

Chapter 1

Introduction to Synthesis in Biometrics

S. Yanushkevich*, V. Shmerko†, A. Stoica‡, P. Wang§, S. Srihari¶

*Biometric Technology Laboratory: Modeling and Simulation,
University of Calgary, Canada*

* *syanshk@ucalgary.ca*

† *vshmerko@ucalgary.ca*

*Humanoid Robotics Laboratory, California Institute of Technology,
NASA Jet Propulsion Laboratory, California Institute of Technology,
Pasadena, CA, USA*

‡ *adrian.stoica@jpl.nasa.gov*

Image Processing Group, Northeastern University, Boston, MA, USA

§ *pwang@ccs.neu.edu, patwang@mit.edu*

*Center of Excellence for Document Analysis and Recognition,
State University of New York at Buffalo, Amherst, NY, USA*

¶ *srihari@cedar.buffalo.edu*

The primary application focus of biometric technology is the verification and identification of humans using their possessed biological (anatomical, physiological and behavioral) properties. Recent advances in biometric processing of individual biometric modalities (sources of identification data such as facial features, iris patterns, voice, gait, ear topology, etc.) encompass all aspects of system integration, privacy and security, reliability and countermeasures to attack, as well as accompanying problems such as testing and evaluation, operating standards, and ethical issues.

Contents

1.1.	Introduction	6
1.1.1.	Basic Paradigm of Synthetic Biometric Data	7
1.2.	Synthetic Approaches	9
1.2.1.	Image Synthesis	9
1.2.2.	Physics-Based Modeling	10

- 1.2.3. Modeling Taxonomy 10
- 1.3. Synthetic Biometrics 10
 - 1.3.1. Synthetic Fingerprints 10
 - 1.3.2. Synthetic Signatures 12
 - 1.3.3. Synthetic Retina and Iris Images 13
 - 1.3.4. Synthetic Speech and Voice 16
 - 1.3.5. Gait Modeling 16
 - 1.3.6. Synthetic Faces 16
- 1.4. Examples of Usage of Synthetic Biometrics 20
 - 1.4.1. Testing 20
 - 1.4.2. Databases of Synthetic Biometric Information 21
 - 1.4.3. Humanoid Robots 21
 - 1.4.4. Cancelable Biometrics 22
 - 1.4.5. Synthetic Biometric Data in the Development of a New Generation of Lie Detectors 22
 - 1.4.6. Synthetic Biometric Data in Early Warning and Detection System Design 23
- 1.5. Biometric Data Model Validation 24
- 1.6. Ethical and Social Aspects of Inverse Biometrics 24
- 1.7. Conclusion 25
- Bibliography 25

1.1. Introduction

The typical application scenario of biometric technologies involves the interaction of different levels of physical access control with different levels of data sensors. The human user of a the biometric system is at the center of this interaction. The centre in this interaction is the human user of a biometric system. The system must assist the user by providing high quality biometric data to ensure optimal system operation, e.g. to minimize false rejection errors or to provide early warning information.

This chapter addresses important questions of protecting against an attack on biometric systems. It focuses on studying the extent to which artificial, or synthetic biometric data (e.g. synthesized iris patterns, fingerprint, or facial images) can be useful in this task. Artificial biometric data are understood as biologically meaningful data for existing biometric systems. Synthetic biometric data can be useful for:

- (a) Testing biometric devices with “variations” or “forgeries” of biometric data,
- (b) Simulation of biometric data on computer-aided tools (decision-making support, training systems, etc.)

Testing biometric devices is of urgent importance [32,56] and can be accomplished by providing variations on biometric data mimicking unavailable or hard to access data (for example, modeling of badly lit faces, noisy

iris images, “wet” fingerprints etc.) Synthetic data can also be used for “spoofing” biometric devices with “forged” data. We argue that synthetic biometric data can:

Improve the performance of existing identification systems. This can be accomplished by using automatically generated biometric data to create statistically meaningful sets of data variations (appearance, environmental, and others, including “forgeries”).

Improve the robustness of biometric devices by modeling the strategies and tactics of forgery.

Improve the efficiency of training systems by providing the user-in-training with the tools to model various conditions of biometric data acquisition (non-contact such as passive surveillance, contact, cooperative, non-cooperative), environmental factors (light, smog, temperature), appearance (aging, camouflage).

Therefore, synthetic biometric data plays an important role in enhancing the security of biometric systems. Traditionally, security strategies (security levels, tools, etc.) are designed based on assumptions about a *hypothetical* robber or forger. Properly created artificial biometric data provides for detailed and controlled modeling of a wide range of training skills, strategies and tactics, thus enabling a better approach to enhancing the system’s performance. This study aims to develop new approaches for the detection of attacks on security systems. Figure 1.1 introduces the basic configuration for inverse biometric problems.

1.1.1. *Basic Paradigm of Synthetic Biometric Data*

Contemporary techniques and achievements in biometrics are being developed in two directions:

Analysis for identification and recognition of humans (direct problems) and
Synthesis of biometric information (inverse problems) (Fig. 1.1).

Note that synthesis also means modeling. In general, modeling is considered to be an inverse problem in image analysis [9]. However, there are several differences between synthesis of realistic biometric data and modeling used in analysis.

Synthesis of artificial biometric data is the inverse task of analysis, performed as a part of the process of verification and identification. The crucial point of modeling in biometrics is the *analysis-by-synthesis* paradigm. This paradigm states that synthesis of biometric data can verify the perceptual equivalence between original and synthetic biometric data, i.e. synthesis

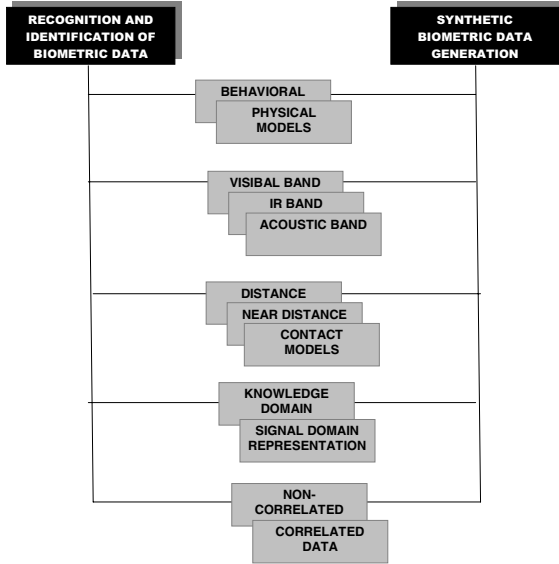


Fig. 1.1. Basic tools for inverse biometric problems include facilities for generation of synthetic data and its analysis.

based feedback control. For example, facial analysis can be formulated as deriving a symbolic description of a real facial image (Fig. 1.2). The aim of face synthesis is to produce a realistic facial image from a symbolic facial expression model [25].

