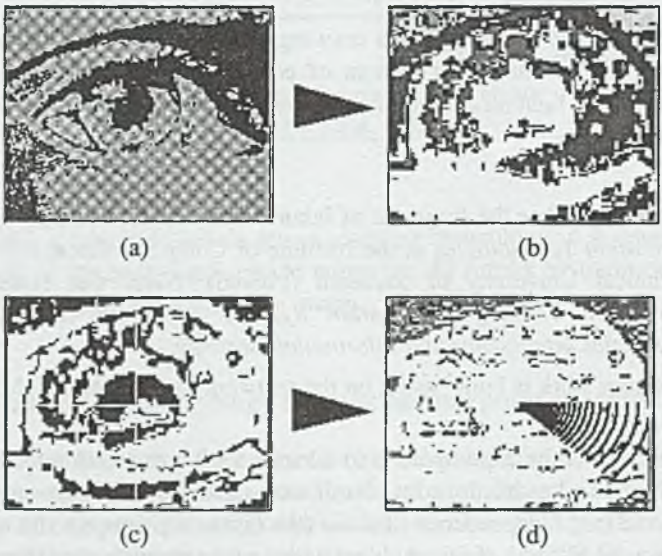


Fig. 11. Elements of processing of the image of an eye: (a) initial image from the videochamber on distance about 1 meter; (b) image increased with the help of software; (c) determination of conditional centre of an eye; (d) division of the image on sectors and transformation of each sector with the purpose of definition statistically of steady attributes.

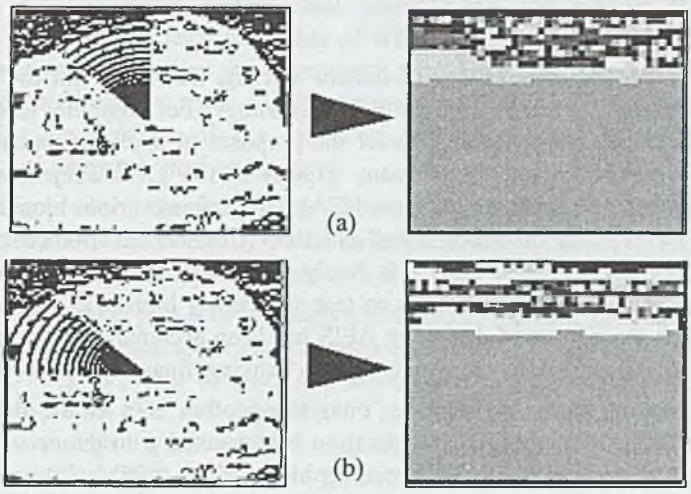


Fig. 12. Transformation of sectors of the image of an eye (the pupil is not allocated) from cartesian in polar system of coordinates: (a) from the eighth sector it is possible to allocate about 20 steady attributes; (b) in the seventh sector are located about 15 attributes, suitable for further processing.

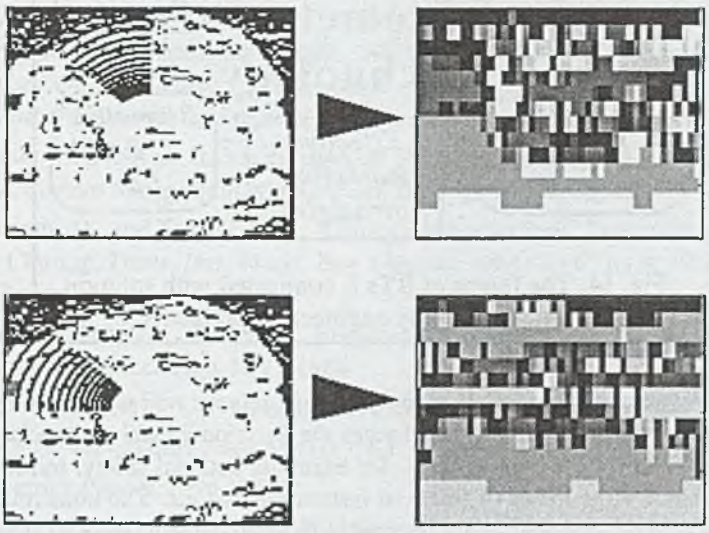


Fig. 13. Transformation of sectors of the image of an eye (the pupil is excluded from sector) from cartesian in polar system of coordinates: in eighth (a) and seventh (b) sectors it is possible to allocate approximately on 30 statistically of steady attributes.

6. 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, larg 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).

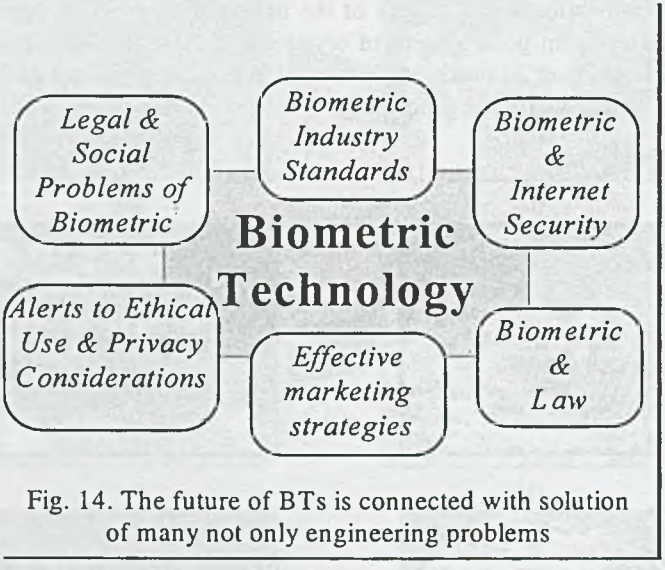


Fig. 14. The future of BTs is connected with solution of many not only engineering problems

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].

7. 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.

References

[1] 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

[2] Ammar M. Progress in Verification of Skillfully Simulated Handwritten Signatures, *Pattern Recognition and Artificial Intelligence,* vol. 5, 1993, pp. 337-351

[3] 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

[4] American National Standards, Fingerprint Identification - Data Format for Information Interchange, N.Y., 1986

[5] *Biometric Digest™ (USA), Ed. William Rogers*, 1996/2000

[6] *Biometric Technology Today™ (UK), Ed. Emma Newham*, 1995/2000

[7] *Biometrics Report, 1996 (UK)*

[8] 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

[9] Chapel C.E., Fingerprint - A Manual of Identification. N.Y., *Coward McCann*, 1971

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] Foltyniewicz R., Automatic Face Recognition via Wavelets and Mathematical Morphology, *Proc. of the 13th Int. Conf. on Pattern Recognition*, vol.2,1966, pp.13-17

[16] 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

[17] 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

[18] 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

[19] 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

[20] Kochergov E., Decision Making System for Handwriting Person Identification Based on Neural Network, *This issue*

[21] Kovalev V., Diakova N., and Bondar Y. On Feature Selection for Face Image Recognition. *In this book*

[22] Kukharev G., Direct and Inverse Transformations of Spectra from Cartesian into Polar System of Coordinates, *Proc. of the Int. Conference Applications of Information Systems - ACS'97, 1997, Szczecin, Poland*

[23] Lee L. L., Berger T., and Aviczer 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

[24] 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

[25] Mechtre B.M., Fingerprint Image Analysis for Automatic Identification, *Mashine Vision and Applications*, vol.6, no.2-3, 1993, pp.124-139

[26] Morgenshtein I. Psycho graphology, *St.Petersburg*, *Publishing House by Vejerman*, 1903 (In Russian)

[27] 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

[28] 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

[29] 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

[30] Polonnikov R., and Korotkov K. (Eds.) Biometric Informatics and Eniology, *St. Petersburg, 'Olga' Publishing House*,1995 (In Russian)

[31] 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

[32] Shmerko V., and Yanushkevich S. (Eds.), *Banking Information Systems,* Technical University of Szczecin, Poland, 1997

[33] 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*

[34] 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.

[35] Shmerko V, Perkowski M., Rogers W., Dueck G., Yanushkevich S., Bio-Technologies in Computing: The Promises and the Reality, *Proc. Int. Conf. on Computational Intelligence & Multimedia Applications,* Australia, 1998, pp.396-409

[36] Tee E.R., and Selvanathan N., Enahancing the Personal Identification Number Input as a Means of Identification Signature. *Malaysian J.Comput. Sci. (Malaysia),* vol.9, no.1, 1996, pp.37-41

[37] 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

[38] 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

[39] Yokoo Y., and Hagiwara M., Human Faces Detection Method Using Genetic Algorithm, *Proc. of 1966 IEEE Int.Conf. on Evolutionary Computation (Japan)*, 1996, pp.113-118

[40] 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

[41] Zhou R.W., and Quck C., An Automatic Fuzzy Neural Network Driven Signature Verification System, *The IEEE Int. Conf. on Neural Networks, Washngton, USA,* vol.2, 1996, pp.1034-1039

G. Ososkov, A. Stadnik
Laboratory of Information Technologies,
Joint Institute for Nuclear Research
DUBNA, RUSSIA

Zastosowanie sieci neuronowych do systemów rozpoznawania twarzy
Neural network application for the face recognition systems

Streszczenie

Zaproponowano nowy typ sieci neuronowych. Są one odpowiednie do bezpośredniej obróbki cyfrowych obrazów twarzy ludzi i wymagają znacznie krótszego okresu uczenia się, aniżeli zwykłe wielowarstwowe perceptrony z algorytmem wstecznej propagacji. Podane są przykłady skutecznych zastosowań do rozpoznawania twarzy ludzi i odręcznych listów. Sporządzono możliwości tolerancji dla różnych zakłóceń obrazu.

Abstract

New type of neural networks is proposed. They are suitable for direct handling of digitized images of human faces and need much less time for training than ordinary multilayer perceptrons with back propagation algorithm. Examples of efficient applications to recognizing of human faces and hand-written letters are given. The tolerance ability to various image distortions was tested.

1. Introduction

The problem of reliable face recognition is of importance and widely explored by various techniques (see, for example [1, 2, 3, 4]). The complexity of this problem leads to very sophisticated hierarchical algorithms. However for some simplier cases, as for frontal view face recognition systems, faster and less complex approaches should be developed. Neural networks (NN) and multilayer perceptrons (MLP), in particular, are very fast means for classifications of complex objects. However MLPs demand a prior procedure of training [5], which is usually realized by the error back propagation (EBP) algorithm and can appear very time consuming. Besides due to tremendous volumes of data after a single face image digitalization they could not be used as a direct input for

MLP. Therefore reports about MLP applications for the frontal face recognition [4] suppose considerable face data preprocessing.

In the given talk a new type of neural networks is proposed. We name them the metric NN. They are suitable for direct handling of digitized images and need much less time for training than ordinary multilayer perceptrons with EBP algorithm. Examples of efficient applications for recognizing of human faces and hand-written letters are given.

2. Problem formulation

Neural network is considered as a mean for the fast recognition of any of a substantial group of human faces. The only frontal views of face images are considered further, which are digitized (by a video-camera, for instance) and stored as 2D raster. It was found that in the majority of cases a raster with not less than 80x100 pixels of 8-bit grey level is efficient to distinguish individual features of a person. To obtain a reliable level of recognizability the NN must be trained before on a training sample of digitized face images of all persons to be recognized. After training NN must adequately recognize any of faces from the sample and undoubtedly indicate any case of a „stranger" face. Network must function in real circumstances when a person can slightly vary its pose, have a minor changes of the face expression, hair-dressing, make-ups, be unshaven etc.

Such the reliability and robustness requirements can be accomplished by including into the training sample more than one face image (up to 10) of the same person.

Next we will study how much the conventional MLP can satisfy such the requirements and what can be modified to fulfil them.

3. Multilayer perceptron and its training problem

A scheme of MLP is shown in Fig.1

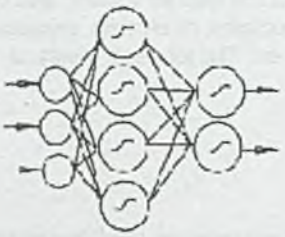


Fig. 1. Scheme of a conventional feedforward three-layer neural network scheme

A neuron is the basic element of any artificial neural network (ANN). It works as:

$$h_j = \sum_k w_{jk}^{(1)} x_k,$$

where x_k are input signals, $w_{jk}^{(i)}$ are the weights of synaptic connections between neu-

rons of i and $i+1$ layers. The output signal of the j-th neuron is $y_j = g(h_j)$, where the activation function $g(x)$ is either a threshold function, or a sigmoid type function, like

$$g(x) = \frac{1}{1+e^x}.$$

In the case of a threshold function and, say two classes, the perceptron attributes the vector x_i to the first class, if $\sum_j w_{ij}^{(2)} h_j \geq 0$, or to the second class, otherwise.

Such a scheme admits the following geometric interpretation (see Fig. 2a): The hyper-plane given by equation $\sum_k w_{ij}^{(2)} h_2 = 0$ divides the space on two half spaces corresponding to classes in question.

If the number of classes is more than two, then several dividing hyper-planes will be defined during the training process.

For the input vector of the classified features $\bar{X}_i$ MLP brings in correspondence an output vector $\bar{Y}_i$. The transformation $\bar{X}_i \Rightarrow \bar{Y}_i$ is completely described by the matrix of synaptic weights to be found as a solution of any concrete problem.

Let us have some training sample as a set of pairs of vectors $\{\{\bar{X}_i^{(m)}\},\{\bar{Z}_i^{(m)}\}\}$. The MLP training is accomplished by minimization of so-called energy function

$$E = \sum_m \sum_i (Y_i^{(m)} - Z_i^{(m)})^2 \Rightarrow min$$

by weights $w_{jk}^{(m)}$ as minimization parameters. Such the EBP method is usually realized by the gradient descent method.

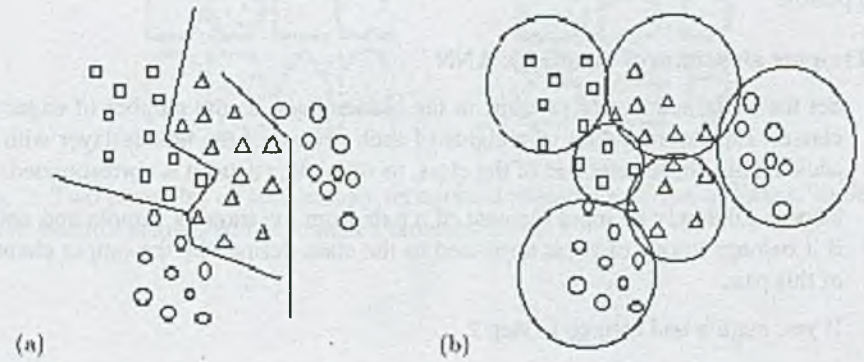


Fig. 2: a) An example of classifying into three overlapped classes by an ordinary MLP. b) Classifying of different feature vectors from the previous example into three classes by the metric ANN.

Arising hindrances:

- "Damnation of dimension" – too high number of weights, i.e. minimization parameters (proportional to number of neurons in power of layers number).
- Arbitrariness in choosing of the hidden layer neurons.
- Difficulties with selecting of the training sample to be long enough to guarantee the correct classification.
- Unlimited time of training procedure and a lack of its convergence guaranty.

4. Proposed ANN design

We propose to replace $\sum_j w_{ij} x_j$ in (1) by

$$\sum_j (x_j - w_{ij})^2.$$

That means we introduce a new L_2^2-type metric in the feature space, i.e. we now classify different classes by covering them with a set of hyperspheres instead of hyperplanes as before (see Fig. 2b).

Thus a metric neural net consists of four layers on neurons with three weight layers between them. The first input layer does not perform any calculations, its neurons just serve to split input signals between neurons of the second layer. The second layer deals with coarsing and averaging of the input signals to transfer them to a feature space. Neurons of the third layer function similarly to Kohonen's neurons (winner-takes-all [5]), i.e. the only one neuron outputs a signal in the case of successful identification, when its input signal exceeds a threshold while all others give zero outputs.

The goal of training is the determination of weight vectors of the second layer and of activation thresholds of the third layer. Neurons of the fourth layer and the third layer of weights make a decision what of faces is closest to the vector of the second weight layer, which is, in fact, an average of features of presented face modifications for the given person.

4.1. Training algorithm of the metric ANN

1. Set the initial number of neurons in the hidden layer as the number of expected classes. Equate the vector of weights of each neuron of the hidden layer with an accidentally chosen element of the class, to which this neuron is corresponded.
2. Choose randomly an input element of a pair from the training sample and check if it belongs to one of areas attributed to the class defined by the output element of this pair.
3. If yes, mark it and then go to step 2.
4. If no, then try to extend the hypersphere radius in order to be able to include this neuron in the area attributed to the given class.
5. Check if some elements of other classes belong to that extended hypersphere.

6. If no, then go to step 2.
7. If yes, than add one more neuron to the hidden layer. Equate the initial weight vector of this neuron with the running input vector. Set up the initial threshold of this new neuron of the hidden layer to a minimal value, which must guarantee that the only given input vector belongs to the new hypersphere, but no one of other elements can appear inside of it.
8. Repeat from step 2, unless the training sample will be exhaust.

What that gives:

- Dynamic change of the number of hidden neurons during the training procedure.
- High speed and finitness of the training process.
- Potential to deal with very large number of neurons.

5. Applications and results

The metric NN described in the previous section was implemented as a C++ program. We started, first, with a simpler task to recognize letters written by computer mouse on the monitor screen. The training sample was also simplified to one of computer fonts. Results (some of them are presented in Fig.3 and 4) were so promising that stimulated our work with the frontal face recognition project.

The program was extended by modules for converting an image into 2D raster format with 80x100 pixels and then to 8000 input neurons. Besides the special means were developed to avoid the full training cycle with every adding a new face to the face bank and fulfil its local changes instead.

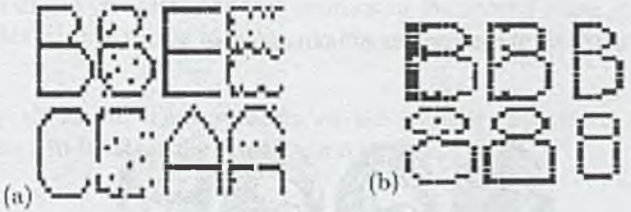


Fig. 3: Two examples of successfully recognized characters. a) Set of letters. b) Second set of various writings of two similar characters B and 8.

