Direct Problems and Inverse Problems in Biometric Systems

Authors: Mihaiescu Marius Iulian, Computer Science Department, Titu Maiorescu University, Bucharest, Romania, mihmariusiulian@gmail.com

The article purpose is to describe the two sides of biometrics technologies, direct problems and inverse problems. The advance that we face today in field of Information Technology makes Information Security an inseparable part. The authentication has a huge role when we deal about security. The problems that can appear in implementing and developing biometrics systems is raising many problems, and one of the goal of this article is to focus on direct and inverse problems which is a new and challenging branch in biometrics technologies.

Keywords: direct problems; inverse problems; biometrics; signature; face recognition

Introduction

In this paper we will talk about the prospective of unity between the two sides of the contemporary biometrics: direct problems, known as the analysis of biometric information and inverse problems, meaning the synthesis of biometric information. We will start by resuming the possible attacks on biometric systems by a forger which uses imitations instead of natural features, thus generating synthetic biometric information. In order to protect the system, we propose in this paper manners to imitate (thus prevent) attacks, using inverse problems of biometrics. In other words, we mimic the attacks, we generate false features to establish the proper
parameters in order to prevent such vulnerabilities of the biometric system, by making hard for the hacker to attack it and by copying as much as possible the strategy and methods of the attacker.

By using real examples, we hope to achieve a better understanding of direct problems, through CAD (Computer Aided Design) and its capacity and tools, able to resolve inverse problems. In order to achieve our purpose, we will start, first of all, by presenting a possible scenario of attack, in the terms that we define it before. We will than present a bit further the typical direct and inverse problems, regarded as a suitable solution for a wide range of problems. It is also imperative to present the basic structures and types of biometric data, in order to learn how to generate synthetic biometric data. We will then talk about biometric interfaces and tools for designing both biometric systems and synthetic biometric information. In the end, we will approach some of the most important ethical issues and propose a few directions for future research.

Fig. 1 : Direct and inverse transformation
Attacks

The final goal of inverse problems is training biometric systems and preparing them for the possibility that fake data will be introduced into the system. The concept of fake data refers to synthetic data which are most resembling to the original, authentic data, meaning the original features. These data could also be divided in copies of the original data or hypothetical (re-constructed, imagined) data. In order for the system to be protected, one must verify the acceptance and rejection rate, systems access to data in various phases of the reading and the way system responds to forger attacks. This is where the inverse problems interfere, to verify, experiment and thus prevent such situations, to train the biometric system in case of such attack, to anticipate it by forcing the system to respond and then improve its response. An interesting work paper for attacks can be found here [13].

Imagine the system and its complex dynamic: an attack could occur in any of the following positions: at the entrance of data (input), during its flow (for example during matching process or attack on channels) or inside the system, in its database (at template level). So either is an active or passive attack (meaning he produces changes or is merely recording and steeling data), the defense against such attacks should be, as well, active or passive. Moreover, the attacks could be based not only on quality of the forgery, but on its multitude, meaning the hacker can attack the system also massively, by “bombing” it with fake resembling data, in an attempt to “fool” it.

The two most representative type of biometrics – signatures and fingerprints – carry the two types of recognition values: psychological and physical. The first depends on subject’s state of mind and evolves with it, while the other is fixed for the entire life of a person. As in all domains, the attacks on signatures must involve a high degree of skills in order to fool the biometric system. Most system that accept signature as biometric feature are capable to discern up to a high degree between a genuine signature and a fake one, based on its static and/or dynamic characteristics, like its structure or trajectory. A homemade forgery is seldom subject to success, as it takes a lot more precision and analytical capability to successfully forge a signature which the system would accept as original. Or, in case of fingerprints, there
can be a series of attacks, either involving the real person, forced to login using its finger, or by capturing the fingerprint and making a mold out of a variety of materials imitating the original.

Given the complexity of the problem and the fact that threats become more and more subtle, it is advisable to search continuously for other methods of recognition, more and more sophisticated like, for instance, the unique frequency of the brainwaves (known as electroencephalogram) or infrared radiation of the body in regards to its temperature. Also, to biometric systems already in function must be added more parameters and thus making more complicate and difficult for the intruders to penetrate the system.