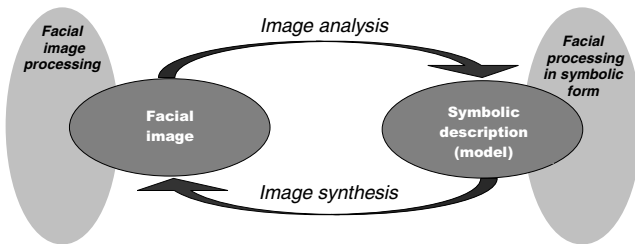


Fig. 1.2. Analysis-by-synthesis approach in facial image.

In Table 1.1, the basic terminology of synthetic biometrics is given. In particular, the term “face reconstruction” indicates a class of problems aimed at synthesizing a model of a static face. The term “mimics

animation” is defined as the process of modeling facial appearance and facial topology, a behavioral characteristic called facial expression, the visible result of synthetic emotion.

We consider synthetic single and synthetic multi-biometric data: eyes, hands, and face are multi-biometric objects because of the different topologies of the iris and retina of the eye; fingerprints, palmprints, and hand-geometry; face geometry which is a highly dynamic topological structure (smile, lip, brow, and eye movements). Synthetic signatures [20], [37], voice, and ears [21], [22] are examples of synthetic biometrics.

Table 1.1. Direct and inverse problems of biometric technology.

DIRECT PROBLEM	INVERSE PROBLEM
Signature identification	Signature <i>forgery</i>
Handwriting character recognition	Handwritten text <i>forgery</i>
face recognition	Face <i>reconstruction</i> and mimics animation
Voice identification and speech recognition	Voice and speech <i>synthesis</i>
Iris and retina identification	Iris and retina <i>image synthesis</i>
Fingerprint identification	Fingerprint <i>imitation</i>
hand geometry identification	Hand geometry <i>imitation</i>
Infrared identification	infrared image <i>reconstruction</i>
Gait identification	Gait <i>modeling</i>
Ear identification	Ear-print <i>imitation</i>

1.2. Synthetic Approaches

There are two approaches to synthetic biometric data design [39]:

- (a) Image synthesis-based, and
- (b) Statistical physics-based.

Both approaches use statistical models in the form of equations based on underlying physics or empirically derived algorithms, which use pseudo-random numbers to create data that are statistically equivalent to real data. For example, in face modeling, a number of ethnic or race models can be used to represent ethnic diversity, the specific ages and genders of individuals, and other parameters for simulating a variety of tests.

1.2.1. Image Synthesis

The image synthesis-based approach falls into the area of computer graphics, a very-well explored area with application from forensics (face reconstruction) to computer animation.

In generating physiological biometric objects (faces, fingerprints), the physics-based approach overlaps with the image-based approach, as it tries to model visual appearance and the physical properties and topology of the objects (including physics-based models to control physical form, motion and illumination properties of materials).

1.2.2. *Physics-Based Modeling*

Physics-based models attempt to mimic biometric data through the creation of a pattern similar to that acquired by biometric sensors, using knowledge of physical processes and sensor measurement.

1.2.3. *Modeling Taxonomy*

A taxonomy for the creation of physics-based and empirically derived models for the creation of statistical distributions of synthetic biometrics was first attempted in [5]. There are several factors affected the modeling biometric data: behavior, sensor, and environmental factors.

Behavior, or appearance, factors are best understood as an individual's presentation of biometric information. For example, a facial image can be camouflaged with glasses, beards, wigs, make-up, etc.

Sensor factors include resolution, noise, and sensor age, and can be expressed using physics-based or geometry-based equations. This factor is also relevant to the skills of the user of the system.

Environmental factors affect the quality of collected data. For example, light, smoke, fog, rain or snow can affect the acquisition of visual-band images, degrading the biometric facial recognition algorithm. High humidity or temperature can affect infrared images. This environmental influence affects the acquisition of fingerprint images differently for different types of fingerprint sensors.

1.3. Synthetic Biometrics

1.3.1. *Synthetic Fingerprints*

Albert Wehde was the first to “forge” fingerprints in the 1920s. Wehde “designed” and manipulated the topology of synthetic fingerprints at the physical level. The forgeries were of such high quality that professionals could not recognize them [11], [33]. Today's interest in automatic fingerprint synthesis addresses the urgent problems of testing fingerprint identification systems, training security personnel, biometric database security,

and protecting intellectual property [7,60].

Traditionally, two possibilities of fingerprint imitation are discussed with respect to obtaining unauthorized access to a system: (i) the authorized user provides his fingerprint for making a copy, and (ii) a fingerprint is taken without the authorized user's consent, for example, from a glass surface (a classic example of spy-work) by forensic procedures.

Cappelli et al. [6,7] developed a commercially available synthetic fingerprint generator called SFinGe. In SFinGe, various models of fingerprints are used: shape, directional map, density map, and skin deformation models (Fig. 1.3). To add realism to the image, erosion, dilation, rendering, translation, and rotation operators are used.



Fig. 1.3. Synthetic fingerprint assembly (growth) generated by SFinGe.

Methods for continuous growth from an initial orientation map, a new synthesized orientation map (as a recombination of segments of the orientation map) using a Gabor filter with polar transform (Fig. 1.4) have been reported in [60]. These methods alone can be used to design fingerprint benchmarks with rather complex structural features.



Fig. 1.4. Synthetic fingerprint assembly (growth) using a Gabor filter with polar transform.

Kuecken [26] developed a method for synthetic fingerprint generation based on natural fingerprint formation and modeling based on state-of-the-

art dermatoglyphics, a discipline that studies epidermal ridges on fingerprints, palms, and soles (Fig. 1.5).