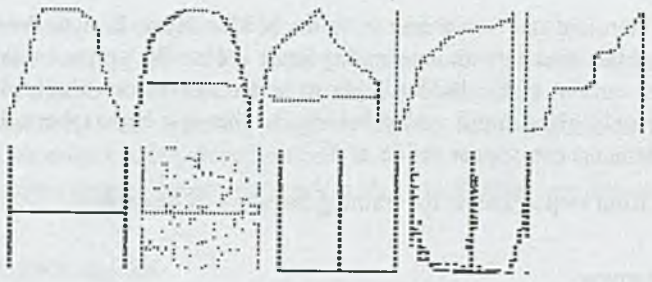


Fig. 4: Imitation of hand-written characters with noise. Metric NN recognizes all characters correctly.

Fig. 5: Training sample of frontal images of human faces.

Fig. 6: Noised or specially distorted faces from the previous set. All them are recognized correctly.

Two sources of face images are used: the face base of the Cambridge University [6] with 10 various frontal face poses of 40 persons and, to be close to reality, face images taken by a digitized video-camera coupled with Pentium-III PC. An example of a training sample of three persons of various age and sex taken by video is shown in Fig.5. Then these images have been considerably noised or specially distorted. Results of correctly recognized images are shown in Fig.6. It was observed that the robustness of the proposed NN to noise and deliberated image distortions directly depends on the number of various modifications of the each face presented in the training sample. The Cambridge face bank was used then for the network training and testing. The recognition efficiency over 95% was achieved. To improve it and also computer memory requirements algorithms for the fast feature extraction are to be incorporated into the system.

6. Conclusion: advantages of the proposed approach

The system was developed for the real time frontal view human face recognition on the low cost basis of Pentium II-like PC coupled with a digitized video-camera. The system implements a new type of the metric neural network. The tolerance ability to various image distortions was tested.

a) High speed and finitness of the training process.

b) Simplicity the classification quality estimation. It is indicated by the number of neurons in hidden layer.

c) Ability to remove non-significant weights after training. If the radius of some hypersphere is small, then corresponding neurons may be deleted from the hidden layer without a serious disturbing of the classification result.

d) Ability to estimate quantitatively an ambiguous situation when one input vector belongs to two di_erent classes. For example, if an input vector activates one neuron of the _rst class and two neurons of the second class, it means that probabilities of this vector to belong to those classes are correspondingly 1/3 and 2/3.

e) Ability to further improvements of the training algorithm, for instance by applying two-levels pattern recognition scheme.

7. Acknowledgements

Authors would like to thank Drs V. Korenkov and J. Slawinski for involving them to the face recognition problem and permanent interest to this work and Dr. L. Rozbicki for the help with the data base information.

References

[1] R. Chellappa et al, *Human and machine recognition of faces: a survey*, Proc. IEEE 83 (5) (1995) 704-740

[2] N. Kruger et al, *Estimation of face position and pose with labeled graphs*, in: Proc. of BMVC (1996)

[3] H. Liu et al, *An automatic human face recognition system*, Opt. and Lasers in Engeneer. 30 (1998) 305-314

[4] K. S. Yoon et al, *Hybrid approaches to frontal view face recognition using the hidden Markov model and neural network*, Pattern Recogn. v. 3, No. 3 (1998) 283-293

[5] P. Wasserman, *Neural computing theory and practice*, Van Nostrand Reinhold, New York (1989)

[6] *ftp://ftp:uk:research:att:com:pub/data/att_faces:zip*

AGNIESZKA JANASZEK
INSTYTUT ELEKTRONIKI,
UNIWERSYTET SZCZECIŃSKI
ANDRZEJ W. MITAS
POLITECHNIKA ŚLĄSKA

System modyfikacji kodu elektronicznego podpisu
The system of the keyword modification in the electronic signature procedure

Streszczenie

W artykule przedstawiono skrótowy opis podstawowych zagadnień związanych z udostępnianiem zasobów informatycznych. Szczególną uwagę poświecono w dalszej części problematyce elektronicznego podpisu. W artykule przypomniano podstawowe zagadnienia z zakresu generatorów liczb pseudoprzypadkowych. W kontekście teorii dzielenia wielomianów nad ciałem GF2 przedstawiono koncepcję modyfikacji hasła za pomocą wyjściowych sekwencji generatora MVL. Zastosowanie kodowania liniowego wielowartościowymi sekwencjami umożliwia istotną modyfikację hasła dostępu do zasobów informatycznych.

Abstract

In the paper is presented a short discussion of the basic questions that are joined with the access to the information sets. A special attention is paid to the electronic signature. In the paper are remembered some crucial problems of the pseudorandom pattern generation. In the context of the polynomial division over the field GF2 is a concept of the keyword modification with the output sequences of the MVL-generator. The application of the linear MVL coding makes possible an essential modification of the keyword.

WSTĘP

Mimo najdoskonalszych zabezpieczeń zawsze istnieje możliwość naruszenia bezpieczeństwa systemu. Jest to tylko kwestią czasu. Określenie sieci mianem bezpiecznej oznacza, że zainstalowane zostały mechanizmy, które ograniczają zakres większości zagrożeń dla jej zasobów.

Kryptografia jest powszechnie stosowanym narzędziem zapewniającym ochronę danych poprzez szyfrowanie. Jest procesem przetwarzania danych w sposób uniemożliwiający ich odczytanie przez osoby niepowołane. W większości mechanizmów

kryptograficznych do odkodowania informacji wymagane jest podanie hasła lub klucza [1].

Transmisja informacji, odbywająca się wieloma różnymi trasami w sieci, narażona jest na podsłuch (ma to miejsce np. w Internecie), aby temu zapobiec tworzone są specjalne kanały, którymi przesyłane są dane w postaci zaszyfrowanej. Deszyfracja odbywa się dopiero w komputerze docelowym. Informacje zabezpieczone przy pomocy szyfrów pozostają nieczytelne dla osób nie posiadających właściwego klucza deszyfrującego.

Kryptografia umożliwia uwierzytelnienie, integralność oraz poufność przesyłanych informacji.

Szyfrowanie informacji stosowane jest między innymi w:

1) sieciach komputerowych, w takich przypadkach jak:
   a. ochrona danych przed niepowołanym odczytem;
   b. uwierzytelnianie dokumentów;
   c. ochrona prywatności poczty elektronicznej;
2) telefonii komórkowej, gdzie niezbędnym elementem w nawiązaniu połączenia jest ustalenie tożsamości abonenta;
3) bankach, bankomatach;
4) kodowanej telewizji cyfrowej;
5) wszędzie tam, gdzie nieodzownym elementem jest zagwarantowanie tajności informacji.

PROBLEMY WIELODOSTĘPU

Fundamentalnym zagadnieniem bezpieczeństwa systemów komputerowych jest kontrola dostępu. Celem kontroli jest ograniczenie praw użytkowników do korzystania z systemu komputerowego zgodnie z uprawnieniami, jakie zostały im nadane przez administratora. Wyróżnia się dwa rodzaje kontroli dostępu:

- do systemu komputerowego;
- do obiektów tego systemu.

Kontrola dostępu do systemu komputerowego oparta jest na uwierzytelnianiu „użytkownika" przez innego „użytkownika" poprzez analizę cech charakterystycznych. Pod pojęciem „użytkownik" może występować człowiek, komputer, terminal, karta sprzętowa itp. Rozróżnia się trzy metody uwierzytelniania:

- ***SYK*** (ang. *by something you know*) – polega na sprawdzaniu przez system informacji, którą posiada użytkownik, może to być np. hasło lub PIN-kod. Wadą tego rozwiązania jest brak gwarancji, że hasło w istocie należy do użytkownika, który się nim posługuje. Zaletą tej metody jest łatwość w stosowaniu oraz wygoda dla użytkowników.
- ***SYH*** (ang. *by something you have*) – polega na sprawdzaniu tego, co użytkownik ma, może to być karta magnetyczna, karta mikroprocesorowa, klucz elektroniczny. Zaletą tego rozwiązania jest fakt, że próba sfałszowania kart wymaga zaangażowania środków finansowych i technologicznych. Wadą jest wrażliwość kart na oddziaływanie pól elektromagnetycznych. Dodatkowo utrata karty uniemożliwia uprawnionemu użytkownikowi dostęp do systemu.

- *SYA* (ang. *by something you are*) – jest kompromisowym rozwiązaniem obu powyższych metod, zwiększając w ten sposób bezpieczeństwo kontroli dostępu. Metoda ta polega na rozpoznawaniu cech charakterystycznych człowieka na podstawie metod biometrycznych lub antropometrycznych. Zaletą tego rodzaju uwierzytelniania jest niepowtarzalność cech charakterystycznych oraz wygoda użytkownika. Wadą natomiast jest konieczność posiadania bardzo skomplikowanych i kosztownych urządzeń rozpoznających, konieczność przechowywania dużej ilości informacji, skomplikowany program rozpoznający oraz zawodność. Urządzenia tego typu nie są przez to powszechnie stosowane. Istotnym problemem jest margines tolerancji urządzeń rozpoznających. Urządzenia te nie powinny odrzucać użytkownika uprawnionego, a jedynie nieuprawnionego.

Kontrola dostępu do obiektów systemu komputerowego. Wyróżnia się następujące rodzaje kontroli dostępu do obiektów systemu:
- swobodna;
- obowiązkowa;
- zależna od zadań.

NIEBEZPIECZEŃSTWA

Bardzo ważnym aspektem bezpieczeństwa systemu jest bezpieczeństwo haseł. Słaby system zabezpieczeń prowadzi do zupełnego otwarcia systemu, poprzez atak na hasło.

Atak na hasło jest terminem opisującym różne czynności, których celem jest ominięcie mechanizmów ochrony systemu komputerowego opartego na systemie haseł, a więc wszelkie próby złamania, odszyfrowania lub skasowania haseł [1]. Początkowo może mieć miejsce uzyskanie ograniczonego dostępu do komputera. Następnie mamy do czynienia z atakiem na słabo zabezpieczone hasła. W konsekwencji może dojść do przejęcia całkowitej kontroli nawet nad kilkoma systemami komputerowymi. Łamanie haseł nie jest z reguły rzeczą trudną. W tym celu używa się gotowych programów.

System zabezpieczeń haseł ma szczególne znaczenie w sieciach rozległych z dostępem do Internetu, ponieważ narażony jest na ataki anonimowych osób o dowolnej porze.

Zabezpieczanie haseł w systemie możliwe jest poprzez:
- instalację systemu maskowania haseł;
- zabezpieczanie haseł wykorzystywanych w aplikacjach;
- utrudnianie ataku na hasła;
- kreowanie efektywnych reguł tworzenia i wykorzystywania systemu haseł;
- korzystanie z zaawansowanych programów narzędziowych wyszukujących luki w systemie haseł.

Najprostszą metodą łamania haseł w systemach operacyjnych są ataki słownikowe. Atak polega na przechwyceniu pliku zawierającego zakodowane hasła. Do złamania haseł wykorzystuje się specjalne, szybkie programy, których zadaniem jest zaszyfrowanie każdego słowa znajdującego się w słowniku przy pomocy odpowiednich algorytmów. Każde nowo tworzone hasło (zaszyfrowane słowo) porównywane jest z hasłem

wzorcowym z pliku, do czasu aż oba szyfry będą identyczne. Taki atak ma na celu znalezienie dowolnego hasła, które umożliwi wejście do systemu, a następnie uzyskanie praw operatora systemu (root). Atak słownikowy opiera się na zjawisku występowania słabych haseł, wybieranych zwykle przez początkujących użytkowników.

Ochrona haseł przed atakami

Aby bronić się przed tymi atakami należy stosować między innymi system maskowania haseł oraz programy do symulacji ataków na hasła użytkowników. W momencie, gdy użytkownik tworzy nowe hasło, jest ono poddawane testowaniu w oparciu o listę słów i zestaw reguł. W przypadku złamania hasła, żąda się od użytkownika zmiany hasła na nowe. Takie postępowanie umożliwia eliminację słabych haseł zanim pojawią się w plikach przechowujących informacje o kontach użytkowników.

UTRATA PRYWATNOŚCI

Jednym z kluczowych zagadnień w zakresie zapewnienia bezpieczeństwa w systemach komputerowych jest problem uwierzytelniania. Musi istnieć możliwość stwierdzenia, czy osoba podająca się za określonego użytkownika jest nim w istocie. Najbardziej rozpowszechnionym sposobem uwierzytelniania jest podanie tajnego hasła.

Początkowo szyfry były dość proste. W ciągu zaledwie kilku godzin lub co najwyżej kilku dni można było odgadnąć zastosowany algorytm. Dopiero pojawienie się komputerów zapoczątkowało prawdziwy rozkwit kryptografii. Jednym z popularniejszych szyfrów jest DES (*Data Encryption Standard*).

Łatwość łamania zakodowanych haseł jest spowodowana dwoma podstawowymi czynnikami:
- czynnik ludzki – charakterystyczne, słabe hasła;
- ograniczona długość klucza.

Użytkownicy powinni przestrzegać podstawowych reguł dotyczących bezpieczeństwa systemu haseł. Do najczęściej popełnianych błędów przez użytkowników można zaliczyć:
- posługiwanie się tym samym hasłem dostępu do kilku aplikacji i serwerów;
- wybieranie prostych lub bardzo podobnych do siebie haseł;
- obawy, czy aby nie zapomną swoich haseł.

ZABEZPIECZENIA BIOMETRYCZNE

Zabezpieczenia biometryczne są nową dziedziną naukową. Kierunkiem badań jest opracowanie takich metod weryfikacji tożsamości użytkownika, aby w każdych warunkach dawały stuprocentowy wynik autoryzacji. Dostęp ograniczany jest przy użyciu urządzeń kontrolujących według biologicznej charakterystyki użytkownika np.:
- zapachu ciała;
- rysów twarzy;
- odcisków palców;
- wyglądu siatkówki lub tęczówki oka;
- barwy głosu.

Jedną z powszechnie stosowanych metod identyfikacji biometrycznej osób jest analiza porównawcza odcisków palców. Do niedawna technologia badania odcisków

palców była prymitywna. Odciski odbijało się na papierze i w takiej formie przechowywano w celu późniejszego wizualnego porównania. Dzisiaj odciski zapisywane są w specjalnym standardzie kompresji. W celu cyfrowego przetworzenia odcisków palców pobierane są one przez kamerę, a następnie poddawane autoryzacji podczas logowania się użytkownika do systemu. Komputer pozwala w łatwy i szybki sposób porównać zgromadzone dane z zadanym wzorcem i wyszukać ten najbardziej podobny. W celu identyfikacji, do kogo należy dany odcisk palca, wystarczy porównać od 8 do 16 punktów próbek. Są jednak osoby, u których na skutek różnych chorób odciski palców są albo cząstkowe, albo nie ma ich wcale.

Inną metodą umożliwiającą jednoznaczną identyfikację osoby jest badanie siatkówki oka. Siatkówka składa się z kilku warstw. Badanie odbywa się za pomocą specjalnego skanera. Analiza wyglądu zaledwie dwóch warstw pozwala na uzyskanie dużej pewności otrzymanego wyniku. Metoda ta staje się jednak nieskuteczna, gdy dana osoba jest niewidoma lub ma kataraktę. Urządzenia skanujące siatkówkę oka mają duży współczynnik odrzucenia, co oznacza, że nawet upoważnieni użytkownicy mogą nie uzyskać autoryzacji przy pierwszym podejściu. Dodatkowym problemem jest ochrona prywatności badanych osób. Przeprowadzone badania wykazały, że obraz siatkówki oka zawiera wiele informacji o zdrowiu człowieka (ślady zażywania narkotyków, AIDS).

Możliwa jest również identyfikacja za pomocą głosu. Jednak system taki może być niewiarygodny, gdy np. badana osoba jest przeziębiona lub ma zachrypnięty głos.

Biometryczne urządzenia stosowane w kontroli dostępu mają swoje wady i zalety. Ich stosowanie wiąże się z totalną personalizacją dostępu. Najmniejsza nawet zmiana biologicznej charakterystyki użytkownika wyklucza jego autoryzację. Powstaje wówczas problem ludzi niezastąpionych w danym, krytycznym momencie. Innym problemem jest złożoność i koszt aparatury używanej do identyfikacji osób. Bardzo wysoki koszt wyklucza powszechne stosowanie tych urządzeń. Niepodważalny jest jednak fakt, że jak dotąd nie udało się opracować innych metod, które dawałyby tak duży stopień wiarygodności. Metody te charakteryzują się niezwykłą dokładnością. Urządzenia tego typu są doskonałe w zastosowaniach domowych, w biurach, zamkniętych oddziałach. Nie sprawdzają się jednak poza siecią lokalną. W sieciach rozległych nie ma możliwości zdalnej identyfikacji logującego się użytkownika przy wykorzystaniu urządzeń biometrycznych.

TECHNIKI KODOWANIA

Mechanizmy kryptograficzne do szyfrowania danych używają algorytmów oraz kluczy. Algorytmy są znane i dostępne. Klucz jest cyfrowym kodem zapewniającym bezpieczeństwo, który może być użyty do zaszyfrowania, rozszyfrowania oraz podpisania informacji [2]. Im więcej jest możliwych wartości klucza, tym trudniej jest go złamać. Optymalnym rozwiązaniem byłoby używanie najdłuższego dostępnego klucza. Ze względu na własności kluczy rozróżnia się następujące metody szyfrowania:

- szyfrowanie symetryczne;
- szyfrowanie asymetryczne;
- jednokierunkowe funkcje mieszające (*hash functions*).

Szyfrowanie symetryczne (kodowanie kluczem tajnym) – klucz do kodowania i dekodowania wiadomości jest ten sam. Obecnie do bardziej znanych algorytmów z tajnym kluczem należą:
- DES (*Data Encryption Standard*);
- 3DES – trzykrotny DES;
- IDEA (*International Data Encryption Algorithm* – międzynarodowy algorytm szyfrowania danych);
- RC5.