**Fig. 2:** Electromagnetic waves provide information used in biometric technologies
Direct and inverse problems

As I pointed out earlier, problems so complex as biometrics and biometric systems involve a complex approach rather than a simple, linear one. Thus, a complex solution would be generated using both direct and inverse modeling. In other words, it requires analysis on one hand and synthesis on the other. However, the latter has more value in case of nonlinear behavior. The best example to illustrate this dynamic is when system accumulates over time sets of features to be incorporated into a database. In order for the system to become more performing, the inverse function (synthesis) sorts through the database and establishes functional criteria, so when hit whit something new or unexpected, the system would be able to adapt quickly and integrate the new features into known parameters. The two approaches are based on a series of inverse functions, inverse operators, inverse Fourier, inverse Euler formulas or Haar transforms. For instance, in order for the input to be extracted from the system it is necessary for the system to be inverse.

Model inversion (the other name for the inverse problems) represents the approximate model conceived after the analysis and study of data. It is rather veridical than real and its function is to predict by approximating, but to obtain it, the conditions, traits and rules of the original model must be extracted. To illustrate the concept, we could take the example of human voice: first part, direct, is recording and analyze it, while the second part, the inverse, is re-creating it with the aid of a voice synthesizer. Anyway, developing such inverse methods helps researchers to better understand their functionality and to prevent attacks at biometric system level, in other words, contributes to system’s optimization, allowing us to create artificial data and manipulate them. Also, inverse problems are crucial to improve efficiency of the biometric algorithms by perpetuating the circle into a better understanding of the two faces of the coin. In other words, artificial models of biometric features can be further subjected to the same process of analysis as in the stage one. This secondary analysis (direct problems) will provide Intel regarding the structural and behavioral differences between the authentic model and the artificial one, resulted after using inverse methods. Furthermore, the latter analysis will provide data for the improvement and optimization of the biometric system.
For the synthesis to be acquired, it is necessary that given data (original data) to be attached to a form of carrier, and only after the analysis was performed. Examples of biometric data which can be synthesized could be: signatures and handwriting, fingerprints, voice and speech patterns, iris and retina scan, infrared identification and the list could continue with other body/face elements. For each of these potential biometric data, a synthesized version can be acquired through a synthesizer, resulting for example in text or handwriting forgeries, reconstruction or imitation of all other features mentioned above. Furthermore, some of the synthesized data can be recognized and thus studied by the system. These types of data are called non-acceptable, while the data that can pass through without being recognized as fakes are called acceptable.

The conception of synthetic data (in regards to biometry) is called modeling and it requires a series of steps, or methods to de-compose the original data and re-compose it into what is intended. The first phase is called segmentation and its purpose is to reduce complexity while still being able to be processed. This phase will be logically followed by composition of given segments, according to the set of rules prevailed from the original data. The process is similar to prevailing cells from human body by medics and growing again the tissue in laboratory. The difference is that, while nature is programed to take its course, artificial design of synthetic biometric data requires algorithms, data structures and models in order to manipulate the data with as fewer errors as possible.

One of the most accurate methods in synthesizing biometric data is through artificial intelligence. Through its features, like self-assembly capacity, a unity can be constructed from different components, pending to inner and outer rules of assembly. This particular method doesn’t involve a preconceived plan. Instead, it depends on an inner rule of association between segments, similarly as cells growing in a laboratory, and on its interaction with the environment, or electron particles attracting each other according to their own set of rules, but not pre-programed to assembly in a certain pre-defined form. The easiest way to successfully assembly in the desired final form is by using a global search algorithm, which searches for global solution to inverse problems, instead of local ones. This type of algorithm modifies the connexions inside the network and receives input concerning the performance of the network. This prevents further mistakes on the way and searches for the optimal final solution.
We will now focus on some of the most frequent synthesized data, bearing in mind that each of them requires different methods and algorithms. We have mentioned earlier the signature and the possibility of faking it. This is a good example of synthesized data, and could be realized by hand, which could bring to unwanted differences in shape, giving the system the possibility to identify it as forgery, or could have different trajectories or pressing points. Another quite known example is voice synthesis or imitation. The difference between the two is that first requires a mechanical synthesizer, while the second is based on a given voice, imitating another. The possibilities don’t stop here, as the technology allows us to detect emotion and feeling by using a voice analyzer. Furthermore, the system can be used to identify patterns of speech or to assess when someone answers truthfully to questions or not. Today’s forensic sciences can also count on face recognition systems, which have known a great improvement over the last years. Nevertheless, there is still work to be done in this area of research. At the moment, these systems are based on detection of shapes, patterns or shadows, but they are incapable of discerning when strong emotions like laugh or cry are evoked, so this would be a great point of start in the research process. Fingerprints are one of the oldest ways to identify a person, as they are unique for each individual, but they were also subject to synthesis, weather the carrier agrees to allow the making of a copy, or its fingerprint is prevailed from him without his awareness of the fact. Going further on this route, we can identify three more biometric features which could be prevailed from one’s hand: palm prints, vein pattern topology and hand topology. First two are used in the same manner as fingerprints, and could also be synthesized, while the last is not became yet subject to forgery. As I specified earlier in the paper, another way to identify a person is through its infrared image, although it carries some problems as well, as it depends not only on the person aside, but on the environment temperature and some internal, somatic conditions, like blood pressure problems and all the affections connected with it, including medicamentation.