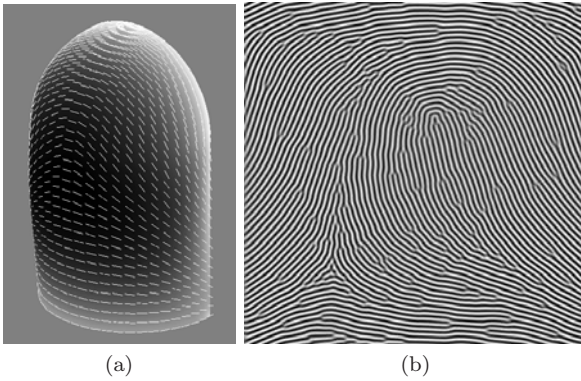


Fig. 1.5. Synthetic 3D (a) and 2D (b) fingerprint design based on physical modeling (reprinted with permission from Elsevier).

The methods of fingerprint synthesis can also be applied to synthetic palmprint generation. Note that the generation of synthetic hand topologies is a trivial problem.

1.3.2. *Synthetic Signatures*

Current interest in signature analysis and synthesis is motivated by the development of improved devices for human-computer interaction which enable input of handwriting and signatures. The focus of this study is the formal modeling of this interaction [4], [10], [20], [23], [37], [42], [44], [57].

Similarly to signature imitation, the imitation of human handwriting is a typical inverse problem of graphology. Automated tools for the imitation of handwriting have been developed. It should be noted that more statistical data, such as context information, are available in handwriting than in signatures.

The simplest method of generating synthetic signatures is based on geometrical models. Spline methods and Bezier curves are used for curve approximation, given some control points. Manipulations of control points give variations on a single curve in these methods [47,60].

The following evaluation properties are distinguished for synthetic signatures [60]: *statistical*, *kinematical* (pressure, speed of writing, etc.), *geometric*, also called *topological*, and *uncertainty* (generated images can be intensively “infected” by noise) properties.

An algorithm for signature generation based on deformation has been introduced in [37]. Hollerbach [23] has introduced the theoretical basis of handwriting generation based on an oscillatory motion model. In Hollerbach's model, handwriting is controlled by two independent oscillatory motions superimposed on a constant linear drift along the line of writing. There are many papers on the extension and improvement of the Hollerbach model.

To generate signatures with any automated technique, it is necessary to consider: (a) the formal description of curve segments and their kinematical characteristics, (b) the set of requirements which should be met by any signature generation system, and (c) possible scenarios for signature generation.

Various characteristics are used in so-called *off-line* (static) analysis and *on-line* (kinematic) analysis of the acquired signature.

A model based on combining shapes and physical models in synthetic handwriting generation has been developed in [57]. The so-called *delta-log normal model* was developed in [42]. This model can produce smooth connections between characters, but can also ensure that the deformed characters are consistent with the models. In [10], it was proposed to generate character shapes by Bayesian networks. By collecting handwriting examples from a writer, a system learns the writers' writing style.

An example of a combined model based on geometric and kinematic characteristics (in-class scenario) is illustrated by Fig. 1.6.

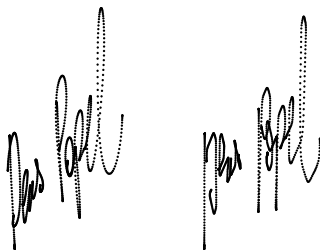


Fig. 1.6. In-class scenario: the original signature (left) and the synthetic one (right), courtesy of Prof. D. Popel, Baker University.

1.3.3. *Synthetic Retina and Iris Images*

Iris recognition systems scan the surface of the iris to compare patterns [13]. Retina recognition systems scan the surface of the retina and compare nerve patterns, blood vessels and such features. To the best of our knowledge,

automated methods of *iris* and *retina image reconstruction*, or *synthesis* have not been developed yet, except for an approach based on generation of iris layer patterns [47,60].

Iris pattern painting has been used by ocularists in manufacturing glass eyes or contact lenses for sometime. The ocularist's approach to iris synthesis is based on the composition of painted primitives, and utilized layered semi-transparent textures built from topological and optic models [27]. These methods are widely used by today's ocularists: vanity contact lenses are available with fake iris patterns printed onto them (designed for people who want to change eye colors). Other approaches include image processing and synthesis techniques such as PCA combined with super-resolution [13], and random Markov field [46].

A synthetic image can be created by combining segments of real images from a database. Various operators can be applied to deform or warp the original iris image: translation, rotation, rendering etc. Various model of the iris, retina, and eye can be used to improve recognition, and can be found in [8,34,48]. In [2], a cancelable iris image design is proposed for the problem as follows. The iris image is intentionally distorted to yield a new version. For example, a simple permutation procedure is used for generating a synthetic iris.

An alternative approach is based on synthesis of patterns of the iris layers [60] followed by superposition of the layers and the pupil (black centre).

Below is an example of generating posterior pigment epithelia of the iris using the Fourier transform on a random signal. A fragment of the FFT signal is interpreted as a grey-scaled vector: the peaks in the FFT signal represent lighter shades and valleys represent darker shades. This procedure is repeated for other fragments as well. The data plotted in 3D, a 2D slice of the data, and a round image generated from the slice using the polar transform, are shown in Fig. 1.7.

Other layer patterns can be generated based on wavelet, Fourier, polar, and distance transforms, and Voronoi diagrams [60]. For example, Fig. 1.8 illustrates how a synthetic collarette topology has been designed using a Bezier curve in a cartesian plane. It is transformed into a concentric pattern, and superimposed with a random signal to form an irregular boundary curve.

Superposition of the patterns of various iris layers form a synthetic iris pattern. Figure 1.9 illustrates three different patterns obtained by this method.

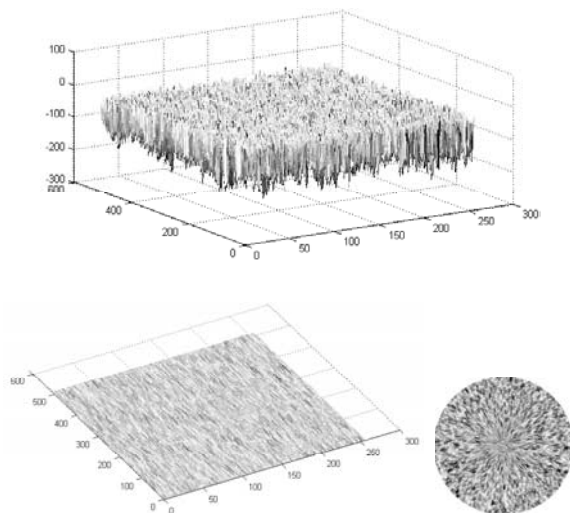


Fig. 1.7. A 3D grey-scale interpretation of the Fourier transform of a random signal, a slice of this image and the result of polar transform for a synthetic posterior pigment epithelia of the iris

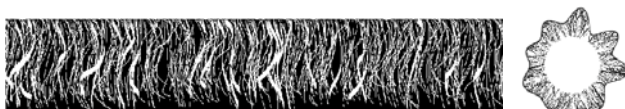


Fig. 1.8. Synthetic collarette topology modelled by Bezier curves and a randomly generated curve.