Szyfrowanie asymetryczne (kodowanie kluczem jawnym) – do szyfrowania oraz deszyfrowania danych wykorzystuje się dwa klucze: jawny – publiczny, prywatny – tajny. Klucze nie są ze sobą powiązane. Do popularnych algorytmów z kluczem publicznym należą:
- RSA – algorytm Rivesta, Shamira i Adlemana;
- algorytm ElGamala.

Jednokierunkowe funkcje mieszające – do szyfrowania danych wykorzystuje się funkcje mieszające, które pobierają wiadomość wejściową o danej długości i generują kod o stałej długości. Do popularnych funkcji mieszających należą:
- algorytm MD4 (Message Digest 4) [2];
- algorytm MD5 (Message Digest 5) [2];
- SHA (*Secure Hash Algorithm – algorytm bezpiecznego mieszania*) [3].

ELEKTRONICZNY PODPIS

Cyfrowy podpis jest elektronicznym identyfikatorem, używanym w celu zapewnienia integralności oraz potwierdzenia tożsamości nadawcy. Za najważniejsze własności podpisów cyfrowych uważa się, że [3]:
- jedynie osoba X może utworzyć podpis osoby X (podrobienie podpisu powinno być niewykonalne);
- powinna być zapewniona możliwość jednoznacznego stwierdzenia, czy podpis został złożony pod danym dokumentem (kopiowanie podpisu powinno być niewykonalne).

Podpis cyfrowy oparty jest na kombinacji szyfrowania kluczem publicznym oraz algorytmów jednokierunkowych bezpiecznych funkcji mieszających.

Wyróżniamy trzy odrębne czynności związane z podpisami cyfrowymi:
- ***czynności wstępne*** polegające na wyznaczeniu niezbędnych parametrów, za pomocą których generowane będą podpisy;
- ***generowanie podpisu*** – osoba podpisująca dokonuje obliczeń, w trakcie których powstaje ciąg bitów będący podpisem konkretnego dokumentu;
- ***weryfikacja podpisu*** – czynność umożliwiająca jednoznaczne stwierdzenie autentyczności podpisu.

Do kilku bardziej znanych algorytmów umożliwiających tworzenie cyfrowych podpisów należą:
- algorytm RSA;
- algorytm ElGamala;
- algorytm DSA.

GENERATORY LICZB PSEUDOLOSOWYCH DO TWORZENIA PODPISÓW

CIĄGI PSEUDOLOSOWE

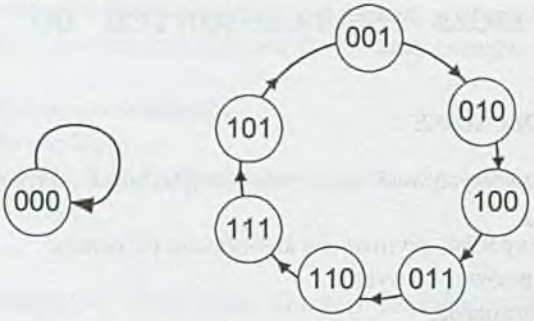
Ciągi losowe wykorzystywane są w wielu algorytmach kryptograficznych. Oto niektóre przykłady [3]:
- generowanie kluczy RSA, szyfrowanie algorytmem ElGamala;
- generowanie podpisów cyfrowych;
- protokoły kryptograficzne;
- „one-time pad" i pokrewne mu szyfrowanie strumieniowe.

Ciągi pseudolosowe, by mogły być stosowane w kryptografii, powinny być:
- ***nierozróżnialne*** – ciągi pseudolosowe nie powinny być rozróżnialne od ciągów losowych przy użyciu żadnych dostępnych metod;
- ***nieprzewidywalne*** – oznacza, że bez znajomości parametrów generatora nie można obliczyć s_i, *i*-tego bitu ciągu pseudolosowego, z bitów s_1, ..., s_{i-1}.

Ciągi pseudolosowe mają wszystkie właściwości ciągów losowych, ale jednocześnie mogą być wygenerowane w sposób deterministyczny. Losowym elementem ciągu pseudolosowego jest ciąg inicjujący. Kolejne ciągi tworzone są w ten sposób, że *i*-ty element s_i jest wyznaczany przez pewien deterministyczny algorytm z ciągu inicjującego, indeksu *i* oraz wartości s_1, ..., s_{i-1}. Ważne jest, aby ciąg był na tyle długi, by wykluczyć możliwość jego odtworzenia poprzez przeglądanie wszystkich możliwych ciągów i sekwencji.

PSEUDOLOSOWY GENERATOR BINARNY

Rejestr liniowy ze sprzężeniem zwrotnym (***Linear Feedback Shift Register – LFSR***) składa się z *n* przerzutników mogących zapamiętać ciąg bitów oraz bramki XOR, wykonującej operacje sumy modulo 2 na wybranych bitach znajdujących się w rejestrze. Do rozpoczęcia pracy LFSR potrzebny jest ciąg inicjujący, który ma postać ciągu losowego. Podczas jednego cyklu zegarowego z wyjść przerzutników określonych sprzężeniem zwrotnym, pobierane są wartości, które następnie są sumowane modulo 2. Obliczona w ten sposób wartość wstawiana jest na pozycji pierwszego przerzutnika, która zwolniła się po przesunięciu pozostałych bitów o jedną pozycję w prawo. Ciągi pseudolosowe generowane przez rejestr LFSR o długość *n*, są ciągami okresowymi, o okresie maksymalnym $N = 2^n-1$ bitów. Generator cyklicznie przechodzi przez wszystkie swoje stany, za wyjątkiem stanu zerowego. Jeżeli generator znalazłby się w stanie zerowym, wówczas pozostałby w nim nieskończenie długo, gdyż wartość sygnału wejściowego do generatora równa jest 0. Dlatego też generatory, w których ciąg wyjściowy ma okres $N = 2^n-1$ bitów, nazywane są także generatorami ciągów o maksymalnej długości (ang. *maximum length sequence generator*). Poniżej przedstawiony został cykl pracy 3-bitowego rejestru LFSR.



Rys. 1. Graf pracy 3-bitowego rejestru LFSR

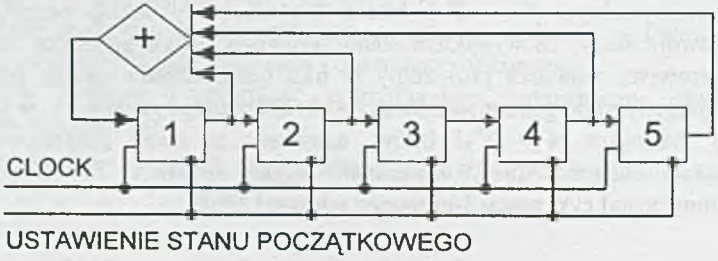
Ciąg wyjściowy z generatora ciągów o maksymalnej długości posiada szereg cech upodabniających go, w pewnym zakresie, do idealnego ciągu losowego:

- w dowolnym okresie o długości N, liczba jedynek wynosi $N/2$, a liczba zer wynosi $N/2-1$ (ponieważ stan zerowy został wykluczony),
- w dowolnym okresie o długości N, liczba pojedynczych jedynek jest dwukrotnie większa niż liczba podwójnych jedynek, czterokrotnie większa niż liczb potrójnych jedynek itd.,
- funkcja autokorelacji $R(k)$ ciągu pseudolosowego przyjmuje dwie wartości: 1 dla wszystkich k będących wielokrotnościami N oraz wartość $1/N$ dla pozostałych k (k – liczba pozycji przesunięcia danego ciągu).

LFSR generuje sekwencje bitów bardzo szybko, pod warunkiem, że odbywa się to sprzętowo. Dane literaturowe [3] wskazują iż kryptograficzne własności ciągów generowanych przez LFSR są relatywnie słabe.

GENERATOR PSEUDOLOSOWY MVL

Innym rozwiązaniem dedykowanym poprawne własności kryptograficzne jest rejestr LFSR zbudowany z bramek wielowartościowych. Generowanie ciągów MVL odbywa się bardzo podobnie jak przy tworzeniu ciągów z wykorzystaniem binarnego rejestru LFSR. Z poszczególnych stopni rejestru pobierane są aktualne stany przerzutników, według wcześniej określonych sprzężeń. Pobrane wartości są sumowane modulo v. Reszta z dzielenia wstawiana jest na pozycji najbardziej znaczącego stopnia. Na rysunku 2 przedstawiony został schemat generatora MVL.



Rys. 2. Schemat generatora MVL

SZYFROWANIE HASEŁ PRZY UŻYCIU GENERATORA MVL

Do określenia konstrukcji generatora MVL liczb pseudoprzypadkowych potrzebne są takie parametry jak:
- długość rejestru (generatora),
- rodzaj sprzężenia,
- ciąg inicjujący,
- parametr v (liczba poziomów logicznych).

Jeżeli przyjęlibyśmy, że parametry takie mógłby podać użytkownik, to przykładowe hasło musiałoby składać się z dość długiego ciągu cyfr. Sytuacja taka jest dość kłopotliwa zwłaszcza, że potencjalni użytkownicy przyjmują z reguły relatywnie trywialne hasła. Z drugiej strony pojawia się pytanie, jak zapamiętać długi ciąg cyfr? Lepszym rozwiązaniem wydaje się możliwość wpisywania hasła w postaci normalnego tekstu np. „Ala125", który łatwiej skojarzyć i zapamiętać. W celu uzyskania z danego tekstu ciągu cyfr, pomocne będą kody ASCII. Odczytane i zapisane kody poszczególnych znaków utworzą ciąg cyfr. Np. kody znaków hasła: „Ala125" mają następujące wartości: 'A'-65, 'l'-108, 'a'-97, '1'-49, '2'-50, '5'-53, pozwalają uzyskać ciąg cyfr postaci: 6510897495053. Jedynym ograniczeniem, jakie należałoby przyjąć dla wpisywanych haseł, jest ich długość. Im hasło jest dłuższe tym dłuższy jest wynikowy ciąg cyfr, a tym samym trudniej jest je rozszyfrować. Hasło składające się z mniej niż trzech znaków nie pozwala uzyskać wystarczająco długiego ciągu, z którego następnie pobierane są parametry do pracy generatora MVL.

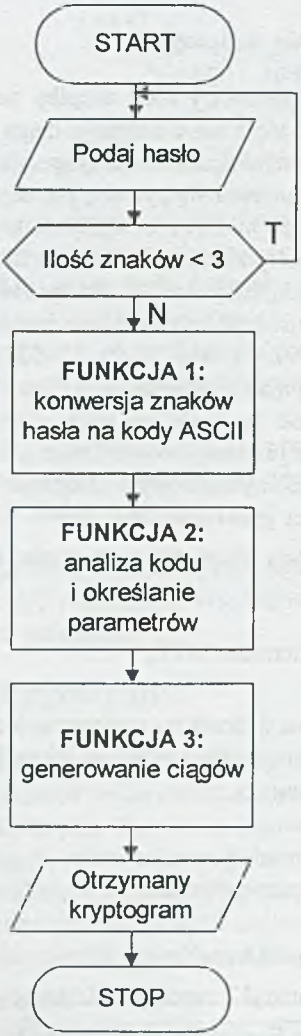
Na rysunku 3 przedstawiony został algorytm szyfrujący MVL. Jest on zbudowany z trzech części:
1) konwersji hasła,
2) określenia parametrów generatora MVL,
3) generacji ciągów MVL.

Funkcja 1 dokonuje konwersji hasła na wspomniany ciąg cyfr. Zadaniem Funkcji 2 jest poddanie analizie otrzymanego ciągu cyfr i na jej podstawie określenie parametrów potrzebnych do pracy generatora:
- n – długość generatora;
- s – zewnętrzne sprzężenie zwrotne;
- p – ciąg rozpoczynający pracę generatora;
- v – parameter MVL;
- z – ilość zmieniających się sekwencji.

Szczegółowy algorytm Funkcji 2 został przedstawiony na rys. 4.

Ciąg cyfr zwrócony przez Funkcję 1 zostaje zapisany do tablicy. Z tablicy pobierana jest pierwsza wartości, w celu przypisania jej pod zmienną z, określającą ilość generowanych sekwencji. Im liczba ta jest większa tym generowane ciągi pseudolosowe bardziej upodobniają się do ciągów losowych. Funkcja 2 zapewnia, aby wartość z nie była mniejsza od 2. Pozostały w tablicy ciąg cyfr dzielony jest na pół i przypisany pod zmienne: s i p. Jeżeli pozostała w tablicy ilość cyfr nie jest parzysta, to dłuższy ciąg przypisywany jest pod zmienną p, określającą stan początkowy pracy generatora. Na podstawie zmiennej tablicowej p obliczana jest:

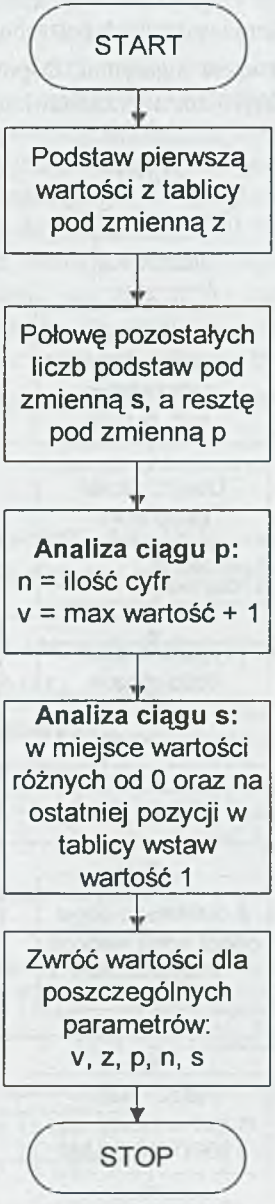
- wartość n określająca długość generatora tj. ilość przerzutników mogących pomieścić zadeklarowany ciąg inicjujący. Wartość ta jest równa ilości cyfr znajdujących się w tablicy p;
- wartość v określająca parametr MVL. Wartość ta równa jest maksymalnej wartość znajdującej się w tablicy, powiększonej o jeden.



Rys. 3. Algorytm szyfrowania haseł za pomocą generatora MVL

Zmienna s potrzebna jest do wyznaczenia, z których przerzutników będą pobierane wartości, tj. do określenia sprzężenia. Założono zewnętrzne sprzężenie zwrotne. Sposób opisu sprzężenia przedstawiany jest jako ciąg binarny, gdzie 1 oznacza występowanie sprzężenia, a 0 jego brak. Na podstawie cyfr znajdujących się w tablicy zmiennej s

możemy przyjąć, ze tam gdzie wartość jest różna od zera wstawiamy 1, w ten sposób uzyskujemy potrzebny ciąg binarny. Ważne jest również, aby ostatni element w tablicy, odpowiadający ostatniemu przerzutnikowi, z którego zawsze wyprowadzane jest sprzężenia miała wartość 1, ponieważ jest to równoważne definicji długości rejestru.



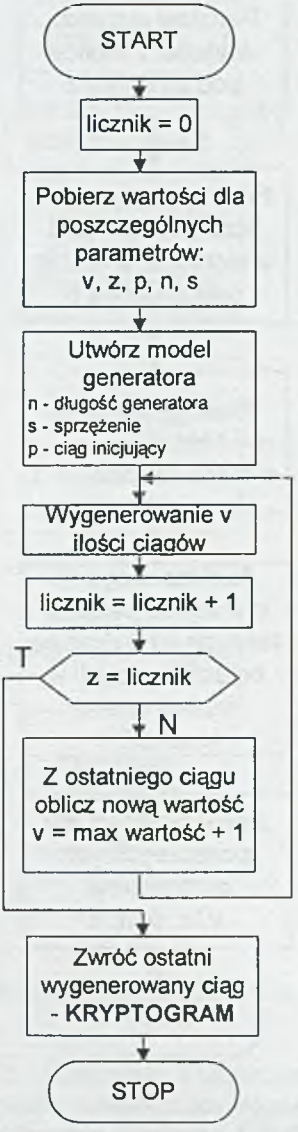
Rys, 4. Algorytm Funkcji 2 (określenie parametrów generatora MVL)

Maksymalna długość sekwencji ciągu jest ściśle związana z wyborem przerzutników do sprzężenia. Ponieważ zależy nam, aby generowane ciągi pseudolosowe były jak najbardziej podobne do ciągów losowych, stąd w algorytmie założono, że:

- różna będzie ilość generowanych sekwencji (zależna od parametru z);
- generowane sekwencje będą miały różną ilość ciągów (zależną od parametru *v*).

Funkcja 2 umożliwia określenie wszystkich potrzebnych parametrów.

Funkcja 3 stanowi główną część algorytmu. Odpowiada za generowanie ciągów pseudolosowych. Algorytm Funkcji 3 został przedstawiony na rys. 5.



Rys. 5. Algorytm Funkcji 3 (generowanie ciągów)

Na wejściu funkcja pobiera parametry zwracane przez Funkcję 2, tj.: v, z, p, n, s. W celu utworzenia modelu generatora MVL pobierane są wartości:

- n – określenie długości rejestru;
- s – z których przerzutników będą wyprowadzone sprzężenia;
- p – ciąg inicjujący pracę generatora.

Generowanie ciągów odbywa się w następujący sposób: z przerzutników określonych parametrem s, pobierane są wartości, które są sumowane modulo v. Uzyskana wartość wstawiana jest na pozycji najbardziej znaczącego stopnia, a pozostałe wartości przesuwane są w prawo. Wygenerowany ciąg jest pierwszym ciągiem danej sekwencji. Zakłada się, że każda sekwencja będzie składała się z v ciągów. Z ostatniego ciągu danej sekwencji określana jest maksymalna wartość, która po zwiększeniu o jeden wyznaczana nową wartość parametru v, należącego do przedziału {2...10}, w wyniku czego generowane cyfry należeć będą do przedziału {0...9}. Od tego momentu rozpoczyna się generowanie drugiej sekwencji, składającej się z v ciągów w oparciu o nową wartość v. Ilość wygenerowanych sekwencji, jest zależna od parametru z, który określa, kiedy generator ma zaprzestać działanie. Po przejściu z sekwencji zwracany jest ostatni wygenerowany ciąg, który jest kryptogramem danego hasła.