The relationship between different types of biometric data is not to be forgotten, or the relation between biometric data and non-biometric data, like devices used to analyze it. The dynamic of these relations can be considered from four points of view: Brain-To-Brain, Brain-To-Machine, Speech-To-Vision or Speech-To-Machine. The relation between brain and machine can be concretized through a brain-machine interface, in which
brain communicates directly with the device through electrophysiological signals. The result is that messages, instead of being passed through nerves to muscles in order to perform a certain action, they go directly machine, which responds by doing the specified action, like moving one part of the body or the cursor. The principal of brain-machine interface is the belief that the machine can identify the intention of a person by measuring elements like blood volume or electrophysiological signals. In order to verify the accuracy of signal reading (intentions), three steps must be taken: read and verify mental data, read and verify facial data and generate a learning pattern, method which involves mutual interactions between the two entities: the subject and the interface. This brings to adaptation in both ways: the subject becomes adapted to the interface and learns to better control its brain signals, while the interface adapts itself to the specific of the subject, learning different patterns of intentions on his behalf and creating this way sort of an electrophysiological profile of intentions. In the following scheme, we have illustrated the interaction between synthetic facial expressions and records of brain’s electrical activity. For the subject/user, this process is similar to learning how to drive a car: at first, he must concentrate very hard to every action it takes, but in time the need for concentration disappears and the “ritual” of driving becomes automatized, as the driver gets used to using the car, - the interface in this case.

The synthesis of human motion through electric impulses of the brain has a particular degree of importance for a series of domains like robotics, practical applications for people with disabilities or games industry. Furthermore, other applications can be available if biometric systems would be designed as to be able to analyze and synthesize at the same time various types of biometric data. Such applications could be lie detectors (in forensic sciences), reconstructive surgery (in medicine) and many others. Such a design wouldn’t be much difficult to realize than a normal biometric system, as it basically uses the same tools, while the degree of performance and security for the user rises accordingly.

The synthetic data generators have to meet a series of requirements, in order for the applications to run properly. For example, to ensure the security of the database, all data should be saved under the form of a synthetic copy. Synthetic benchmarks are required, for example, for testing the system, benchmarks containing different aspects regarding the use of biometric devices and synthetic biometric data which are unique should be
embedded in a carrier in using watermarking techniques. At a more practical level, like reconstructive surgery, the details of the patient’s face are first scanned and then reconstructed, or in robotics industry, robots should be able to produce synthetic voice or limited interactive conversations. Which bring us to the problem of artificial intelligence: here, in case of human-machine interfaces, the most important factors in its success and evolution are the automated support and tools, constantly developed on various levels.

It isn’t easy to build a biometric system, considering the complex relations between human decision process and tools of artificial intelligence. Depending on the direct problem (which could be either identification or simply verification), the inverse problem (the classification we have given earlier, including testing and attack prevention schemes), the biometric database, capacity to measure and/or the process of decision, which could be based, as I stated earlier, on human or artificial intelligence factor. It is also very important, when testing biometric data, to use both artificial-intelligence factor and human eye, as first can test the information (the specific biometric element) at different levels – which could all be forged -, while a person has a more global view and could also determine if the given data are authentic or fake.

We will now focus a little on artificial-intelligence structures, which basically have two levels: collected data level (database) and analyze data level (an engine used to analyze data for given purposes and synthesize information from given data). Finding its inspiration in nature, artificial-intelligent devices act like a brain: they accumulate and stock data, than analyze them. So far, artificial-intelligent structures could be classified as artificial neuronal networks, algorithms for implementing evolution strategies and expert systems. The last are capable of identifying both local and global problems, and correlate its decisions with human factor, using statistics to ascertain four variables: the rate of success, the false rejection rate (FRR), equivalent to false negatives, the false acceptance rate (FAR), equivalent to false positives, and the equal error rate (EER) oriented to design of synthetic data or automatized support for expert decision process. Both false positives and false negatives are problematic in case of fraud and wrongful application, which leads to the need of low such, rates [6-9].