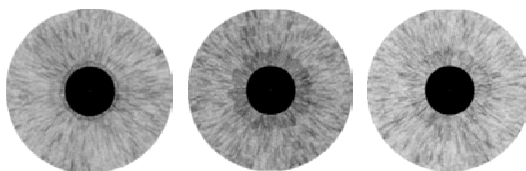


Fig. 1.9. Synthetic iris patterns.

1.3.4. *Synthetic Speech and Voice*

Synthetic speech and voice have evolved considerably since the first experiments in the 1960s. New targets in speech synthesis include improving the audio quality and the naturalness of speech, developing techniques for emotional “coloring” [12,16,52,58], and combining it with other technologies, for example, facial expressions and lip movement [16,38,58]. Synthetic voice should carry information about age, gender, emotion, personality, physical fitness, and social upbringing. A closely related but more complicated problem is generating a synthetic singing voice for training singers, studying the famous singers’ styles, and designing synthetic user-defined styles combining voice with synthetic music.

1.3.5. *Gait Modeling*

Gait recognition is defined as the identification of a person through the pattern produced by walking [14,35]. The potential of gait as a biometric was encouraged by the considerable amount of evidence available, especially in biomechanics literature [51,41]. A unique advantage of gait as biometrics is that it offers potential for recognition at a distance or at low resolution, when other biometrics might not be perceivable. As gait is behavioural biometrics there is much potential for within-subject variation [3]. This includes footwear, clothing and apparel. Recognition can be based on the (static) human shape as well as on movement, suggesting a richer recognition cue. Model-based techniques use the shape and dynamics of gait to guide the extraction of a feature vector.

Gait signature derives from bulk motion and shape characteristics of the subject, articulated motion estimation using an adaptive model and motion estimation using deformable contours; examples of all of these processes can be seen in Fig. 1.10.

The authors of [61] propose to use the gait biometrics in the pre-screened area of a security system.

1.3.6. *Synthetic Faces*

Face recognition systems detect patterns, shapes, and shadows in the face. The reverse process — face reconstruction — is a classical problem of criminology.

Many biometric systems are confused when identifying the same person smiling, aged, with various accessories (moustache, glasses), and/or in badly lit conditions (Fig. 1.11). Facial recognition tools can be improved by training on a set of synthetic facial expressions and appearance/environment

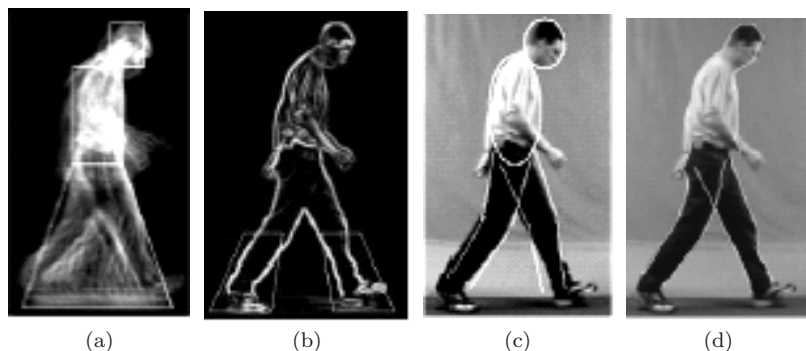


Fig. 1.10. Parameter extraction in gait model: shape estimation (a), period estimation (b), adaptive model (c), and deformable contours (d), courtesy of Prof. M. Nixon, University of Southampton, UK.

variations generated from real facial images.



Fig. 1.11. Modeling of facial accessories, aging, drunk, and a badly lit faces.

A face model is a composition of various sub-models (eyes, nose, etc.) The level of abstraction in face design depends on the particular application. Traditionally, at the first phase of computer aided design, a generic (master) face is constructed. At the next phase, the necessary attributes are added. The composition of facial sub-models is defined by a global topology and generic facial parameters. The face model consists of the following facial sub-models: *eye* (shape, open, closed, blinking, iris size and movement, etc.), *eyebrow* (texture, shape, dynamics), *mouth* (shape, lip dynamics, teeth and tongue position, etc.), *nose* (shape, nostril dynamics), and *ear* (shape). Figure 1.12 illustrates one possible scheme for automated facial generation [60].

Usage of databases of synthetic faces in a facial recognition context has been reported in [55].

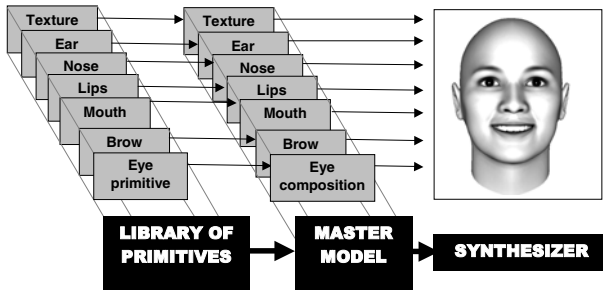


Fig. 1.12. Partitioning of the face into regions in the model for facial analysis and synthesis.

1.3.6.1. Animation as Behavioral Face Synthesis

An example of a direct biometric problem is identifying speech given a video fragment without recorded voice. The inverse problem is mimicry synthesis (animation) given a text to be spoken (synthetic narrator) [37,52,58]. Behavioral biometric information can also be used in evaluation of the truth in answers to questions, or the truth of a person speaking [17].

Facial expressions are formed by about 50 facial muscles that are controlled by hundreds of parameters. Psychologists distinguish two kinds of short-time facial expressions: *controlled* and *non-controlled* facial expressions [40]. Controlled expressions can be fixed in a facial model by generating control parameters, for example, a type of smile. Non-controlled facial expressions are very dynamic and are characterized by short time durations^a. The difference between controlled and non-controlled facial expressions can be interpreted in various ways. The example below illustrates how to use short-term facial expressions in practice.