Działanie algorytmu szyfrującego MVL ilustruje poniżej przedstawiony przykład.

PRZYKŁAD

Konwersja hasła

Przyjmijmy, że nasze hasło ma postać: „Ala125"

Na podstawie kodów ASCII odczytywane są kody dla poszczególnych znaków i zapisywane jak ciąg cyfr.

Kody dla znaków hasła: A-65, l-108, a-97, 1- 49, 2-50, 5-53.

Uzyskany ciąg cyfr: 6510897495053

Określanie parametrów generatora

Ciąg zostaje zapisany do tablicy tabMVL:

6	5	1	0	8	9	7	4	9	5	0	5	3
1	2	3	4	5	6	7	8	9	10	11	12	13

Z tablicy pobierana jest pierwsza wartości: z = 6 (co oznacza, że wygenerowanych). zostanie 6 sekwencji

W tablicy tabMVL pozostają następujące wartości:

5	1	0	8	9	7	4	9	5	0	5	3
1	2	3	4	5	6	7	8	9	10	11	12

Tablica dzielona jest na pół i zapamiętywana jest pod zmiennymi tablicowymi p i s.

p

5	1	0	8	9	7
1	2	3	4	5	6

W tablicy s wartości różne od zera zastępowane są 1.

s

4	9	5	0	5	3
1	2	3	4	5	6

$\Rightarrow$

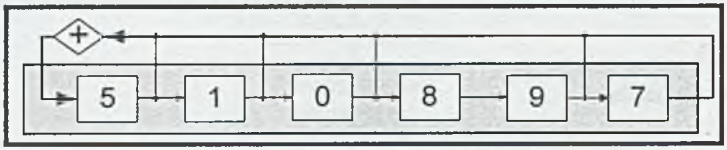
1	1	1	0	1	1
1	2	3	4	5	6

Tabela 1 Uzyskane parametry

Uzyskane parametry:	
Długość generatora	$n = 6$
Zewnętrzne sprzężenie zwrotne	$s = 111011$
Ciąg rozpoczynający pracę generatora	$p = 510897$
Parametr MVL	$v = 10$
Ilość zmieniających się sekwencji	$z = 6$

Generowanie sekwencji MVL

Generator zbudowany jest z $n = 6$ przerzutników. Posiada zewnętrzne sprzężenie zwrotne określone parametrem $s = 111011$. Zero na czwartej pozycji oznacza brak sprzężenia na czwartym przerzutniku. Ciąg rozpoczynający pracę generatora zostaje ustawiony na $p = 510897$.



Rys. 6. Schemat utworzonego generatora MVL

W tabeli 2 przedstawiony został przykładowy przebieg generowanych ciągów w sekwencjach dla hasła: Ala125

Tabela 2 Szyfrowanie hasła

		n = 6						v = max+1
z = 6		1	2	3	4	5	6	v = 10
Sekwencja 1	1	5	1	0	8	9	7	
	2	2	5	1	0	8	9	
	3	5	2	5	1	0	8	
	4	0	5	2	5	1	0	
	5	8	0	5	2	5	1	
	6	9	8	0	5	2	5	
	7	4	9	8	0	5	2	
	8	8	4	9	8	0	5	
	9	6	8	4	9	8	0	
	10	6	6	8	4	9	8	v = 10

Sekwencja 2	1	7	6	6	8	4	9	
	2	2	7	6	6	8	4	
	3	7	2	7	6	6	8	
	4	0	7	2	7	6	6	
	5	1	0	7	2	7	6	
	6	1	1	0	7	2	7	
	7	1	1	1	0	7	2	
	8	2	1	1	1	0	7	
	9	1	2	1	1	1	0	
	10	5	1	2	1	1	1	v = 6
Sekwencja 3	1	4	5	1	2	1	1	
	2	0	4	5	1	2	1	
	3	0	0	4	5	1	2	
	4	1	0	0	4	5	1	
	5	1	1	0	0	4	5	
	6	5	1	1	0	0	4	v = 6
Sekwencja 4	1	5	5	1	1	0	0	
	2	5	5	5	1	1	0	
	3	4	5	5	5	1	1	
	4	4	4	5	5	5	1	
	5	1	4	4	5	5	5	
	6	1	1	4	4	5	5	v = 6
Sekwencja 5	1	4	1	1	4	4	5	
	2	3	4	1	1	4	4	
	3	4	3	4	1	1	4	
	4	4	4	3	4	1	1	
	5	1	4	4	3	4	1	
	6	2	1	4	4	3	4	v = 5
Sekwencja 6	1	4	2	1	4	4	3	
	2	4	4	2	1	4	4	
	3	3	4	4	2	1	4	
	4	1	3	4	4	2	1	
	5	1	1	3	4	4	2	

Uzyskany kryptogram z hasła „Ala125" to: 113442.

PODSUMOWANIE

Zastosowanie generatora liczb pseudolosowych w oparciu o technologię MVL niesie ze sobą liczne zalety. Przede wszystkim dzięki większej liczbie dyskretnych poziomów logicznych zwielokrotnia się ilość kodów wynikowych przy zachowaniu liczby pozycji kodu. Z drugiej strony możliwe jest użycie relatywnie trywialnych haseł, które następnie przekodowane dają w efekcie „nieczytelne" parametry opisujące

strukturę i stan startowy generatora liczb pseudolosowych. Większa liczba parametrów generatora oznacza naturalnie utrudnienie analizy jego działania, co w konsekwencji poprawia jakość szyfrowania.

Literatura

[1] Anonim: "*Maximum Security: A Hacker's Guide To Protecting Your Linux Server and Workstation*" (przekład z języka angielskiego - "Linux. Agresja i ochrona"), 1999

[2] Merike Kaeo: „*Designing Network Security*" (przekład z języka angielskiego - „Tworzenie bezpiecznych sieci"), Warszawa 2000

[3] Mirosław Kutyłowski, Willy-B. Strothmann: „*Kryptografia – Teoria i praktyka zabezpieczania systemów komputerowych*", Warszawa 1999

[4] Piotr Hoffman: „*Kryptografia a generatory liczb losowych w systemie Linux*", http://www.linux.itt.pl/LabLinux/WEJSCIE-WYJSCIE/PODTEMAT_1/crypto.html

ANDRZEJ MITAS
POLITECHNIKA ŚLĄSKA

Zastosowanie funkcji rejestru liniowego do osobistej ochrony danych w transmisji informacji
A linear register function application for personal data protect in the information transmission

Streszczenie

W artykule przedstawiono skrótowo problematykę chronionego dostępu do zasobów informatycznych poprzez zaburzenie ciągu transmitowanych danych. Wobec transmisji danych w sieciach publicznych szczególnie ważne staje się szyfrowanie danych. Na szczególną uwagę zasługuje możliwość kodowania CDMA (*code division multiple* access) stosowana od kilku lat także w cywilnych systemach transmisji z poszerzonym widmem. Na tym tle dyskutuje się współcześnie o możliwości parametryzacji funkcji poszerzającej widmo, np. poprzez dobór funkcji sprzężenia rejestru liniowej kompresji LFSR lub określenie stanu startowego oraz długości sekwencji wyjściowej.

Abstract

In this paper was shortly described the problem of the numeric databases protect in the form of the transmitted data destroying. With regard to the popular data transfer procedures in the public networks increases the problem of the data encryption. A very interesting solution gives the CDMA method (code division multiple access). On this base has been discussed the possibility of the parameter setting of the spread spectrum function, for example trough the choose of the feedback function or of the start point state or of the sequence length.

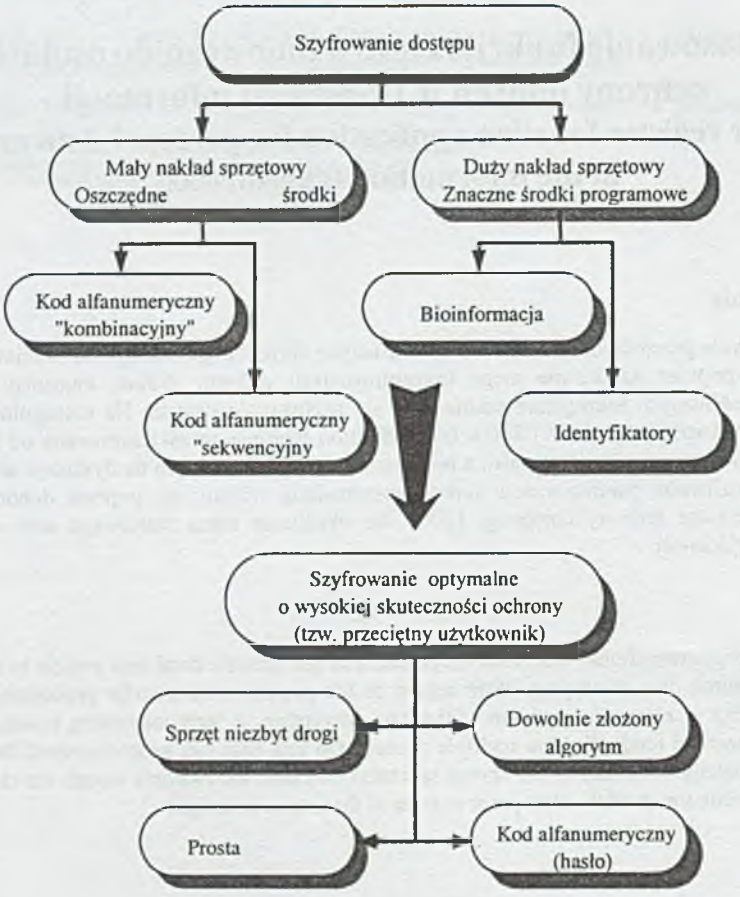
1. Wstęp

Dynamiczny postęp techniki cyfrowej i oprogramowania implikuje rozwój narzędzi i metod przetwarzania informacji. Ze względu na ogromne ilości ważnych danych o charakterze ekonomicznym, związanych przede wszystkim z zarządzaniem środkami finansowymi, jak również wiążących się z utrzymywaniem potencjału militarnego, bardzo istotne znaczenie mają techniki służące ochronie tych informacji. Problem tego rodzaju wynika stąd, iż dla sprawnego zarządzania przepływem wiedzy w ogóle, należy własne zasoby informatyczne dołączyć do ogólnej sieci telekomunikacyjnej.

W konsekwencji otrzymuje się dostęp do powszechnego kanału informacyjnego. Wówczas jednak trzeba zadbać o tajność własnych, niepublicznych zasobów.

Potrzeba przełamywania zabezpieczeń chroniących dostępu do niepublicznych danych jest wprost proporcjonalna do atrakcyjności tych informacji. Możliwości zabezpieczeń są naturalnie ogromne, o ile założy się nieudostępnianie danych, dotyczących szyfru, osobom niepowołanym. W przeciwnym wypadku dyskusja jest bezprzedmiotowa.

Szyfrowanie dostępu można sklasyfikować na wiele sposobów. Jeden z przykładów prezentuje rysunek 1.



Rys. 1. Ogólna klasyfikacja sposobów weryfikacji uprawnień

Z jednej strony mamy kody o niewielkim stopniu złożoności, realizowane za pomocą oszczędnych środków sprzętowo-programowych. Kod taki możemy sobie wyobrazić jako kombinację typowych, zadawanych z klawiatury, znaków alfanumerycznych, dających w efekcie słowo kodowe. Nieco bardziej złożony sposób, wymagający już pewnego nakładu software'owego polega na zadawaniu sekwencji znaków, np. w określonych odstępach czasu (naturalnie z pewną dopuszczalną tolerancją). Kod taki można

by określić jako sekwencyjny. Kodowanie w obu tych przypadkach odbywa się podobnie i polega na zadaniu jawnej nazwy użytkownika w czasie logowania, po czym właściwe hasło udostępniające nam zasoby jest wprowadzane tajnie. Naturalnie oba powyższe rodzaje słów kodowych są jednakowo łatwo dostępne w powszechnej sieci telekomunikacyjnej.

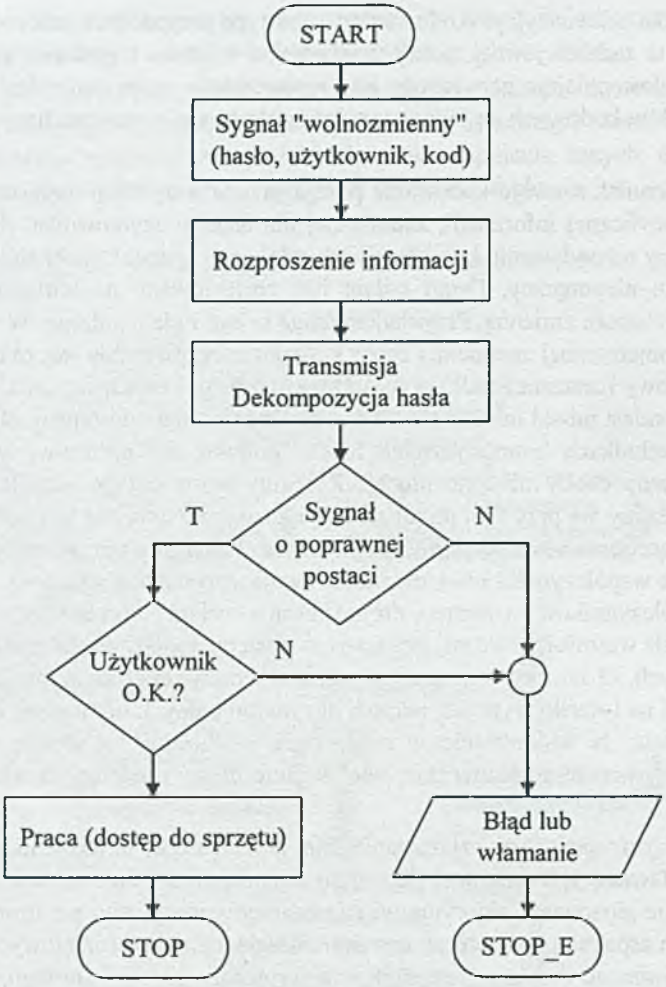
Drugi kierunek rozwoju kodowania polega przede wszystkim na znacznym nagromadzeniu specyficznej informacji, znamiennej dla danego użytkownika. Pierwszy sposób, polegający na podawaniu kombinacji lub sekwencji grubej książki słów kodowych, jest po prostu nieporęczny. Drugi odłam jest zorientowany na bioinformację, jako informację osobniczo zmienną. Przykładem mogą tu być linie papilarne. W przypadkach informacji biometrycznej znamienną cechą systemu zabezpieczenia jest relatywnie duży nakład sprzętowy i znaczne środki programowe do obsługi zabezpieczenia. Stosunkowo mały jest natomiast udział intelektu samego zainteresowanego dostępem. Nieco pesymistycznie w technikach biometrycznych należy potraktować niezerowy współczynnik zakwalifikowania osoby nieuprawnionej. Z reguły wartość tego współczynnika jest znikoma. Godzimy się przy tym na niezerową i zazwyczaj znaczną wartość współczynnika określającego częstość niepoprawnego odrzucenia osoby uprawnionej do dostępu do danych. Te współczynniki mają naturalnie swoją statystyczną wymowę. Małe wartości tych współczynników są zachętą do stosowania technik biometrycznych. Dotkliwe stają się te małe wartości wówczas, gdy dotyczą dostępu do naszych osobistych zasobów informatycznych. O ile możemy sobie wyobrazić teoretycznie, że system identyfikacji biometrycznej na wszelki wypadek odrzuci nas, mimo pełnych uprawnień, o tyle trudno sobie wyobrazić, że kilkukrotnie w ciągu dnia, odchodząc na chwilę od systemu, będziemy po powrocie, nieskutecznie, wielokrotnie prosić o dostęp do własnego komputera.

Optymalnym sposobem szyfrowania dla przeciętnego użytkownika byłby kod zadawany z klawiatury, o rozsądnej (łatwej do zapamiętania) długości, który poddawany byłby dowolnie złożonemu algorytmowi przetwarzania wstępnego po stronie użytkownika. Ważnym aspektem jest naturalnie minimalizacja nakładów sprzętowych do obsługi tego weryfikowanego dostępu. Optymalizacja sprowadza się więc do tego, by kodowanie dostępu było proste, ale protokół zastosowania kodu, czyli algorytm przetwarzania tej informacji, był programowalny specyficznie dla użytkownika i przez to złożony.

Rozpraszanie widma informacji

Zagadnienie rozpraszania widma można w skrócie określić jako uzmiennianie sygnału wolnozmiennego za pomocą szybkozmiennego sygnału kodującego. Zysk przetwarzania w aspekcie modulacji polega na poprawie stosunku sygnału do szumu. W podstawowej swej funkcji wielodostęp kodowy ma tę zaletę, że umożliwia eliminację zakłóceń występujących typowo w kanale teletransmisyjnym. W sensie kodowanego dostępu do chronionych danych rozproszenie widma może przyjąć postać modyfikacji hasła.

Do modyfikacji hasła można użyć dowolnego ciągu szybkozmiennego. Ilustrację algorytmu warunkowego dostępu do danych stanowi rysunek 2.



Rys. 2. Przykładowy algorytm modyfikacji hasła w procedurze dostępu do chronionej informacji

Zadaniem wstępnym użytkownika jest podanie swojego imienia przy próbie nawiązania łączności. Po tej operacji system użytkownika pozyskuje od niego (np. z klawiatury) informację charakteryzującą modyfikator hasła (np. przez bezpośrednie wprowadzenie sekwencji modyfikującej). Modyfikator ten musi być kompatybilny z tym, który jest w posiadaniu systemu, do którego dostęp warunkowy ma zostać udzielony. Następnie realizowane jest połączenie obu informacji, tak by zatrzeć czytelność hasła, tzn. dokonuje się rozproszenia informacji. Czynność tę można interpretować w sensie algebraicznym jako operację dzielenia wielomianów nad ciałem GF(n), gdzie n oznacza liczbę poziomów logicznych. W szczególnym przypadku typowej logiki binarnej traktujemy tę operację jako sumę modulo 2 wolnozmiennego sygnału hasła i szybkozmiennej sekwencji modyfikatora, co powoduje naturalnie *B*-krotne poszerzenie

pasma, gdzie $B=T_h/T_m$ (stosunek czasu trwania bitu hasła do bitu modyfikatora). Taka częstotliwościowa interpretacja jest ważna z punktu widzenia pasma przenoszenia w kanale teletransmisyjnym. W tym przypadku, przy ograniczeniu sprzętowym medium transmisyjnego oraz użytych elementów interfejsowych istnieje możliwość spowolnienia przekazu hasła, tak by częstotliwość zmian modyfikatora nie przekroczyła granicznej częstotliwości kanału. Dzięki zastosowaniu sekwencji modyfikatora u odbiorcy (etap dekompozycji) ciąg danych zostaje zdeszyfrowany do postaci pierwotnego hasła, które jest kluczem, warunkującym dostęp do danych.