The artificial-intelligent biometric systems have many uses in different domains of activity, like security (police, justice, airport control
If we take as example a scenario in which a person tries to fraudulently pass the border, we must take into consideration the fact that he will most likely use fake biometrics (face, voice, signature), not to mention fake documents. In order for the system to identify the forgery (forgeries), presented biometric details must be compared to a database of previous details. We can now conclude that one very important variable for success is also the dimension of the database: the more complete and diversified, the more chances to identify differences between patterns and thus identify the forged biometric traits.

Besides the richness of the database, there are other methods to better ensure the effectiveness of the system at different levels. One of these methods would be encryption, which consists of encrypting biometric data so even if they were to be stolen from the database, the attacker wouldn’t be able to use them without the decryption key. Steganography and watermarking are both based on the same principle: embedding a message or public data into the host, using a key. While encryption is focused on turning real information in apparently random for unauthorized persons, the steganography tries to hide information from ill-intended eyes. On the other hand, watermarking techniques can assure security even after the data being decrypted. Moreover, there are over five types of watermarking techniques, fact that makes it so much secure: visible, spatial, image-adaptive, blind or fragile, semi-fragile and robust watermarking techniques [12-16].

After describing the function, the uses and the way inverse problems work, we must take into concern the ethical problems involved by them. Given the sensitivity of information with which these area of expertise works, social sciences have to explore and identify the boundaries of inverse problem’s use, in order to ensure a more secure environment of its use and avoid eventual side or undesired effects. The main concern is that synthesized biometric features, like many other new areas of research, are like a coin with two faces: on one hand, they can help improve the functionality and efficacy of biometric systems, on the other, they can be an excellent resource for the forgers, to search for new way to attack the system, as the inverse techniques can reproduce original biometric data into multiple copies. So in a common effort to constantly improve the systems, and, at the same time, decreasing the risks connected to harmful use of inverse biometric problems, engineers and social scientists, sociologists,
philosophes and psychologists give hands, as the problems become more and more complex.

Conclusions

In conclusion, biometry becomes one of the key sciences in present and future development of society. Its technologies, based on human traits (psychological or physiological, intellectual or emotional) are used to identify persons, ensure security or predict behavior. In connection to biometric systems, inverse problems contribute to increasing security, by pre-testing and training the system in case of attempts of real forgery. This helps as it is a step forward in improvement of the systems, thus in aiding security. As for the research areas in which inverse problems are best put in use, evolutionary algorithms and strategies are one of the most favorable environments for inverse problem development. They are based on techniques of selection and they can be very effective in synthesis of image, recognition of fingerprints or generation of various objects (physical, biological, chemical etc.). Another application consists in generators of random data and stochastic process or converging technologies like human-machine interfaces, of which we have talk about earlier. All these applications must be observed and monitored, so they activate according to general and established rules of ethic.

In biometry, each type of features must be evaluated according to a specific set of criteria, like purpose, effectiveness, urgency, exclusivity and receptiveness, each of them noted on a scale from 1 to 10. The latter refers to the openness of the people with regards to using specific biometric features.

After resuming the principles and methodology used in biometric systems, mostly from the perspective of biometric synthesis, known as inverse problems of biometry, after giving a broad perspective of types of biometrics which can become subject to inverse problems and classifying them, after a offering a general perspective of the ethical concerns involving inverse biometry, we now must set the scene for future areas and directions of research. Each of key components and steps are analyzed in various papers. Among these components we can enumerate basis and fundaments of biometric, trends, algorithms design, and involvement of artificial intelligence in the process of decision making, security and privacy of
biometric systems, testing and development. Furthermore, there are numerous papers which treat separately each biometric feature, in both analyzing and synthesizing states, in order to predict the behavior of the system in case of attack by forgery and try to come with new, improved methods and algorithms to ensure the success rate for each and every piece of biometry, like signature, fingerprints, palm prints, iris and retina, voice, face and so on.

Besides the problems mentioned above, there are big areas of research in the field of robotics. For instance, in order to conceive a robot it is necessary to appeal to biometrics, as they represent the interface of human communication. Speech recognition and voice synthesis are just a small example of how biometrics can contribute to the field of robotics, when talking about interaction with persons.

Another spread area of research is convergent technologies, which include various new types of sciences, like bioscience (in connection to medicine), nanotechnology and biometrics. These are considered all together, in an effort to find new optimal solutions for different kinds of problems that will benefit the humanity. Some of these problems are of medical concern, like Magneto-encephalography, EEG, resonance imaging or video imaging. The complex field of applied mathematics is also a good point of start in searching for methods to improve biometric systems, by perfecting evolutionary algorithms or watermarking techniques.

The main idea we should all keep in mind is that biometry and all its extensive research fields is a domain of primary concern at the given moment and it may be for a long time, as it is applicable in many sciences considered to be of utmost critical human interest.

References