In Fig. 1.13, a sample of two images taken two seconds apart shows the response of a person to a question [60]. The first phase of the response is a non-controlled facial expression that is quickly transformed into another facial expression corresponding to the control face. The *facial difference* of topological information Δ , for example, in mouth and eyebrow configurations, can be interpreted by psychologists based on the evaluation of the first image as follows

^aVisual pattern analysis and classification can be carried out in 100 msec and involves a minimum of 10 synaptic stages from the retina to the temporal lobe (see, for example, Rolls ET. Brain mechanisms for invariant visual recognition and learning, *Behavioural Processes*, 33:113–138, 1994).

$$\text{Mouth} = \begin{cases} \text{Irritation;} \\ \text{Aggression;} \\ \text{Discontent.} \end{cases} \quad \text{Brows} = \begin{cases} \text{Unexpectedness;} \\ \text{Astonishment;} \\ \text{Embarrassment.} \end{cases}$$

Decision making is based on analysis of facial expression change while the person listens and responds to the question. More concretely, the *local facial difference* is calculated for each region of the face that carries short-term behavioural information. The local difference is defined as a change in some reliable topological parameter. The sum of weighted local differences is the *global facial difference*.

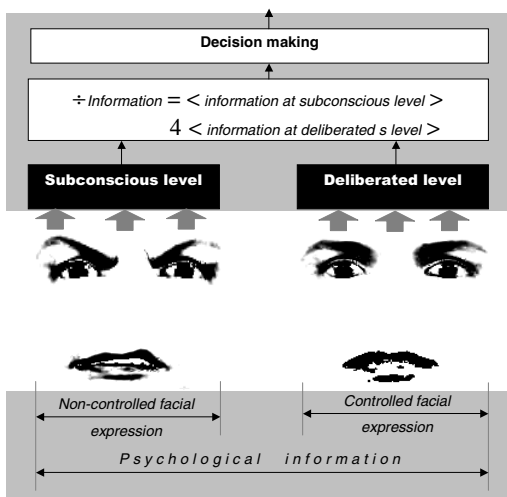


Fig. 1.13. The controlled and non-controlled phases of facial expressions.

1.3.6.2. Caricature as Synthetic Face

Caricature is the art of making a drawing of a face which makes part of its appearance more noticeable than it really is, and which can make a person look ridiculous. A caricature is a synthetic facial expression, where the distances of some feature points from the corresponding positions in the normal face have been exaggerated (Fig. 1.14).

Exaggerating the Difference from the Mean (EDFM) is widely accepted among caricaturists to be the driving factor behind caricature generation. The technique of assigning these distances is called a *caricature style*, i.e. the

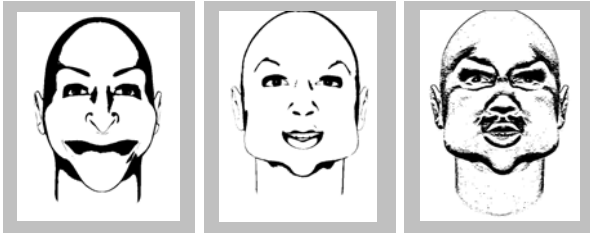


Fig. 1.14. Three caricatures automatically synthesized given some parameters.

art-style of the caricaturist. The reason why the art-style of the caricaturist is of interest for image analysis, synthesis, and especially facial expression recognition and synthesis is as follows [19,28]. Facial caricatures incorporate the most important facial features and a significant set of distorted features. Some original features (coordinates, corresponding shapes, and the total number of features) in a caricature are very sensitive to variation, however the rest of the features can be distorted significantly. Restoration of a facial image based on caricatures is an inverse problem itself [29]. Various benefits are expected in identification, recognition and matching techniques, if the art-style of the caricaturist can be understood.

1.3.6.3. *Synthetic Emotions and Expressions*

Synthetic emotions and expressions are more sophisticated real world examples of synthesis. People often use their smile to mask sorrow, or mask gladness with a neutral facial expression. Such facial expressions can be thought of as artificial or synthetic in a social sense. Facial topologies are carriers of information, that is, emotions. Visual-band images along with thermal (infrared) images can be used in this task [38,54]. These results have been used, in particular, in a new generation of lie detectors [17,43].

1.4. Examples of Usage of Synthetic Biometrics

In this section, we consider several problems where synthetic data is useful.

1.4.1. *Testing*

The commercially available synthetic fingerprints generator [6,7] has been used, in particular, in the Fingerprint Verification Test competition

since 2003. An example of a tool used to create databases for fingerprints is SFInGe, developed at the University of Bologna (<http://bias.csr.unibo.it/research/biolab/sfinge.html>). The generated databases were entered in the Fingerprint Verification Competition FVC2004 and performed just as well as real fingerprints [18].

1.4.2. *Databases of Synthetic Biometric Information*

Collection of large databases of biometric data, such as fingerprints, is troublesome for many researchers due to the protection of personal information. Imitation of biometric data allows the creation of databases with tailored biometric data without expensive studies involving human subjects [59].

Usage of databases of synthetic faces in a facial recognition context has been reported in [55].

A simulator of biometric data is understood as a system for modeling specific conditions of intake and processing of biometric data. An example of such a system is a simulator for training bank officers (supported by signature imitation and handwriting character imitation), or a simulator for training customs officers (supported by a signature imitator, face imitator, and fingerprint imitator) [59]. The multi-biometric system constitutes the core of the simulator. It provides the user identification based on the traditional methods of biometrics. This basic configuration inherits all the pitfalls of current biometric systems. In the development of training simulators, such infrastructure can be configured to meet specific customer requirements.

It is difficult to satisfy the requirements of different standard testing methodologies because of the limited set of standard tests. Hence, developing a methodology for generating biometric tests (standard as well as special customer requirements) is an urgent problem.

1.4.3. *Humanoid Robots*

Humanoid robots are anthropomorphic robots (have human-like shape) that include also human-like behavioral traits. The field of humanoid robotics includes various challenging direct and inverse biometrics. Examples include:

Language technologies such as voice identification and synthesis, speech-to-text (voice analysis) and text-to-speech (voice synthesis)

Face and gesture recognition, to recognize and obey the “master”, also to recognize the “moods” of the instructor, following of cue and to act intelligently depending on the mood context.

Vision, hearing, olfaction, tactile, (implemented through artificial retinas, e-nose, and e-tongue, etc.) provide senses analogous to those of humans, and allow the robot an analysis of the world and humand with whom it interacts.

On the other hand, in relation to inverse biometrics, robots attempt to generate postures, poses, face expressions to better communicate their human masters (or to each other) the internal states [53]. Robots such as Kismet express calm, interest, disgust, happiness, surprise, etc. (see (MIT, <http://www.ai.mit.edu/projects/humanoid-robotics-group/kismet/>)). More advanced aspects include dialogue and logical reasoning similar to those of humans. As more robots would enter our society it will become useful to distinguish them among each other by robotic biometrics.