Jak wynika z danych literaturowych z dziedziny telefonii bezprzewodowej sygnał rozproszony jest trudno uchwytny. Rozpraszanie widma metodą FH-SS (*frequency hopping spread spectrum*) właściwie nie daje szansy odbioru informacji on-line bez znajomości sekwencji przełączania syntezatora częstotliwości nośnej odbiornika idealnie synchronicznej z sekwencją w nadajniku. Podobnie w przypadku modyfikacji hasła – jeśli sekwencja modyfikująca ma charakter przypadkowy, wówczas możliwość złamania kodu jest niewielka, o ile naturalnie osoba dokonująca włamania nie dysponuje wiedzą o oryginalnym modyfikatorze. W praktyce nietrudno sobie wyobrazić dodatkowe warunki ograniczające dostęp, np. blokadę użytkownika po podaniu niewłaściwego hasła itp. Podsłuchanie hasła jest natomiast nierealne ze względu na nieznany modyfikator. W szczególności sygnałem modyfikującym może być binarna sekwencja losowa (jeśli ograniczymy rozważania do systemów dwuwartościowych). Technicznie realnym przybliżeniem sekwencji losowej jest ciąg wyjściowy z rejestru liniowego, którego wielomian sprzężenia jest wielomianem pierwotnym. Spełnione mają być jedynie warunki:

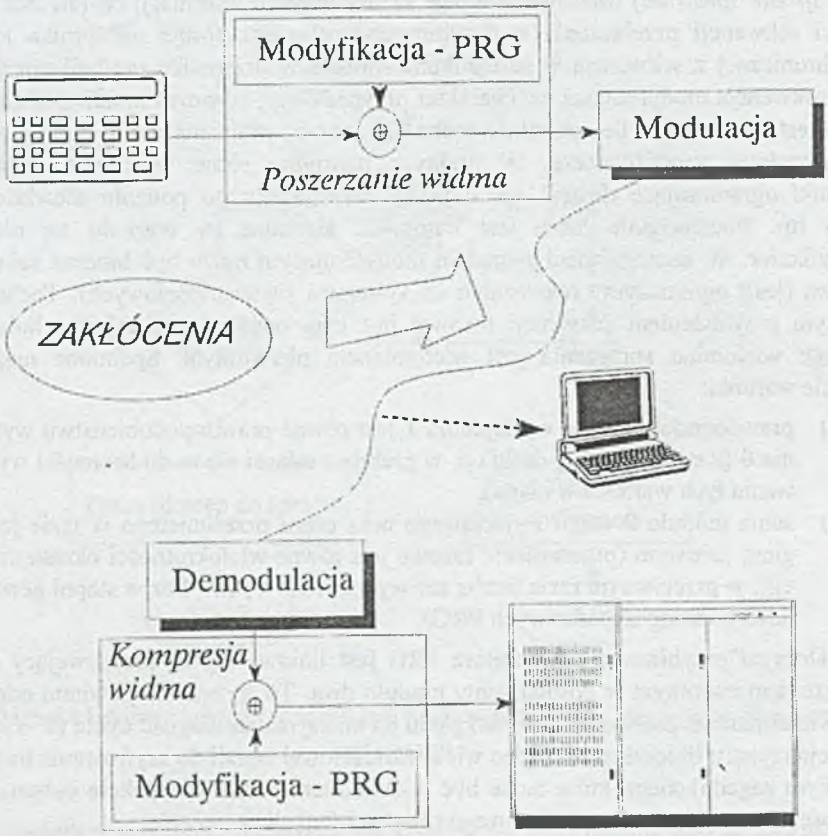
1) prawdopodobieństwo wystąpienia 1 jest równe prawdopodobieństwu wystąpienia 0 (z częstościowej definicji, w praktyce odnosi się to do krotności występowania tych wartości w ciągu),
2) suma modulo 2 ciągu wyjściowego oraz ciągu przesuniętego w fazie jest ciągiem zerowym (przesunięcie fazowe jest równe wielokrotności okresu sekwencji), w przeciwnym razie liczba zer wynosi $1/(2^n-1)$ (n - liczba stopni generatora liczb pseudoprzypadkowych PRG).

Dobrym przybliżeniem generatora PRG jest liniowy rejestr przesuwający objęty sprzężeniem zwrotnym w postaci sumy modulo dwa. To sprzężenie powinno odpowiadać wielomianowi pierwotnemu ze względu na maksymalną długość cyklu (2^n-1). Konstrukcja rejestru liniowego oraz jego wielowartościowej wersji do szyfrowania hasła jest osobnym zagadnieniem, które może być przedmiotem badań w aspekcie optymalizacji długości modyfikatora, stanu startowego rejestru i funkcji sprzężenia.

Ochrona danych w osobistej wymianie informacji

Niezależnie od obecnie stosowanych systemów ochrony danych w komputerach osobistych podłączonych do globalnej sieci teleinformatycznej, niewątpliwie interesujące dla przeciętnego, zaawansowanego użytkownika jest rozwiązanie polegające na osobistym "rozpraszaniu widma informacji. Szczególnie spektakularnym obszarem zastosowań jest kodowanie osobistej poczty elektronicznej. Na rysunku 3 przedstawiono w blokowej postaci koncepcję zaburzania strumienia przesyłanych danych poprzez modyfikację informacji liczbami pseudolosowymi. Dalszym etapem transmisji jest modulacja sygnału, prze-

nosząca go w pasmo kanału teletransmisyjnego, przydzielonego przez operatora sieci telekomunikacyjnej. W trakcie przesyłania pojawiają się zakłócenia, immanentne dla transmisji w ogóle. Dzięki operacji rozproszenia widma [2] osiąga się redukcję wpływu tych zakłóceń, ponieważ operacja dekodowania zaszyfrowanej informacji polega na kompresji widma za pomocą identycznego jak w kodowaniu ciągu liczb pseudolosowych. W trakcie tej właśnie kompresji następuje zaburzenie tych danych, które stanowiły wolnozmienne zakłócenie. Po zaburzeniu informacji zakłócającej szybkozmiennym ciągiem pseudoprzypadkowym następuje przesunięcie jego widma do wyższych zakresów częstotliwości, dzięki czemu drogą zwykłej filtracji można łatwo pozbyć się wpływu tych zakłóceń.



Rys. 3. Przykład osobistej ochrony danych w rozległym systemie telekomunikacyjnym

W praktyce utajnienie własnych danych, obejmujące w ogólnym algebraicznym sensie dzielenie wielomianów nad ciałem GF(n) dla logiki n-wartościowej, można zupełnie bezproblemowo rozwiązać w fazie zapisu danych na nośniku. Dzięki temu dane stają się nieczytelne już od momentu zapisu na dysku, co pozwala je chronić przed kradzieżą przy zdalnej penetracji osobistych zasobów. Jeśli dane mają być przekazane

na odległość lub też odczytane przez standardowy program, wówczas należy je poddać operacji kompresji za pomocą takiego samego ciągu zaburzającego, jak w procedurze kodowania. W przypadku transmisji odbiorca musi dysponować słowami programującymi generator pobudzeń pseudolosowych, a w szczególności wiedzą o wielomianie sprzężenia zwrotnego, długości cyklu i stanu startowego. Brak tych parametrów czyni poszukiwania włamywacza zupełnie pozbawione szans, ze względu na sekwencyjny charakter kodowania informacji. Przekazanie parametrów programujących generator musi mieć charakter poufny. Dużą szansę stanowi w tym przypadku zastosowanie logiki wielowartościowej, ponieważ wówczas parametry programujące generator pseudolosowy w zasadniczo bardziej kompaktowy sposób opisują jego budowę oraz unikalny, w sensie aplikacji w szyfrowaniu, cykl pracy.

Podsumowanie

Wysiłki zmierzające do podniesienia bezpieczeństwa danych są ze wszech miar uzasadnione. Pozostawienie danych ich własnemu losowi oznacza nieuchronne naruszenie przysługujących każdemu człowiekowi podstawowych konstytucyjnych uprawnień. Świadomość możliwości wykrycia sprawcy włamania przy totalnej komputeryzacji sprzętu i oprogramowania telekomunikacyjnego jest nikła, a przypadki wynoszenia na wyżyny intelektualne prymitywnych włamań sieciowych są powszechne. Stan ten jest społecznie akceptowalny, co naturalnie rodzi w praktyce dalsze patologie. Tolerancji takiego stanu rzeczy można się jednakże przeciwstawić. Koncepcje szyfrowania i weryfikacji uprawnień w sieciach wielodostępnych zyskują wielu zwolenników, zwłaszcza wśród tych, którzy plagą przestępstw komputerowych zostali już dotknięci.

Osobnym problemem jest użycie takich zabezpieczeń, które samej osobie chronionej, często leniwej i upartej, nie przysparzają problemów, nadwyrężających zmęczony codziennością umysł. Zapamiętywanie kodów, kluczy etc. często polega, jak wiadomo, na odnotowaniu tej informacji w czytelnym miejscu. Tu z pomocą przychodzą techniki biometryczne, poszukujące haseł w osobniczo zmiennej informacji genetycznej. W centrum zainteresowań są te próby, które pozyskują znamienne cechy szczególnie łatwo i bezbłędnie. Możliwości błędnych zakwalifikowań osoby nieuprawnionej są większe w technikach koncepcyjnie silnie maskujących informację genetyczną. Z reguły jednak należy się spodziewać, że techniki słabiej maskujące odbieraną bioinformację są obarczone dużą złożonością sprzętu i oprogramowania.

Nie należy się spodziewać radykalnej poprawy bezpieczeństwa danych wbrew woli użytkowników. Nawet najlepszy zamek do drzwi nie zabezpieczy naszego mieszkania, jeśli klucz schowamy pod wycieraczkę i pozostawimy dla odbiorcy czytelną kartkę: Klucz pod wycieraczką.

Literatura

[1] Hołubowicz W.: Systemy łączności bezprzewodowej. Poznań 1998

[2] Janaszek A., Mitas A.: Metody biometryczne w systemach identyfikacji i kontroli dostępu. Biuletyn Informacyjny Techniki Komputerowe Nr 1, 2000

JERZY SAWICKI, ADAM PODHORSKI
INSTYTUT ELEKTRONIKI,
TELEKOMUNIKACJI I INFORMATYKI
POLITECHNIKA SZCZECIŃSKA

Rejestracja i analiza sygnału akustycznego czynności jelit
Recording and analysis of the human intestinal activity acoustical signal

Streszczenie

W artykule omówiono problemy cyfrowego zapisu sygnału akustycznego czynności jelit człowieka. Opisano urządzenie, które zostało specjalnie zaprojektowane do zapisu tego sygnału. Przedstawiono wyniki analizy zapisanych próbek zarówno w funkcji czasu jak i częstotliwości. Wyniki te dały podstawę do scharakteryzowania tego sygnału, określenia jego parametrów, do dyskusji o celach dalszych badań w tym zakresie.

Abstract

In this paper we discuss problems of digital recording of the human intestinal activity acoustical signal. We describe equipment, which has been specially designed to record such signal and present results of the analysis of the recorded samples both in the time and in the frequency domain. Those results provided basis for giving the characteristics of the signal, it's main parameters and for the discussion on the aims of further research in this field.

1. Temat badań

Temat badań zaproponowali lekarze z III Kliniki Chirurgii Pomorskiej Akademii Medycznej w Szczecinie. Wielogodzinna rejestracja i analiza sygnałów akustycznych towarzyszących czynności jelit jest potrzebna szczególnie po operacjach narządów jamy brzusznej. Operacje chirurgiczne porażają (wstrzymują) czasowo prawidłową pracę jelit. Określenie czasu powrotu prawidłowej perystaltyki jelit wymaga częstej kontroli lekarskiej i jak się wydaje może zostać zastąpione systemem elektronicznej rejestracji i analizy sygnału akustycznego towarzyszącego czynności jelit. Lekarze widzieliby chętnie w swojej pracy przenośne urządzenie do 24-godzinnego zapisu czynności jelit oraz system szybkiej analizy zarejestrowanego materiału na wzór urządzeń monitorujących pracę serca. Prototyp takiego urządzenia jest przedstawiony w niniejszej pracy. W dalszych planach jest opracowanie takich metod analizy sygnału czynności

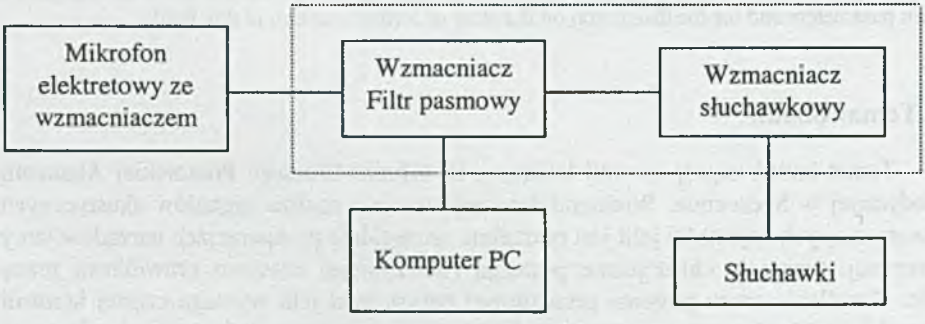
jelit, które będą mogły być użyteczne w diagnostyce medycznej. Literatura naukowa na ten temat jest skromna, ale kilka wymienionych na końcu artykułu pozycji świadczy, że tego rodzaju badania i prace konstrukcyjne nad aparaturą są prowadzone. W niniejszym artykule traktuje się perystaltykę jelit jako główną przyczynę analizowanych sygnałów, trzeba jednak w tym miejscu zaznaczyć, że czynności motoryczne jelita cienkiego są bardziej złożone i zapewne rejestrowany materiał dźwiękowy zawiera odzwierciedlenie także innych procesów zachodzących w organizmie człowieka.

2. Podstawowe założenia systemu rejestracji sygnału czynności jelit

Przyjęto, że system rejestracji powinien umożliwiać zapis długich odcinków sygnału (do 24 godzin). Wstępne badania pokazały, że pasmo sygnału wynosi przynajmniej 5 kHz. Objętość informacyjna sygnału jest zatem znacznie większa niż sygnału EKG i nie jest możliwe zaadaptowanie znanych rozwiązań do 24-godzinnego monitorowania pracy serca (Holter). Zarejestrowanie sygnału o takim parametrach na taśmie magnetycznej uznano za trudne, niepraktyczne i nienowoczesne. Zdecydowano o rejestracji cyfrowej na dysku twardym przenośnego komputera osobistego (notebook) z wykorzystaniem standardowej 16 bitowej karty dźwiękowej typu Sound Blaster. Przy projektowanej maksymalnej częstotliwości próbkowania sygnału: 16000 razy na sekundę, objętość informacyjna sygnału zarejestrowanego w czasie jednej doby będzie wynosić: 16000 próbek x 24 godziny x 3600 sekund x 2 bajty = 2,8 GB. Taka ilość danych bez trudu może być zapisana na twardym dysku komputera. Istotnym czynnikiem przy wyborze takiej koncepcji była także możliwość bateryjnego zasilania całego systemu, co eliminuje zasilanie z sieci elektroenergetycznej i związane z tym problemy bezpieczeństwa pacjenta.

3. Sprzęt do rejestracji sygnału

Do rejestracji sygnału akustycznego perystaltyki jelit została specjalnie opracowana aparatura pomiarowa, której schemat blokowy przedstawiono na rys. 1.



Rys. 1. Schemat blokowy systemu do rejestracji sygnału perystaltyki jelit

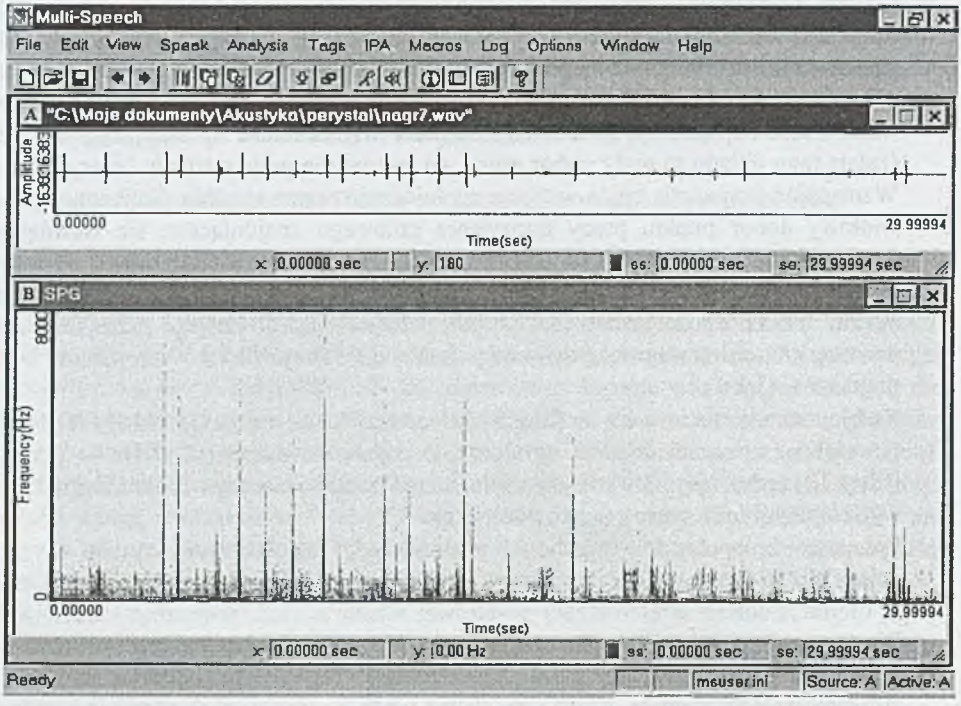
Omówienie zasadniczych elementów systemu:

- Do odbioru sygnału akustycznego zastosowano standardowy mikrofonowy przetwornik elektretowy o średnicy 9 mm umieszczony w teflonowej tulei dystansowej o średnicy ok. 4 cm. Zadaniem teflonowej obudowy mikrofonu jest dopasowanie przetwornika do ciała ludzkiego i zmniejszenie zakłóceń spowodowanych tarciem mikrofonu o skórę. Tuż przy mikrofonie umieszczono zminiaturyzowany wzmacniacz napięciowy, zbudowany na bazie wzmacniacza operacyjnego TL062 (zaleta tego układu to mały pobór mocy, co jest ważne przy zasilaniu bateryjnym). Wzmacniacz zapewnia także wstępne ograniczanie pasma sygnału. Zadbano o prawidłowy dobór punktu pracy tranzystora polowego znajdującego się wewnątrz przetwornika mikrofonowego i w efekcie przy prostej konstrukcji całego wzmacniacza możliwe było uzyskanie sygnału wyjściowego o poziomie 1 V, bez słuchowo odczuwanej obecności szumu. Taki sygnał nadaje się już do łatwego przesyłania za pomocą kilkumetrowego ekranowanego kabla do dalszych bloków systemów bez pogorszenia jakości.
- Kolejny wzmacniacz wraz z filtrem zbudowano także na bazie układu TL062. Niewielkie wzmocnienie oraz ograniczenie pasma do zakresu 200 Hz – 8 kHz (filtry II rzędu) były łatwymi do spełnienia wymaganiami tego bloku. Sygnał na wyjściu tego bloku może osiągać poziom ok. 3 V.
- Przenośny komputer PC (notebook) musi posiadać zainstalowany system operacyjny Windows oraz kartę dźwiękową o możliwie najwyższych parametrach jakościowych. Pomimo deklarowanej 16-bitowej rozdzielczości, większość kart Sound Blaster ma rozdzielczość znacznie mniejszą, gdyż duży poziom zakłóceń wewnątrz komputera powoduje zmiany na najmniej znaczących pozycjach bitów nawet przy zwartym wejściu sygnału. Karta dźwiękowa użyta w opisywanym systemie pomiarowym zapewniała rozdzielczość 13-bitową.
- Dodatkowo system pomiarowy zawiera wzmacniacz słuchawkowy umożliwiający kontrolę rejestrowanego materiału i sprawdzenie poprawności zamocowania mikrofonu oraz jakości sygnału.

4. Analiza zarejestrowanego materiału dźwiękowego

Do analizy nagranych plików dźwiękowych zastosowano program komputerowy Multi-Speech Analysis Workstation, firmy Kay Elemetrics. Program ten jest zasadniczo przeznaczony do analizy sygnału mowy, jednakże ze względu na podobne pasmo częstotliwości sygnału mowy i sygnału perystaltyki jelit okazał się bardzo użyteczny w analizie tego ostatniego sygnału.

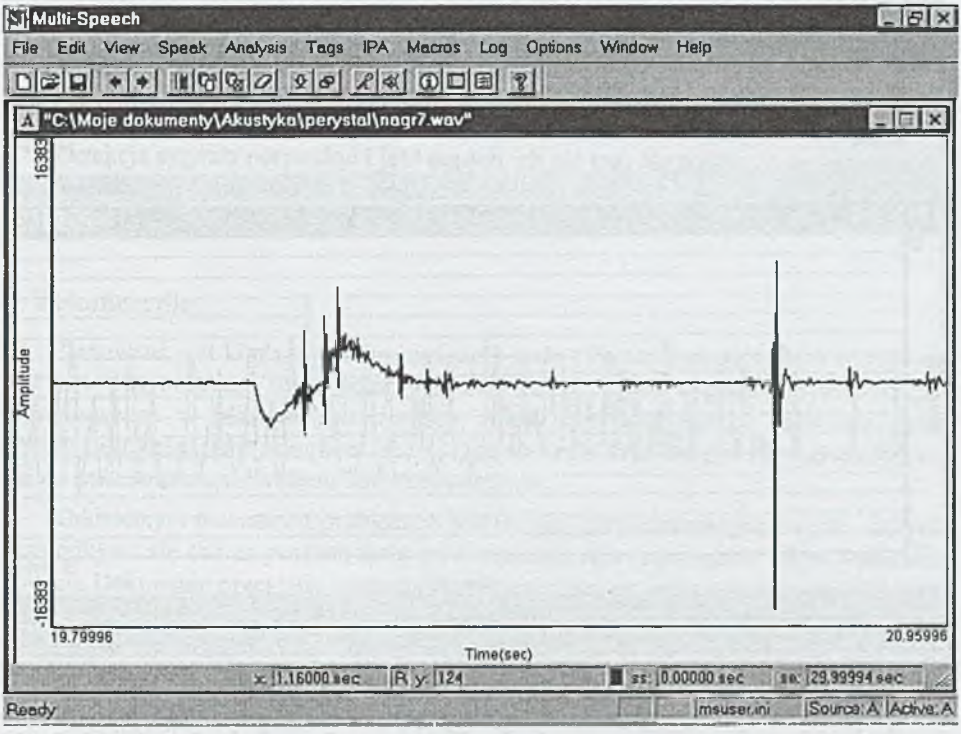
Zarejestrowano kilkadziesiąt minut sygnału czynności jelit u wielu osób zdrowych i chorych. Wspólna cechą wszystkich zarejestrowanych sygnałów jest występowanie w odstępach kilku lub kilkunastu sekund pojedynczych, izolowanych zdarzeń, które opisowo można nazwać: pukaniem, przelewaniem, burczeniem itp. W przykładowym 30 sekundowym odcinku sygnału akustycznego czynności jelit, przedstawionym na rys. 2, można wyróżnić kilkanaście izolowanych dźwięków o dużych amplitudach.



Rys. 2. Przebieg czasowy (okno górne) i spektrogram (okno dolne) 30-sekundowego odcinka nagrania sygnału akustycznego czynności jelit

Sygnał przedstawiony na rys. 1 został zarejestrowany z częstotliwością próbkowania 16 kHz. Widoczny na rysunku spektrogram został wykonany za pomocą 512 punktowej FFT i z użyciem okna czasowego Hamminga.

Jak wspomniano poszczególne dźwięki można umownie zaklasyfikować do pewnych kategorii. Na rys.3 przedstawiono wybrany z poprzedniego nagrania krótki odcinek czasowy (długość 1,16 sekundy) zawierający dwa wyraźne sygnały, z których pierwszy ma charakter „przelewania", a drugi „puknięcia".



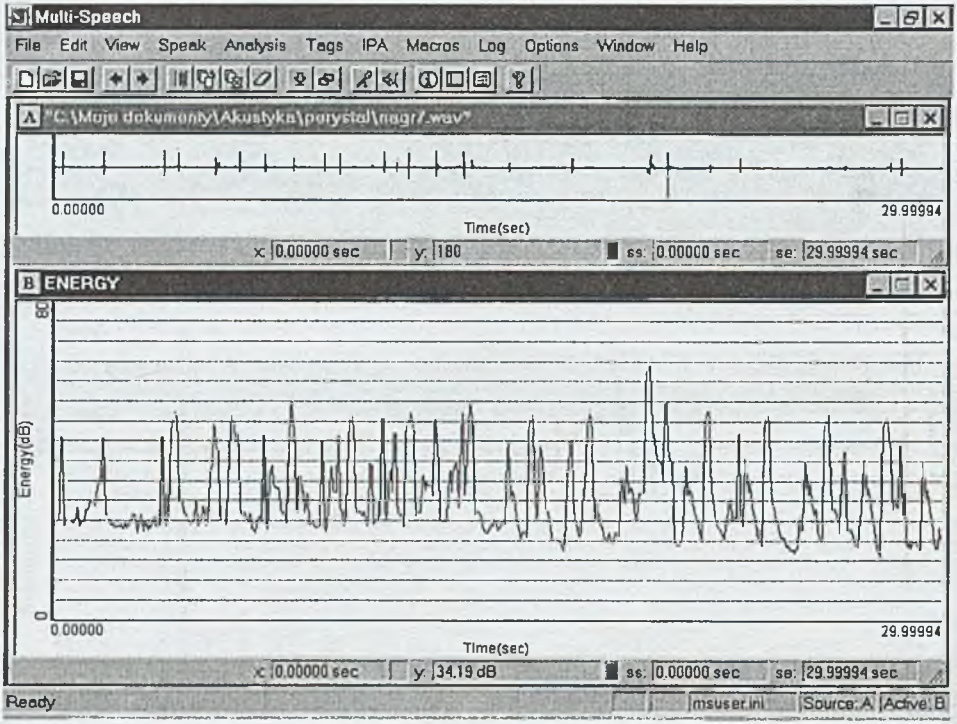
Rys. 3. Krótki fragment (1,2 sekundy) przebiegu czasowego sygnału czynności jelit

Analiza czasu trwania kilkudziesięciu izolowanych zjawisk akustycznych odpowiadających czynności jelit, pozwoliła określić przeciętne czasy trwania różnych dźwięków:

- „puknięcia" o czasie trwania do 150 ms,
- „głośne przelania" o czasie trwania do 420 ms,
- „burczenia" o czasie trwania do ok. 400 ms,
- „ciche przelania" o czasie trwania do 600 ms.

Dźwięki słyszalne jako „puknięcia" posiadają wyraźne maksima w okolicy 250 i 600 Hz, charakterystyka częstotliwościowa pozostałych jest bardziej równomierna.

Na rys. 4 przedstawiono przebieg czasowy zmian energii sygnału akustycznego czynności jelit. Energia była uśredniana w przedziałach o czasie trwania 100 ms. Przebieg czasowy zmian energii pozwala na łatwą lokalizację położenia i klasyfikację pod względem głośności poszczególnych dźwięków.



Rys. 4. Przebieg czasowy zmian energii sygnału akustycznego perystaltyki jelit (dolne okno)

5. Wnioski

Na podstawie przeprowadzonych badań można wyprowadzić następujące wnioski:

- Do rejestracji sygnału perystaltyki jelit wystarczający jest prosty mikrofon elektretowy umieszczony w obudowie tłumiącej tarcie mikrofonu o skórę przy ruchach pacjenta.
- Zaproponowane rozwiązania wzmacniaczy i filtrów są wystarczające i nie jest potrzebne stosowanie innych bardziej niskoszumnych układów.
- Najważniejszym sygnałem zakłócającym są zakłócenia elektroenergetyczne o częstotliwości 50 Hz i ich harmoniczne (należy zadbać o skuteczne zaekranowanie wzmacniaczy).
- Wymagana częstotliwość próbkowania sygnału perystaltyki wynosi nie więcej niż 16 kHz i można rozważać jej zmniejszenie nawet do 8 kHz.
- Kwantowanie sygnału powinno odbywać się z maksymalną rozdzielczością karty Sound Blaster, czyli teoretycznie 16 bitów.
- Objętość sygnału w czasie 24 godzinnego zapisu nie przekracza pojemności stosowanych obecnie twardych dysków.
- Do analizy sygnału nadaje się zarówno dziedzina czasu jak i częstotliwości.

- W dziedzinie częstotliwości skuteczne są wypróbowane dotąd metody tzn. spektrogramy, i widma chwilowe sygnału, natomiast w dziedzinie czasu użyteczna jest analiza zmian energii sygnału.
- Problemem w analizie sygnałów perystaltyki są zakłócenia pochodzące z tarcia mikrofonu o skórę brzucha – niekiedy trudno je odróżnić słuchowo od czynności jelit.
- Detekcja sygnału perystaltyki jelit (są lub ich nie ma) nie nastręcza poważniejszych problemów, natomiast automatyczne rozpoznawanie typów dźwięków wymaga jeszcze dodatkowych prac związanych przede wszystkim z ich klasyfikacją.

6. Zakończenie

Planowana jest kontynuacja prowadzonej pracy. Przedstawiony system pomiarowy jest testowany obecnie przez lekarzy i służy do rejestracji sygnału perystaltyki jelit występującego w różnych schorzeniach. Wadą dotychczasowego rozwiązania jest konieczność ustawienia komputera przy łóżku chorego. Problem ten ma być rozwiązany dzięki zastosowaniu mikrofonu bezprzewodowego.

Oddzielnym poważnym problemem jest analiza zarejestrowanych nagrań. Dotychczas odbywa się ona za pomocą dość uniwersalnego oprogramowania jakim jest Multi-Speech. Dokonanie przeglądu wielogodzinnego zapisu jest jednak bardzo pracochłonne i należy myśleć o zautomatyzowaniu tej procedury. Nie wiadomo jeszcze czy w automatycznym systemie analizy nagrań będzie możliwe tylko stwierdzenie obecności czynności jelit (to nie wydaje się trudne) czy też uda się klasyfikować poszczególne dźwięki. Pomyślne wykonanie tych zamierzeń będzie wymagało ścisłej współpracy lekarzy i inżynierów.

Literatura

[1] Arnbjornsson E., Bengmark S.: Asculation of bowel sounds in patients with suspected acute appendictis – an aid in the diagnosis? Eur. Surg. Res. 15, 1983, str. 24-27

[2] Garner C.G.,Ehrenreich H.: Non-invasive topographic analysis of intestinal activity in man on the basis of acustic ohonema. Res. Exp. Med., 189, 1989, str. 129-140

[3] Gniwecki M.: Analiza akustyczna sygnałów akustycznych perystaltyki jelit (praca magisterska napisana pod kierunkiem dr inż. Jerzego Sawickiego). Politechnika Szczecińska. Szczecin 2000

JAN RYŻKO, JERZY SŁAWIŃSKI
INSTYTUT MASZYN MATEMATYCZNYCH WARSZAWA

Metody biometryczne w systemach identyfikacji i weryfikacji – techniki, zastosowania, aktualny stan rozwoju

Biometric methods used in the identification and authentication systems – technologies, applications, current state of development

Streszczenie

W referacie przedstawione są przyczyny stosowania metod biometrycznych do identyfikacji i weryfikacji osób oraz charakterystyki poszczególnych technik. Podane są parametry urządzeń wykorzystujących te techniki i omówiono przykładowe realizacje.

Następnie wymieniono dziedziny, w których metody te są stosowane, ilustrując je przykładami projektów i zwracając uwagę na perspektywy rozwoju. W zakończeniu opisany jest tworzący się rynek biometryczny i rola opracowywanych i wprowadzanych tu standardów.

Abstract

The lecture presented reasons for the use of biometric methods to identify and verify human beings as well as characteristics of particular technologies. It also presented parameters of devices, which use these technologies and described exemplary realisations.

Subsequently the lecturers mentioned fields in which the methods were applied and gave examples of projects. Particular stress was put on perspectives of their development. Finally the emerging biometric market was described as well as the role of the worked out and established standards.

1. Bezbłędna personalizacja

W okresie znacznego wzrostu zagrożenia zarówno dóbr materialnych jak i intelektualnych szczególnego znaczenia nabiera odpowiednie ich zabezpieczenie. Dotychczas stosowane środki ochrony w postaci różnego rodzaju zamków, haseł, numerów ewidencyjnych, a nawet rozmaitych kart czy innych żetonów okazują się w określonych sytuacjach mało skuteczne, gdyż hasło czy numer łatwo zapomnieć, a zapisane udostępnić niepowołanym osobom, natomiast klucz czy karta mogą być

zgubione, skradzione lub podrobione i wykorzystane do uzyskania dostępu do pomieszczeń, skrytek, kont, urządzeń, sieci itp. Istotnym więc staje się sprawdzenie uprawnień osoby domagającej się dostępu, co najczęściej sprowadza się do potwierdzenia jej tożsamości. W dodatku potwierdzenie to powinno być uzyskane poprzez pomiar indywidualnych i niepowtarzalnych, a najlepiej i niezniszczalnych cech tej osoby. Rozwiązania tego problemu dostarczają nam metody biometryczne, które są zautomatyzowanymi metodami identyfikacji lub weryfikacji osób w oparciu o ich właściwości fizjologiczne lub behawiorystyczne [1].

Do cech fizjologicznych najczęściej tu wykorzystywanych należą: linie papilarne, kształt dłoni i twarzy, charakterystyczne właściwości tęczówki i siatkówki oka, czasami sięga się też po geometrię uszu, ust, układ żył (zwykle w nadgarstku) lub takich cech jak głos, zapach czy DNA danego człowieka. Natomiast cechy określające zachowanie się człowieka to: sposób uderzania w klawisze, chodzenia, a także weryfikacja podpisu i osoby mówiącej (speaker), na podstawie analizy głosu, ewentualnie ruchu ust.

Zaletą większości technik biometrycznych jest ich nieinwazyjność, pomiar odbywa się w pewnej odległości, najczęściej przy użyciu kamer.

2. Techniki biometryczne

2.1 Linie papilarne

Jest to najdawniej stosowana metoda biometryczna. Odciski palców znaleziono na tabliczkach w Babilonii sprzed kilku tysięcy lat, a Chińczycy podpisywali nimi dokumenty. O ich niezmienności pisał profesor uniwersytetu bolońskiego Malpighi w XVII wieku, a od końca XIX wieku technikę tę zaczęto powszechnie stosować w dziedzinie przestrzegania prawa. Zwrócono przy tym uwagę, że przy porównywaniu tych niepowtarzalnych obrazów, nie trzeba brać pod uwagę wszystkich ich elementów, ale wystarczy określić usytuowanie kilkudziesięciu lub nawet kilkunastu tzw. minucji, czyli punktów początkowych lub przecięć linii papilarnych, by jednoznacznie określić osobę. Ogranicza to ilość informacji, którą musimy zapisać do porównywania w przyszłości, a ponadto uwalnia nas od zarzutu naruszania prywatności.