1.4.4. *Cancelable Biometrics*

The issue of protecting privacy in biometric systems has inspired the area of so-called *cancelable biometrics*. It was first initiated by the Exploratory Computer Vision Group at IBM T.J. Watson Research Center and published in [2]. Cancelable biometrics aim to enhance the security and privacy of biometric authentication through generation of “deformed” biometric data, i.e. synthetic biometrics. Instead of using a true object (finger, face), the fingerprint or face image is intentionally distorted in a repeatable manner, and this new print or image is used. If, for some reason, the old print or image is “stolen”, an essentially “new” print can be issued by simply changing the parameters of the distortion process. This also results in enhanced privacy for the user since his true print is never used anywhere, and different distortions can be used for different types of accounts.

1.4.5. *Synthetic Biometric Data in the Development of a New Generation of Lie Detectors*

The features of the new generation of lie detectors include [17,43,60]: (a) Architectural characteristics (highly parallel configuration), (b) artificial intelligence support of decision making, and (c) New paradigms (non-contact testing scenario, controlled dialogue scenarios, flexible source use, and the possibility of interaction through an artificial intelligence supported machine-human interface). The architecture of the new generation of lie detectors includes (Fig. 1.15): an interactive machine-human interface, video and infrared cameras, and parallel hardware and software tools.

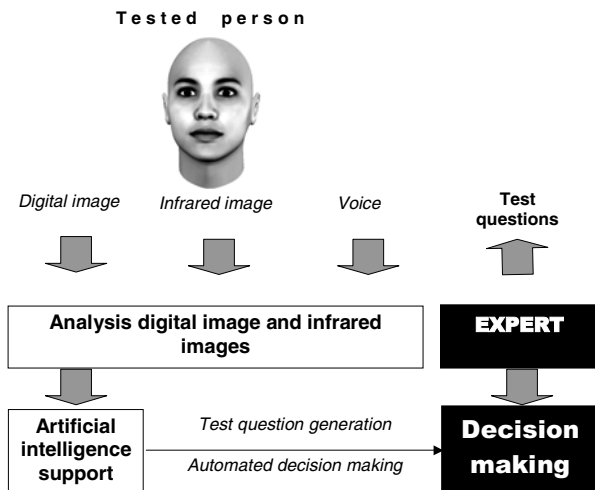


Fig. 1.15. The next generation of non-contact lie detector system.

1.4.6. *Synthetic Biometric Data in Early Warning and Detection System Design*

The idea of modeling biometric data for decision making support enhancement at checkpoints is explored, in particular, at the Biometric Technologies Laboratory at the University of Calgary (<http://enel.btlab.ucalgary.ca>) [61]. A facial model of a tested person is captured, and can be manipulated to mimic changes in visual and infrared bands caused by physiological changes during the questioning period. These can be compared against generic models of change based on statistical data. This approach can also be used to train personnel involved in questioning procedures. The decision making support system utilizes synthetic models for modeling of biometric data to support decision making.

Simulators of biometric data are emerging technologies for educational and training purposes (immigration control, banking service, police, justice, etc.). They emphasize decision-making skills in non-standard and extreme situations. For instance, the simulator for immigration control officer training must include various scenarios of generation of biometric data. This information is the system's input data. The system then analyzes the current biometric data (collates the passport photo with the present image, verifies signatures, analyzes handwriting, etc.).

1.5. Biometric Data Model Validation

Data generated by various models are classified as *acceptable* or *unacceptable* for further processing and use in various applications. The application-specific criteria must provide a *reasonable level of acceptability*. Acceptability is defined as a set of characteristics which distinguish original and synthetic data. A model that approximates original data at reasonable levels of accuracy for the purpose of analysis is not considered a generator of synthetic biometric information.

Artificial biometric data must be verified for their meaningfulness. Statistical model verification is accomplished by solving the equations that describe physics-based models, and obtaining the correct values. Model validation must prove if the equations that describe the model are right. Comparing the statistical distributions of real biometrics to the statistical distributions from empirical and physics-based models for a wide range of operational conditions validates these models for the range of conditions provided by the real biometric samples [30]. A simple method for validating these distributions is via visual comparison of overlapped distributions. For example, Daugman used plots for comparing the hamming distances for 9.1 million iris comparisons to the Beta-binomial distribution, showing that the data fit the distribution remarkably well [15].

The MITRE research project [39] used synthetically generated faces to better understand the performance of face recognition systems. If a person's photo in the system's database was taken 10 years ago, is it possible to identify the person today? A pose experiment was also conducted with synthetic data to isolate and measure the effect of camera angle in one-degree increments.

The modeling technique will provide an effective, more structured basis for risk management in a large biometric system. This will help users choose the most effective systems to meet their needs in the future.

1.6. Ethical and Social Aspects of Inverse Biometrics

Ethical and social aspects of inverse biometrics include several problems, in particular, the prevention of undesirable side-effects, and targeting of areas of social concern in biometrics. Prevention of undesirable side effects aims at studying the potential negative impacts of biometrics, as far as important segments of society are concerned, and how can these be prevented. The undesirable ethical and social effects of the solutions of inverse biometrics have not been studied yet. However, it is possible to predict some of them.

The particular examples of negative impact of synthetic biometrics are as follows:

- (a) Synthetic biometric information can be used not only for improving the characteristics of biometric devices and systems, but also can be used by forgers to discover new strategies of attack.
- (b) Synthetic biometric information can be used for generating multiple copies of original biometric information.

1.7. Conclusion

The concept of inverse biometrics arose from the *analysis-by-synthesis* paradigm, and has become an integral part of the modeling and simulation of human biometrics in many applications. Data generated by various models are used as databases (for example, databases of synthetic fingerprint) of synthetic biometrics for testing biometric hardware and software. The other application is biometric-based decision making support systems for security, banking, and forensic applications. A generator of synthetic biometric information (for example, an aging or surgically changed face), is a vital component of such systems. Yet another recently emerging application is the creation of simulators for training highly qualified personnel in biometric-based physical access control systems such as airport gates, hospital registration, and others. The ability to increase the reliability and accuracy of these systems while probing their vulnerabilities under numerous environmental conditions is critical, as biometrics becomes an essential part of law enforcement and security communities.