Rozwój daktyloskopii, która stała się podstawowym działem kryminalistyki, doprowadził do nowoczesnych laboratoriów wyposażonych bogato w odczynniki chemiczne i nowoczesną aparaturę. Pojawiły się systemy automatycznej identyfikacji daktyloskopijnej AFIS (Automated Fingerprint Identification Systems), pozwalające wielokrotnie poprawić wyniki dochodzeń. W roku 1978 pierwszy taki system oferowała w USA firma Printrak, potem pojawiły się systemy konkurencyjne: francuski Morpho, japoński NEC, amerykańskie Cogent i Goldfinger, niemiecki S-AFIS i inne. Już wcześniej podjęto prace nad skonstruowaniem urządzenia zamieniającego obraz linii papilarnych na postać cyfrową (kod), a następnie porównującego te kody. Stosowane są różne technologie dla realizacji tych zadań. Początkowo były to prawie wyłącznie układy optyczne, gdzie obraz oświetlonych linii papilarnych padał na matrycę CCD (coupled-charge device – układ ze sprzężeniem ładunkowym), obecnie przeważają układy sensorowe, gdzie palec przykłada się, poprzez powłokę ochronną, bezpośrednio do płytki krzemowej, doprowadzając do utworzenia matrycy, najczęściej pojemnościowej, której

rozkład ładunku odpowiada obrazowi linii. Przykłady obecnie oferowanych na rynku tych urządzeń podane będą w punkcie 4.

W dalszym ciągu technika linii papilarnych jest intensywnie rozwijana. W roku 1999 ponad 55% (80 na 145) firm biometrycznych związane było z tą metodą [1], a jej udział w rynku biometrycznym był największy (34,7% plus 4,4% systemy AFIS – [2]). W układach fizycznej kontroli dostępu [3] udział tej techniki wzrósł z 19,4% w 1998 roku do 21,7% w 1999 roku.

Do wad tej metody należy zaliczyć wpływ stanu powierzchni palca na wynik pomiaru (zabrudzenia, uszkodzenia, stopień nawilżenia).

Więcej danych na temat tej techniki, łącznie z zastosowaniami można znaleźć w przeglądzie [4], a odnośnie najnowszych rozwiązań sensorowych w [5].

2.2 Kształt dłoni

Jest to również bardzo popularna metoda, może nieco mniej dokładna od linii papilarnych, ale nie posiadająca jej wad i zwłaszcza w dziedzinie kontroli fizycznego dostępu dominująca na rynku biometrycznym (48,4% udziału w 1998 roku i 42,2% w 1999 roku – [3]), udział w całym tym rynku wyniósł w 1999 roku 31% [2].

Po umieszczeniu dłoni w czytniku jest ona oświetlana zwykle promieniami podczerwonymi, a trójwymiarowy obraz odczytywany jest z matrycy CCD, co umożliwia pomiar wymiarów i kształtu ręki oraz tworzony jest wzorzec, zapisywany wraz z numerem ewidencyjnym osoby. Wzorce w tej technice zajmują wyjątkowo mało miejsca w pamięci – zwykle od kilku do kilkunastu bajtów.

Mimo znacznej popularności tej metody, gdyż oprócz kontroli dostępu stosuje się ją również przy rejestracji czasu pracy, a także przy kontroli granicznej i w bankach, zajmuje się nią niewiele firm biometrycznych, z których najbardziej znaną jest Recognition Systems (RSI). Czytniki tego rodzaju działają poprawnie mimo postępujących zmian wymiarów ręki. Istnieją również ich specjalne wykonania, wymagające np. poprawnej pracy przy specjalnie trudnych warunkach zewnętrznych.

Więcej o tej technice i innych technikach związanych z ręką człowieka można dowiedzieć się z prac [6,7], a przykłady czytników podane będą w punkcie 4.

2.3 Geometria twarzy

Jest to metoda mniej rozwinięta od dwóch uprzednio omawianych (7,1% udziału w rynku biometrycznym w 1999 roku – [2]), ale czyniąca postępy (wzrost udziału z 2,3% w 1998 roku do 15,1% w 1999 roku w dziedzinie fizycznego dostępu – [3]). Nawiązuje niewątpliwie do stosowanych od dawna dokumentów ze zdjęciem, ale ze względu na stosowany algorytm, oparty na tworzeniu geometrycznej siatki charakterystycznych punktów twarzy [8] i automatycznym porównywaniem z wzorcem, jest bardziej skuteczna od subiektywnych decyzji sprawdzających dokument.

Pomiar dokonywany jest przy pomocy jednej lub kilku kamer, kiedy to uzyskuje się obraz przestrzenny, a orientacja twarzy następuje poprzez ustalenie położenia oczu. Aby uniknąć prób podsunięcia kamerze zdjęcia, stosuje się w złożonych układach nie tylko

zwiększenie ilości kamer, ale i odczyt termiczny, wykrywający różnice, niewidoczne optycznie.

Nowsze doniesienia [9,10] mówią o jeszcze większym udziale tej techniki w układach kontroli dostępu i walce sił porządkowych z terroryzmem i chuligaństwem na stadionach, często we współpracy z telewizją przemysłową.

2.4 Tęczówka oka

Jest to najszybciej rozwijająca się metoda biometryczna. W dziedzinie kontroli fizycznego dostępu [3] jej zastosowanie wzrosło z 0,5% w 1998 roku do 4,25% w roku 1999, kiedy to jej udział w całym rynku biometrycznym wyniósł 3,7% [2] i według [11] osiągnął ponad czterokrotny wzrost w ciągu 21 miesięcy. Można powiedzieć, że technika ta w ostatnim okresie czasu przesunęła się z grupy drugorzędnych, egzotycznych metod do jednej z bardziej poszukiwanych na rynku [12]. Spowodowane jest to dużą ilością (dwieście kilkadziesiąt) punktów charakterystycznych tęczówki, która okazuje się być najbardziej matematycznie rozróżnialną cechą ludzkiego ciała i daje trafność identyfikacji lepszą niż przy użyciu linii papilarnych, a nawet DNA. Jest to przy tym metoda nieinwazyjna, pomiar dokonywany jest z odległości kilku do kilkudziesięciu centymetrów, przy użyciu ewentualnie kamer naprowadzających. Na wynik nie wpływają żadne okulary ani soczewki kontaktowe.

Zakres zastosowań jest bardzo wszechstronny i wciąż rośnie. Wzorce zajmują nieco więcej miejsca niż w metodach tutaj omawianych (zwykle 512 bajtów), a cena urządzeń jest jeszcze wysoka, ale i tu obserwuje się postęp. Główną firmą działającą w tej dziedzinie jest Iriscan, która opatentowała w wielu krajach większość związanych z tym rozwiązań.

2.5 Siatkówka oka

Wykorzystanie cech siatkówki oka (przede wszystkim rozkładu jej naczyń krwionośnych) jako techniki biometrycznej rozpoczęto nawet wcześniej niż tęczówki. Jej stabilność i unikalność jest równie wysoka. Ze względu na usytuowanie wewnątrz oka jest ona doskonale chroniona, a użytkownik musi wyrazić zgodę na oświetlenie dna oka promieniowaniem niskiej mocy i odczytanie kamerą obrazu siatkówki dla porównania z wzorcem. Tak więc mimo braku fizycznego kontaktu z urządzeniem, można mówić o pewnym stopniu inwazyjności w związku z koniecznością zbliżenia oka na odległość kilku centymetrów, możliwe jest też uszkodzenie przy zaistniałych błędach. W wyniku tego, mimo wysokiej precyzji i trudnej dostępności, metoda ta nie rozwija się. W dziedzinie kontroli dostępu jej udział spadł dwukrotnie - z 0,9% w 1998 roku do 0,45% w roku 1999 [3], kiedy ogólny udział wyniósł tylko 0,6%. Nie można tu więc mówić o jakichś perspektywach. Wiodącą firmą jest tu EyeDentify.

2.6 Weryfikacja mówiącego

Omawiając tę metodę należy zwrócić uwagę na stosowaną terminologię. Jeżeli bowiem użyje się stosowanego czasami określenia „rozpoznawanie głosu" lub „rozpoznawanie mowy", to może to oznaczać, że chodzi nam o treść rozpoznawanej informa-

cji, a nie o osobę mówiącą. Dziedzina ta jest od dość dawna przedmiotem zainteresowania wielu firm biometrycznych (32 na 145 w 1999 r. – [1]). Tak jak w innych technikach porównuje się tu wzorzec zwykle konkretnych nagranych słów z aktualnie analizowanym głosem. Atrakcyjność metody polega na możliwości przeprowadzania pomiaru na odległość i wykorzystania jej w zastosowaniach takich jak telefony komórkowe, usługi bankowe w domu i handel elektroniczny. Jednakże duża wrażliwość na zmiany parametrów głosu spowodowane np. chorobą, czy stanem emocjonalnym mówiącego, zmniejsza użyteczność tej techniki w praktyce. Dlatego udział tej metody w układach kontroli fizycznego dostępu spadł z 28,6% w 1998 roku do 21,7% w roku 1999 [3] (udział w całym rynku biometrycznym wyniósł w 1999 roku 15,8%). Więcej na ten temat można znaleźć w przeglądach [13].

2.7 Weryfikacja podpisu

Ta ostatnia ze znaczących technik, chociaż nie odgrywa jeszcze większej roli na rynku (2,7% w 1999 r. – [2]). Uwierzytelnianie podpisem stosowane było oczywiście od wieków, ale biometryczna weryfikacja podpisu uwzględnia takie elementy jak szybkość i kolejność pisania, siłę nacisku w poszczególnych punktach, a nawet nachylenie narzędzia piszącego. Konwersję podpisu ręcznego do postaci cyfrowej realizuje się za pomocą specjalnych tabliczek, narzędzi piszących (piór), bądź rozwiązań niezależnych od sprzętu. Natomiast wśród zastosowań można by wymienić przede wszystkim handel elektroniczny. Do najbardziej znanych firm zajmujących się ta dziedziną należą CyberSign i PenOp, udział ma tu również IriScan. Bardziej wyczerpujące informacje zawierają przeglądy [14].

2.8 Inne techniki

Oprócz omówionych wyżej technik „głównego nurtu" istnieją metody, które nie odgrywają, bądź jeszcze nie zaczęły odgrywać znaczącej roli w praktycznych rozwiązaniach. Wymienić można tu rozpoznawanie kształtu ucha, gdyż odciski takie często znajdowane są na miejscu przestępstw. Aktywne są tu zwłaszcza instytucje i firmy europejskie [11]. Obiecująco wygląda również pomiar dynamiki uderzeń w klawiaturę, tym bardziej, że nie potrzeba tu dodatkowego sprzętu, a oprogramowanie nie jest drogie. Opatentował je między innymi kanadyjski dostawca NetNanny Software, lecz działa tu również wiele ośrodków uniwersyteckich jak New Mexico State University. Pojawiają się też pierwsze prace w dziedzinie rozpoznawania zapachów (np. firma Mastiff Electronics), ale trzeba jeszcze poczekać na rozwój sensorów i zastosowań tego typu. Ostatnią z tych drugoplanowych technik jest weryfikacja sposobu chodzenia, będąca między innymi przedmiotem badań uniwersytetu w Southamptom. Można jeszcze wspomnieć o badaniu ruchu warg, co stosuje niemiecka firma DCS, która w swym wyrobie *BioID* wykorzystuje rozpoznawanie twarzy, głosu i właśnie ruchu warg.

Do mniej znaczących, ale już istniejących na rynku, należy zaliczyć technikę rozpoznawania układu żył na dłoni. Kierunek ten reprezentuje południowo-koreańska firma B-K (zewnętrzne powierzchnie dłoni) i brytyjska firma Neusciences (zastosowanie jako jedna z technik dla wielofunkcyjnych kart inteligentnych).

3. Urządzenia biometryczne i ich parametry

Omówione wyżej techniki wykorzystywane są w różnego rodzaju systemach stosowanych do identyfikacji i weryfikacji osób. Systemy identyfikacyjne porównują daną cechę biometryczną, znalezioną np. na miejscu przestępstwa, z wieloma zapisami tej cechy, przechowywanymi zwykle w bazie danych i w wyniku uzyskujemy jednoznaczną lub prawdopodobną identyfikację. Natomiast systemy weryfikacyjne dokonują najpierw rejestracji wzorca danej cechy, a przy weryfikacji dokonywane jest porównywanie mierzonej cechy z tym wzorcem w celu otrzymania jednoznacznej odpowiedzi, czy osoba jest rzeczywiście tą, za którą się podaje. Wybór wzorca następuje zwykle przez wprowadzenie numeru identyfikacyjnego weryfikowanego użytkownika. W obu przypadkach wykorzystujemy urządzenia służące do odczytu, analizy i porównania danej cechy, zwanych zwykle czytnikami biometrycznymi, które dla identyfikacji są zwykle bardziej rozbudowane i droższe (często rzędu setek tysięcy dolarów), a dla weryfikacji możliwie uproszczone i znacznie tańsze.

Mają one różną organizację od prostych czytników wykonujących tylko odczyt, ewentualnie digitalizację i transmisję nieprzetworzonych danych poprzez interfejsy takie jak RS170, Centronics lub USB, poprzez czytniki wyposażone w procesor i pamięć, wykonujące weryfikację i transmitujące wynik najczęściej poprzez interfejs RS232, a także terminale, które poza funkcjami czytnika realizują funkcje wykonawcze, np. sterują ryglem drzwi. Wybór rozwiązań określa środki, jakie trzeba przedsięwziąć dla ochrony np. nieprzetworzonych danych osobowych.

Zarówno całe systemy jak i poszczególne urządzenia można scharakteryzować poprzez zespół parametrów określających ich jakość. Najbardziej znane z nich to:

1. współczynnik fałszywej akceptacji osoby nieuprawnionej (FAR),
2. współczynnik fałszywego odrzucenia uprawnionej osoby (FRR), podawane są wykresy zmian tych współczynników w funkcji wartości progu i punkt ich przecięcia nazywa się EER (Equal Error Rate),
3. czasy rejestracji, weryfikacji lub identyfikacji określane zwykle w sekundach,
4. pojemność (długość) i ilość zapisywanych w urządzeniu wzorców.

Dodatkowe parametry mogą dotyczyć takich wielkości jak graniczne napięcia wyładowań elektrostatycznych, ilości przechowywanych wzorców itp.

Możliwe jest także tworzenie systemów, obejmujących kilka różnych technik biometrycznych (tzw. biometria warstwowa, ang. layered) i wówczas parametry wypadkowe mogą być korzystniejsze niż dla poszczególnych podzespołów składowych.

4. Realizacje przykładowe

Rozwój biometrii w ostatnich latach dostarcza ciągle nowe opracowania w tej dziedzinie, charakteryzujące się coraz lepszymi parametrami i niższą ceną. Krótko omówimy tu tylko nieliczne przykłady dla poszczególnych technik

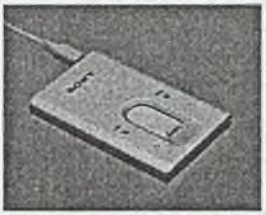
4.1 Linie papilarne

Rys 1

Rys. 1 przedstawia czytnik IMMSkan 100 wykorzystujący głowicę Sony FIU 500 F 13, działającą na zasadzie matrycy CCD. Jego podstawowe parametry to FAR mniejsze lub równe 0,1%, FRR mniejsze lub równe 1%, czas rejestracji poniżej 1 sekundy, a czas weryfikacji poniżej 0,1 sekundy.

Rys. 2

Na rys. 2 natomiast przedstawiony jest czytnik firmy Guard wykorzystujący nowoczesny, półprzewodnikowy sensor linii papilarnych FPS110 firmy Veridicom, w którym znajduje się matryca 300x300 płytek pojemnościowych. Współczynnik FAR jest tu mniejszy od 0,01%, a FRR nie większy od 1%. Posiada on wbudowany konwerter analogowo cyfrowy, zamieniający zmierzone różnice pojemności na 8-cyfrową liczbę.



Rys. 3

Jeszcze inny czytnik, o płaskim kształcie wielkości karty kredytowej (ale o grubości 8,6 mm), ważący tylko 37 gramów (rys 3), to czytnik FIU-710 firmy Sony o parametrach FAR i FFR takich samych jak czytnik z rys 1. Działa on również z sensorem półprzewodnikowym o matrycy 128x192 pikseli (10,2x15,4 mm). Czasy rejestracji i weryfikacji wynoszą co najwyżej 1 sekundę. Poszczególne wzorce zajmują 512 bajtów, a pojemność pamięci wynosi 512 kB. Ponadto posiada on także funkcje kryptograficzne (algorytm symetryczny DES 56-bitowy, asymetryczny RSA 1024-bitowy i spełnienie normy PKCS#11), co wraz z możliwością podpisu cyfrowego wprowadza nowy standard bezpieczeństwa informacji. Wykorzystuje on szynę USB zarówno do zasilania jak i przesyłania danych.

4.2 Geometria dłoni

Rys. 4

Rys 4 przedstawia czytnik Handpunch 3000 firmy Recognition Systems. Jest on znacznie większy (22,3 x29,6x21,7 cm – szer. x wys. x głęb.) i cięższy (2,7 kg) od poprzednio omawianych czytników. Czas weryfikacji też wynosi poniżej 1 sekundy, a liczba rejestrowanych użytkowników standardowo 512 z możliwością powiększenia do 32512. Użytkownik ma do dyspozycji 10 poziomów ufności. Czytniki takie oferowane są również na naszym rynku z systemem kontroli dostępu lub rejestracji czasu pracy XChronos opracowanym przez IMM m. in. przez firmę jak Andover Controls.

4.3 Tęczówka oka

Rys 5

System Sensar firmy o tej samej nazwie oferowany u nas przez Apexim zapewnia bezinwazyjną i niekłopotliwą dla użytkownika metodę rejestracji i uwierzytelniania. W urządzeniu znajdują się trzy kamery. Jedną z nich pokazuje rys 5. Najpierw powstaje przybliżony obraz osoby i zostaje odnalezione oko. Potem robione jest zdjęcie tęczówki o wysokiej rozdzielczości. Prawdopodobieństwo błędu jest rzędu 10^{-10}. Wadą jest stosunkowo długi czas rejestracji (około 30 sekund), ale czas identyfikacji wynosi już tylko 2-4 sekundy. Nawet przymknięcie oczu nie wpływa na wynik rejestracji.