Acknowledgment

The authors acknowledge the help and suggestions of Dr. M. S. Nixon and Dr. D. J. Hurley.

Bibliography

1. Boles, W. and Boashash, B. (1998). A human identification technique using images of the iris and wavelet transform, *IEEE Trans. Signal Processing*, **46**, 4, pp. 1185–1188.
2. Bolle, R., Connell, J., Pankanti, S., Ratha, N. and Senior, A. (2004). *Guide to Biometrics*, Springer.

3. Boulgouris, N. V., Hatzinakos, D. and Plataniotis, K. N. (2005). Gait recognition: A challenging signal processing technology for biometric identification, *IEEE Signal Processing Magazine*, November, pp. 78–90.
4. Brault, J. J. and Plamondon, R. (1993). A complexity measure of handwritten curves: modelling of dynamic signature forgery, *IEEE Trans. Systems, Man and Cybernetics*, **23**, pp. 400–413.
5. Buettner, D. J. and Orlans, N. M. (2005). A taxonomy for physics based synthetic biometric models, *Proc. 4th IEEE Workshop on Automatic Identification Advanced Technologies*, pp. 10–14.
6. Cappelli, R. (2003). Synthetic fingerprint generation, In D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Eds., *Handbook of Fingerprint Recognition*, pp. 203–232, Springer.
7. Cappelli, R. (2004). SFinGe: Synthetic fingerprint generator, *Proc. Int. Workshop Modeling and Simulation in Biometric Technology*, Calgary, Canada, pp. 147–154.
8. Can, A., Steward, C. V., Roysam, B. and Tanenbaum, H. L. (2002). A feature-based, robust, hierarchical algorithm for registering pairs of images of the curved human retina, *IEEE Trans. Analysis and Machine Intelligence*, **24**, 3, pp. 347–364.
9. Chalmond, B. (2003). Modeling and Inverse Problems in Image Analysis, *Applied Mathematical Sciences*, vol. 155, Springer.
10. Choi, H., Cho, S. J. and Jin Kim, J. H. (2003). Generation of handwritten characters with bayesian network based on-line handwriting recognizers, In *Proc. 17th Int. Conf. Document Analysis and Recognition*, Edinburgh, Scotland, pp. 995–999.
11. Cole, S. A. (2001). *Suspect Identities – A History of Fingerprinting and Criminal Identification*, Harvard University Press.
12. Cook, P. R. (2002). *Real Sound Synthesis for Interactive Applications*, A K Peters, Natick, MA.
13. Cui, J., Wang, Y., Huang, J., Tan, T., Sun, Z. and Ma, L. (2004). An iris image synthesis method based on PCA and super-resolution, *Proc. Int. Conf. Pattern Recognition*.
14. Cunado D., Nixon, M.S., and Carter, J.N. (2003). Automatic extraction and description of human gait models for recognition purposes, *Computer Vision and Image Understanding*, **90**, 1, pp. 1–14.
15. Daugman, J. (2003). The importance of being random: Statistical principles of iris recognition, *Pattern Recognition*, **36**, 2, pp. 279–291.
16. Du, Y. and Lin, X. (2002). Realistic mouth synthesis based on shape appearance dependence mapping, *Pattern Recognition Letters*, **23**, pp. 1875–1885.
17. Ekman, P. and Rosenberg, E. L., Eds. (1997). *What the Face Reveals: Basic and Applied Studies of Spontaneous Expression Using the Facial Action Coding System (FACS)* Oxford University Press.
18. The Fingerprint Verification Competition FVC2004 <http://bias.csr.unibo.it/fvc2004/databases.asp>
19. Fujiwara, T., Koshimizu, H., Fujimura, K., Kihara, H., Noguchi, Y. and Ishikawa, N. (2001). 3D Modeling System of Human Face and Full 3D Fa-

- cial Caricaturing. In *Proc. 3rd IEEE Int. Conf. 3D Digital Imaging and Modeling*, Canada, pp. 385–392.
20. Guyon, I. (1996). Handwriting synthesis from handwritten glyphs, *Proc. 5th Int. Workshop Frontiers of Handwriting Recognition*, Colchester, UK, pp. 309–312.
 21. Hurley, D. J. (2006). Synthetic ear biometric based on force field modeling, *Private Communication*, University of Southampton, UK.
 22. Hurley, D. J. Nixon, M. S. and Carter, J. N. (2005). Force field feature extraction for ear biometrics, *Computer Vision and Image Understanding*, **98**, pp. 491–512.
 23. Hollerbach, J. M. (1981). An oscillation theory of handwriting, *Biological Cybernetics*, **39**, pp. 139–156.
 24. Jain, A. K. Ross, A. and Prabhakar, S. (2004). An introduction to biometric recognition, *IEEE Trans. Circuit and Systems for Video Technology*, **14**, 1, pp. 4–20.
 25. Koch, R. (1993). Dynamic 3-D scene analysis through synthesis feedback control, *IEEE Trans. Pattern Analysis and Machine Intelligence*, **15**, 6, pp. 556–568.
 26. Kuecken, M. U. and Newell, A. C. (2004). A model for fingerprint formation, *Europhysics Letters* **68**, 1, pp. 141–146.
 27. Lefohn, A., Budge, B., Shirley, P., Caruso, R. and Reinhard, E. (2003). An ocularists approach to human iris synthesis, *Computer Graphics and Applications*, IEEE Magazine, **23**, 6, pp. 70–75.
 28. Luo W. C., Liu, P. C. and Ouhyoung, M. (2002). Exaggeration of Facial Features in Caricaturing, *Proc. Int. Computer Symposium*, China.
 29. Luo, Y., Gavrilova, M. L., Sousa, M. C., Pivovarov, J. and Yanushkevich, S. (2005). Morphing Facial Expressions from Artistic Drawings, In T. Simos, G. Maroulis, Eds., *Advanced in Computational Methods in Sciences and Engineering. Lecture Series on Computer and Computational Sciences*, Brill Academic Publishers, The Netherlands, Vol. 4, pp. 1507–1511.
 30. Ma, Y., Schuckers, M. and Cukic, B. (2005). Guidelines for appropriate use of simulated data for bio-authentication research, *Proc. 4th IEEE Workshop Automatic Identification Advanced Technologies*, Buffalo, New York, pp. 251–256.
 31. Manolakis, D. and Shaw, G. (2002). Detection algorithms for hyperspectral imaging applications, *IEEE Signal Processing Magazine*, **19**, pp. 29–43.
 32. Mansfield, A. and Wayman, J. (2002). Best Practice Standards for Testing and Reporting on Biometric Device Performance, *National Physical Laboratory of UK*.
 33. Matsumoto, H., Yamada, K. and Hoshino, S. (2002). Impact of Artificial Gummy Fingers on Fingerprint Systems, In *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, **4677**, pp. 275–289.
 34. Moriyama, T., Xiao, J., Kanade, T. and Cohn, J. F. (2004). Meticulously Detailed Eye Model and its Application to Analysis of Facial Image. *Proc. IEEE Int. Conf. Systems, Man, and Cybernetics*, pp. 629–634.
 35. Nixon, M. S., Carter, J. N., Grant, M. G., Gordon, L. and Hayfron-Acquah,