5. Zastosowania

Metody biometryczne coraz częściej stosowane są w różnych dziedzinach, gdy zawodzą metody tradycyjnych zabezpieczeń. Udział poszczególnych zastosowań w rynku biometrycznym zmienia się z upływem czasu [2], ale wciąż dominuje tu kontrola fizycznego dostępu, która pod koniec 1996 roku stanowiła 63% tego rynku, a trzy lata później tylko 38,4%. Na drugim miejscu znalazło się wówczas prawo i porządek (19,2%), który to dział tylko na początku 1998 roku dał się wyprzedzić zastosowaniom medycznym. Natomiast udział zastosowań finansowych wzrósł w tym okresie ponad trzykrotnie osiągając 17% w grudniu 1999. Ostatnim znaczącym zastosowaniem biometrycznym jest właśnie służba zdrowia, która w ostatnich dwóch latach nie zwiększała swego udziału. Potem idą: imigracja (5,3%), omawiana tu krótko przy prawie i porządku, ubezpieczenia społeczne (3,9%), zaliczone do systemów płatniczych i zabezpieczenia komputerów (3,8%) oraz telekomunikacja (2,8%). Te dwa ostatnie działy, chociaż jeszcze marginalne, mają szansę na zwiększenie swego udziału. Poniżej przedstawiono krótkie omówienie najważniejszych zastosowań głównie na podstawie przeglądu zamieszczonego w czasopiśmie Biometric Technology Today.

5.1 Kontrola fizycznego dostępu [3]

Jest to niewątpliwie podstawowy obszar wszelkich zabezpieczeń i usprawnienia w tej dziedzinie musiały objąć omawiane tu metody, jako najbardziej pewne i niezawodne. Początkowo, ze względu na wysokie koszty z systemów biometrycznych mogły korzystać tylko bogate instytucje rządowe i wojskowe, obecnie przy znacznym spadku cen biometryczne układy dostępu wchodzą do powszechnego użytku. Stosowane są w rozwiązaniach inteligentnych budynków różnej wielkości, do kontroli wejścia na teren różnych instytucji i stref w nich chronionych. Wyodrębnił się tu kierunek rejestracji czasu pracy, ułatwiający zakładom pracy kontrolę obecności pracowników, a potem przygotowanie list płac. W 1999 roku kierunek ten stanowił ponad 10% instalacji biometrycznych. Systemy kontroli dostępu wchodzą też w skład innych omawianych tu zastosowań i wykorzystują niemal wszystkie omawiane techniki, choć wyróżnić tu można czytniki Handkey firmy RSI wykorzystywane i w punktach sprzedaży hodow-

ców świń w Montanie (USA) i w holenderskich więzieniach. Projektowane są też układy dostępu do droższych pojazdów.

5.2 Prawo i porządek [15]

Jednym z najbardziej masowych zastosowań w tej dziedzinie, a może i całej biometrii są dokumenty tożsamości wykorzystujące techniki biometryczne. Najczęściej spotkać je można w krajach rozwijających się, a typową przyczyną ich wydania była rejestracja wyborców. W przeważającej liczbie rozwiązań stosowano technikę linii papilarnych (połowa systemów to AFIS), przy czym w większości połączone to było z stosowaniem jakichś kart, najczęściej z kodem kreskowym. Ciekawym rozwiązaniem jest system na Filipinach, gdzie są to nieobowiązkowe karty ubezpieczeń społecznych, ale uzyskały powszechną aprobatę i stały się faktycznymi dowodami tożsamości. Przykładem lokalnego wykorzystania biometrycznych dokumentów identyfikacyjnych mogą być prawa jazdy wydawane w indyjskim stanie Gujarat na kartach inteligentnych.

Wiele z omawianych systemów stosują służby imigracyjne, zwłaszcza w USA. System INSPASS umożliwia rejestrację z dużą wydajnością często podróżujących wykorzystując technikę geometrii dłoni. Obecnie w zastosowaniach tych pojawiają się karty inteligentne zawierające wzorce linii papilarnych [16] i systemy tęczówki oka [17]. Szeroki rozgłos uzyskał izraelski projekt Basel, gdzie początkowo chodziło o 40 tys. robotników palestyńskich przekraczających codziennie granice Izraela i proponowano technikę linii papilarnych lub kształtu dłoni. Później okazało się [18], że system ma obsługiwać dwukrotnie większą ilość osób, a za rozwiązanie docelowe przyjęto jednocześnie sprawdzanie geometrii dłoni i rozpoznawania twarzy.

W więzieniach zastosowano wiele interesujących nas systemów, najwięcej w USA, Wielkiej Brytanii i Meksyku. Polowa z nich działała w oparciu o technikę rozpoznawania kształtu dłoni, najczęściej firmy RSI, a 30% wykorzystywało linie papilarne. Jeden z większych kontraktów był podpisany przez holenderskie Ministerstwo Sprawiedliwości z firmą Iolan na instalację w więzieniach tego kraju 10 tys. czytników Handkey II wraz z czytnikami kart Milfare.

Ożywioną dyskusję w prasie USA wywołały propozycje „inteligentnej broni", z której mógłby strzelać tylko zarejestrowany właściciel lub osoba uprawniona. Oferty złożyli tu producenci sensorów krzemowych ze wspomożeniem firm specjalistycznych.

5.3 Systemy płatnicze [19]

Obejmują one zarówno banki jak i ubezpieczenia społeczne, przy czym w pierwszym przypadku chodzi głównie o weryfikację transakcji, a w drugim o bezpieczną rejestrację. O ile w systemach fizycznego dostępu metody biometryczne mogły eliminować karty, tutaj techniki te wykorzystuje się do weryfikacji posiadacza karty najczęściej inteligentnej. W tym celu umieszcza się ostatnio [20] na karcie już nie tylko wzorce biometryczne, co czyni zbędnym przesyłanie ich do zewnętrznych baz danych, ale sensory linii papilarnych, co umożliwia odczyt palca i przeprowadzenie dopasowania na karcie. Tak samo łączy się biometrię z infrastrukturami klucza publicznego (PKI – Public Key Infrastructures), by uczynić certyfikaty bardziej efektywnymi. To wszystko

przyczyni się również do znacznego rozwoju handlu elektronicznego i możliwości świadczenia usług bankowych w domu za pomocą Internetu. Szczególnie istotne jest tu zabezpieczenie bankomatów, gdzie technika tęczówki wydaje się najodpowiedniejsza, choć w omawianym przeglądzie zastosowań płatniczych była ona na trzecim miejscu (11,5%) po liniach papilarnych (34,5%) i kształcie dłoni (23,1%).

Jeśli chodzi o ubezpieczenia społeczne, to główną rolę odgrywają systemy AFIS (41,5% same, a ponadto w kombinacji z rozpoznawaniem ręki, twarzy i siatkówki – łącznie 57,7%). Oprócz wspomnianego już systemu na Filipinach, który już w sierpniu 1999 roku [18] obsługiwał 21 milionów ludzi, znany jest też wcześniejszy (1996) projekt hiszpański, gdzie wykorzystywano linie papilarne i karty inteligentne w Andaluzji, ale nie rozszerzano systemu na cały kraj.

5.4 Służba zdrowia [21]

Ten rodzaj zastosowań rozwinął się przede wszystkim w USA ze względu na ostre przepisy odnośnie prywatności i identyfikacji. Chodziło głównie o rejestrację pacjentów i historię ich chorób. Posługiwano się tu najczęściej liniami papilarnymi i tęczówką, wykorzystując systemy firm NEC i IriScan. Innym zastosowaniem jest tu automatyczne podawanie leków, lecz tutaj wykorzystywano też rozpoznawanie głosu i twarzy firm Keyware Technologies i Visionics.

6. Rynek biometryczny

Jest to stosunkowo młody, dopiero rozwijający się rynek. Jego początki [1] sięgają lat 70 i 80-tych, kiedy powstało kilkanaście niewielkich firm, dopiero formułujących podstawy nowych koncepcji, a których pierwsze wyroby oparte były na tradycyjnych technologiach. Dopiero lata 90-te przyniosły zarówno wzrost nakładów na badania jak i wzrost ilości firm (około 150 w 1999 roku), a przede wszystkim realizację różnych projektów zastosowań jak omawiane w dziedzinie ubezpieczeń społecznych czy eksperyment w bazie wojskowej Ft. Sill z zakupami elektronicznymi dla 20 tysięcy żołnierzy. Jest to jednocześnie okres znacznych zmian, kiedy firmy łączą się i są wykupywane. Np. wytwórca najpopularniejszych czytników linii papilarnych *DFR-200* (ponad 100000 sprzedanych urządzeń) firma Identicator została wchłonięta przez firmę Identix [22] w połowie 1999 roku, a ostatnio [23] ogłoszono o połączeniu się czołowych firm techniki tęczówki oka. Przychody niektórych firm (Printrak) osiągnęły 100 mln dolarów w 1998 roku. Wzrasta też zainteresowanie inwestorów tą dziedziną, a są wśród nich Citibank, Intel, Lucent Technologies i inni. Notowania firm biometrycznych na giełdach przebiegają podobnie do innych firm nowych technologii [24].

Podział rynku na techniki i zastosowania omawiany był już poprzednio, natomiast podział geograficzny wyglądał na koniec 1999 roku w ten sposób [2], że Ameryka Płn. stanowiła 57% tego rynku, Europa (bez Wschodniej) – 18%, Azja i kraje Pacyfiku – 9,5%, Ameryka Płd. – 9,3%, Afryka i Bliski Wschód – 4,4% i Europa Wschodnia 1,8%. Zmiany w tym zakresie można prześledzić na podstawie rynku kontroli fizycznego dostępu [3], gdzie w latach 1998-99 udział Ameryki Płn zmalał z 74,7 do 59,4%, Europy wzrósł z 7,4 do 23,8%, Azji i Pacyfiku zmalał z 12 do 10%, Ameryki Płd.

zmalał z 5,1 do 3%, Afryki i Bliskiego Wschodu wzrósł z 0,5 do 3%, a Europy Wschodniej wzrósł z 0,5 do 0,85%.

7. Doświadczenia IMM w zakresie wdrażania metod biometrycznych

Instytut Maszyn Matematycznych rozpoczął prace w dziedzinie metod biometrycznych od opracowania w 1998 roku systemu kontroli dostępu oraz rozliczania czasu pracy XChronos wykorzystującego czytniki linii papilarnych Fingerscan firmy Identix. Próby zainteresowania nim krajowych odbiorców napotkały na poważne opory. Z przeprowadzonych przez nas analiz wynikało, że wystąpiły trzy bariery w zakresie zastosowań. Pierwsza to wysoka cena czytnika (ponad 10000 zł), druga to bariera psychiczna przed zdejmowaniem linii papilarnych, a trzecia to brak zrozumienia przez pracodawców, że karta nie identyfikuje osoby, co w praktyce prowadzi do pożyczania kart przez pracowników. Natomiast ze strony nieuczciwych pracowników uświadomienie pewności tej weryfikacji doprowadzało nawet do wystąpienia problemu niszczenia fizycznego urządzenia.

W tej sytuacji w 1999 roku podjęliśmy zadanie opracowania taniego czytnika linii papilarnych, który został pokazany na wystawie Innowacje w Łodzi i otrzymał tam wyróżnienie. Wykorzystano w nim głowicę firmy Sony. Seria próbna tego czytnika znalazła zastosowanie w prywatnych firmach, głównie w systemach rejestracji czasu pracy, przy czym okazało się, że system jest bardziej przydatny w miejscach pracy typu biuro lub nowoczesne zakłady produkcyjne, a mniej w tych miejscach, gdzie w procesie pracy występują uszkodzenia skóry palców. Dlatego w miejscach takich korzystniejszy jest czytnik geometrii dłoni i taki został w 2000 roku wprowadzony do systemu zwiększając listę odbiorców. W dalszym ciągu natomiast istnieją obawy przed odtwarzaniem pełnego obrazu zapisanych linii papilarnych, podczas gdy w rzeczywistości we wzorcach zapisywane są tylko punkty charakterystyczne, niezbędne do weryfikacji, z których nie można odtworzyć tego obrazu.

Dodatkowym problemem w polskich warunkach jest powszechne stosowanie wykładzin dywanowych i ubraniowych materiałów syntetycznych nie zapewniających antystatyczności, co prowadzi do powstawania dużych ładunków elektrostatycznych i w konsekwencji naraża czytniki na silne wyładowania elektrostatyczne. Zwrócono więc szczególna uwagę w naszym opracowaniu na uodpornienie urządzeń na wyładowania elektrostatyczne zwłaszcza, że rozpoznanie wśród krajowych dostawców tego sprzętu wykazało, że wielu producentów tego nie doceniło, co prowadzi do pewnych problemów eksploatacyjnych (częste występowanie przekłamań, zawieszanie działania systemu, uszkodzenia).

W niektórych zastosowaniach wymagane są bardzo niskie wartości parametrów FAR i FRR, co zapewniają obecnie rozwiązania sensorowe. Dlatego IMM opracowuje nową wersję czytnika opartą na rozwiązaniu sensorowym zapewniającą te parametry na poziomie czytnika Fingerscan firmy Identix.

Opracowane w Instytucie czytniki dzięki modułowej budowie i mikroprocesorowemu sterowaniu zapewniają możliwość łatwego dostosowania parametrów do wymagań różnych odbiorców (np. zapis kilku odcisków palców dla jednego użytkownika, różne rodzaje interfejsu, łatwa integracja z innymi systemami itp.).

8. Dwa słowa o standardach

Tak jak w każdej nowej dziedzinie, wytwórcy zastosowań biometrycznych wprowadzają swe własne rozwiązania, które potem wspólnie trudno integrować. Dlatego postęp w tej dziedzinie uwarunkowany jest nie tylko usprawnieniami technicznymi, ale i opracowywaniem oraz przyjmowaniem właściwych standardów.

Najwięcej zrobiono w zakresie interfejsu programów użytkowych (API – Application Program Interface). Początkowo powstało nawet zbyt wiele inicjatyw w tym zakresie, które następnie łączyły swe wysiłki, by w końcu utworzyć konsorcjum BioAPI złożone z ponad 50 firm i organizacji, które w końcu marca 2000 roku opublikowało *BioAPI V1.0* [25]. Pewne zamieszanie wniosło potem oświadczenie Microsoftu, iż ma on zamiar wykorzystać w następnej wersji systemu Windows standard BAPI, opracowany przez firmę I/O Software, która jest aktywnym członkiem konsorcjum BioAPI.

Podejmowane są różne działania w zakresie normalizacji danych biometrycznych, zwłaszcza danych rejestracji, oraz standardów łączących biometrię, PKI i karty inteligentne. Więcej danych na ten temat można znaleźć w przeglądach [26, 27].

Literatura

[1] Erik Bowman, Identix Corporation: Everything You Need to Know About Biometrics, January 2000

[2] Survey – 1999 Market Review, Biometric technology today (Btt), no 8 v. 7, 2000, s. 8-11

[3] Survey – Physical access control, Btt, no 5 v. 7 1999, s. 8-11 Survey – Finger technologies point way ahead, Btt, no 10 v. 6, 1999 s. 8-16

[4] Survey – Finger technologies point way ahead, Btt, no 10 v. 6, 1999 s. 8-16

[5] Survey – Silicon fingerprint sensors, Btt, no 2 v. 8, 2000 s. 8-11

[6] Survey – Hand measuring systems, Btt, no 4 v. 7, 1999 s. 9-12

[7] Rozbicki L., Ryżko J., Sławiński J.: Czytniki biometryczne związane z wykorzystaniem ręki człowieka – przegląd metod realizacji, zastosowania, przykłady rozwiązań, I Szkoła-Konferencja „Nowoczesne Techniki Ochrony" Rynia k/Warszawy 25-27 wrzesień 2000 r.

[8] Nitka A.: Biometria w technice zabezpieczeń, j.w.

[9] Survey – Face recognition, Btt, no 6 v. 7, 1999 s. 8-12

[10] Football hooligans meet their match at West Ham, Btt, no 9 v. 7, 2000 s. 2

[11] Survey – Other biometrics, j. w. s. 8-11

[12] Iris gains market recognition, j. w. s. 9

[13] Survey – Speaker verificatiom, Btt, no 2 v. 7, 1999 s.9-12, 10 v. 7, 2000 s. 8-11

[14] Survey – Signature Verification Technologies, Btt, no 2 v. 7, 1999 s. 7-9, no 1 v. 1, 2000 s. 8-11

[15] Survey – Law & order – national ID, immigration and prisons, Btt, no 9 v. 6, 1999 s. 9-16

[16] 'Touch and go' passport clearance for Malaysians, UAE prepared to bring in biometric ID cards?, Btt, no 5 v. 8, 2000 s. 4

[17] Olympic success for EyeTicket... as US airport enters second stage of iris test, j.w. s. 5

[18] Project management – Special report: Managing biometrics, Btt, no7 v. 7, 1999, s. 8-11

[19] Survey – Payments systems – banking & welfare, Btt, no 1 v. 7, 1999, s. 7-11

[20] Survey – Biometrics and smart cards, Btt no 4 v. 8, 2000 s. 8-11

[21] Survey – The healthcare market, Btt, no 3 v. 3, 1999 s. 7-11

[22] L. Whitted, J. Loughran: Making a Market in Biometrics, presentation to the IBIA, 15IX1999 L. Whitted, J. Loughran: Making a Market in Biometrics, presentation to the IBIA, 15I.X.1999

[23] Iriscan and Sensar find synergies in merger, Btt, no 5 v. 8, 2000 s. 2

[24] Survey – Financing the biometrics business, Btt, no 3 v. 8, 2000 s. 8-11

[25] BioAPI standard marks major industry milestone, Btt, no 2 v. 8, 2000 s. 2

[26] Update – Latest developments in standards and testing, Btt, no 4 v. 7, 1999 s. 7-8.

[27] Survey – APIs and Interoperability, Btt, no 5 v. 8, 2000 s. 8-11