- J. B. (2003). Automatic recognition by gait: progress and prospects, *Sensor Review* **23**, 4, pp. 323-331.
36. Okabe, A. Boots, B. and Sugihara, K. (1992). *Spatial Tessellations. Concept and Applications of Voronoi Diagrams*. Wiley, New York.
 37. Oliveira, C., Kaestner, C. Bortolozzi, F. and Sabourin, R. (1997). Generation of signatures by deformation, *Proc. the BSDIA97*, pp. 283-298, Curitiba, Brazil.
 38. Oliver, N. Pentland, A. P. and Berard, F. (2000). LAFTER: a real-time face and lips tracker with facial expression recognition, *Pattern Recognition*, **33**, 8, pp. 1369-1382.
 39. Orlans, N. M., Buettner, D.J. and Marques, J. (2004). A Survey of Synthetic Biometrics: Capabilities and Benefits, *Proc. Int. Conf. Artificial Intelligence*, CSREA Press, vol. I, pp. 499-505.
 40. Pantic, M. and Rothkrantz, L. J. M. (2000). Automatic analysis of facial expressions: the state-of-the-art, *IEEE Trans. Pattern Analysis and Machine Intelligence*, **22**, 12, pp. 1424-1445.
 41. Pappas, I.P.I., Popovic, M.R., Keller, T., Dietz, V., and Morari, M. (2001). A reliable gait phase detection system, *IEEE Transaction on Neural System Rehabilitation Engineering*, June, **9**, 2, pp. 113-125.
 42. Plamondon, R. and Guerfali, W. (1998). The generation of handwriting with delta-lognormal synergies, *Biological Cybernetics*, **78**, pp. 119-132.
 43. *The Polygraph and Lie Detection*. The National Academies Press, Washington, DC, 2003.
 44. Popel, D. (2006). Signature analysis, verification and synthesis in pervasive environments, This issue.
 45. Reed, I. S. and Yu, X. (1990). Adaptive multiple-band CFAR detection of an optical pattern with unknown spectral distribution, *IEEE Trans. Acoustic, Speech and Signal Processing*. **38**, pp. 1760-1770.
 46. Makthal, S. and Ross, A. (2005). Synthesis of iris images using Markov random fields, *Proc. 13th European Signal Processing Conf.*, Antalya, Turkey.
 47. Samavati, F. F., Bartels, R. H., and Olsen, L. (2006). Local B-spline multi-resolution with example in iris synthesis and volumetric rendering, this issue.
 48. Sanchez-Avila, C. and Sanchez-Reillo, R. (2002). Iris-based biometric recognition using dyadic wavelet transform, *IEEE Aerospace and Electronic Systems Magazine*, October, pp. 3-6.
 49. Shmerko, V., Phil Phillips, Kukharev, G., Rogers, W. and Yanushkevich, S. (1997). Biometric technologies, *Proc. Int. Conf. The Biometrics: Fraud Prevention, Enhanced Service*, Las Vegas, Nevada, pp. 270-286.
 50. Shmerko, V., Phil Phillips, Rogers, W., Perkowski, M. and Yanushkevich, S. (2000). Bio-technologies, *Bulletin of Institute of Math-Machines*, Warsaw, Poland, ISSN 0239-8044, **1**, pp. 7-30.
 51. Sloman, L., Berridge, M., Homatidis, S., Dunter, D., and Duck, T. (1982). Gait patterns of depressed patients and normal subjects, *American Journal of Psychiatry*, **139**, 1, pp. 94-97.
 52. Sproat, R. W. (1997). *Multilingual Text-to-Speech Synthesis: The Bell Labs*

Approach, Kluwer.

53. Stoica, A. (1999). Learning Eye-Arm Coordination Using Neural and Fuzzy Neural Techniques, In H. N. Teodorescu, A. Kandel, and L. Jain, Eds., *Soft Computing in Human-Related Sciences*, pp. 31–61, CRC Press, Boca Raton, FL.
54. Sugimoto, Y., Yoshitomi, Y. and Tomita, S. (2000). A Method for detecting transitions of emotional states using a thermal facial image based on a synthesis of facial expressions, *Robotics and Autonomous Systems*, **31**, pp. 147–160.
55. Sumi, K., Liu, C. and Matsuyama, T. (2006). Study on Synthetic Face Database for Performance Evaluation, *Proc. Int. Conf. Biometric Authentication*, pp. 598–604, LNCS-3832, Springer.
56. Tilton, C. J. (2001). An Emerging Biometric Standards, *IEEE Computer Magazine*. Special Issue on Biometrics, **1**, pp. 130–135.
57. Wang, J., Wu, C., Xu, Y. Q., Shum, H. Y. and Li, L. (2002). Learning Based Cursive Handwriting Synthesis, *Proc. 8th Int. Workshop Frontiers in Handwriting Recognition*, Ontario, Canada, pp. 157–162.
58. Yamamoto, E, Nakamura, S. and Shikano, K. (1998). Lip Movement Synthesis From Speech Based on Hidden Markov Models, *Speech Communication* **26**, 1,2, pp. 105–115
59. Yanushkevich, S. N., Stoica, A. Srihari, S. N., Shmerko, V. P. and Gavrilova, M. L. (2004). Simulation of Biometric Information: The New Generation of Biometric Systems, In *Proc. Int. Workshop Modeling and Simulation in Biometric Technology*, Calgary, Canada, pp. 87–98.
60. Yanushkevich, S. N., Stoica, A., Shmerko, V. P. and Popel, D. V. (2005). *Biometric Inverse Problems*, Taylor & Francis/CRC Press, Boca Raton, FL.
61. Yanushkevich, S. N., Stoica, A. and Shmerko, V. P. (2006). Fundamentals of Biometric-Based Training System Design, this issue.