

BRIEF INTRODUCTIONS TO THE MARKET OF AUTOMATIC FINGERPRINT PROCESSING

Bernard Didier,

Director, Technical and Business Development
Defense and Security Division
Security Business Unit
bernard.didier@sagem.com

The weight of History:

If there is really a biometrics technique seen as different from the others, it is fingerprinting. It carries behind it more than a century of history: it was, in fact, recognized scientifically as a means of identification of people during the demonstration by Sir Francis Galton of the « Royal Society » in 1888. The processing of the fingerprint has since then, indisputably, been the most demonstrated and tested technology. But it is also due to this weight of history and all these images from police movies, where there is no doubt that the smallest fingerprint will lead to the inescapable identification of the suspect, that fingerprinting, more than any other technique, carries certain risks in the matter of individual freedom.

Should this, in matters of biometrics, lead to particular attention in the use of fingerprinting? It is certainly an error that the collective subconscious has a natural chance of committing. Where it concerns their use, all the biometrics techniques merit the same attention and return to the debate: are biometrics an aggression against individual liberties or a means of protecting patrimony and privacy?

Some definitions and consequences:

The fundamental objective of processing fingerprints is to « identify » or « authenticate » people. By « identify » we understand: find the reference of one person among a group of people already known. In other words, we also say that identifying is a function of comparing one person with n persons, or a « 1 : n » operation.

By « authenticate » we mean confirm, from the information supplied by a person (PIN, biometric data, etc.) that this person really is who he claims to be. It is a « 1 : 1 » operation. In this respect, it is useful to note that the function of authenticating, where the result is resumed by « yes » or « no », does not put the identity of the person at stake.

In a more general manner, the security of systems is based on the carefully combined use of these two functions. During the granting of a right, identification serves to verify that the petitioner is not subject to an interdiction and that he does not already exist in the system under another name. It is at this stage also that the biometric reference information (template) is created, which will later serve to authenticate the petitioner when he exercises his right.

All the biometrics techniques offer authenticating functions; that is not the case in the matter of identification. Only the techniques which are fundamentally based on the biometric information unique to each person can correctly fulfil this function. Historically, fingerprinting is the first

technique which allows us to both identify and authenticate. In the present state of our knowledge, apart from the iris and DNA, there are no other techniques which could claim to fulfil a function of authenticating efficiently.

The markets for automatic processing of the fingerprint:

The automatic processing of the fingerprint cannot be resumed by a monolithic industrial activity. A good segmentation of the markets, of the products, and of the players is a prior requirement for any analysis of this sector of activity. In the past, certain market studies on biometry have shown a lack of attention to the definition of segments of activity, and have led to forecasts of turnover which were rather surprising. This market is, indeed, difficult to grasp: we avail of very little public information and there is a plethora of actors. It would be necessary for the various associations which group the biometrics manufacturers to make a permanent effort in the matter of financial legibility of the biometrics industry's activity. In the current context of interrogation on the new technologies, this prior requirement would increasingly necessary, in order for this budding sector of activity to develop itself and to acquire credibility in the eyes of the financial actors and the potential clients.

Among the various types of possible segmentation we will retain:

Systems of automatic fingerprint processing in the fight against criminality (Police):

These systems are better known under the acronym of AFIS (Automatic Fingerprint Identification Systems). As research work initially conducted at the request of the FBI in the 1970s, notably by Calspan Autonetics and Rockwell, these systems really had to wait for a dozen years before obtaining the confidence of the police community in the United States. Today, almost all modern police forces are equipped with them.

On the technical level, these systems are capable of managing several thousands of identifications a day on databases of several millions, even tens of millions of people. The latest system, with which the FBI equipped itself in the 1990s, with about 40,000 searches a day on a population of 40 million people, is the most powerful in the world. These police systems allow the identification of people from prints taken of the ten fingers, but they, particularly, distinguish themselves from other institutional or civil systems by their ability to identify partial fingerprint traces, often of bad quality, left on crime scenes.

At the industrial level, these systems are supplied by companies who market, install, and develop these AFIS. There are three historic actors, NEC (Japan), Printrak, recently taken over by Motorola (USA), and Sagem (France), and a more recent actor, Cogent (USA). Sagem, both by its turnover and by its references, particularly those of the FBI and Interpol, is the world leader in this market segment. It is a mature market segment, essentially of renewal, of approximately 150 to 200 million Dollars per year.

Institutional systems of automatic fingerprint processing :

This is the market segment of management of the delivery and use of institutional rights, such as, identity cards, pensions, social security, passports, etc.. This market demand is relatively recent and dates from the years 1992/1993.

On the technical level, the AFIS is only one of the elements of a more complex solution, based on the manufacture of secure certificates, which allow for the subsequent control of the holder by

fingerprint analysis, and, sometimes, including registry management. These systems apply to bigger populations than those of the systems dedicated to fighting against criminality, and are characterized by high demands for identification, dozens of thousands on databases of several dozens of millions of people. The size of the flows to be managed needs different and more complex structures than the AFIS for police purposes. The identification of traces disappears for the more systematic use of authentication.

At the industrial level, the replies to the tenders put out by the States are given through consortiums led by « integrators » (TRW, Unisys, Siemens, IBM, etc.) beside which one finds the traditional manufacturers of AFIS (Motorola, Nec, Sagem, and Cogent) and the manufacturers of certificates (Polaroid, Gemplus, Oberthur, Gesiecke, and Devrient, etc.). On this market, Sagem has reaped the majority of the tenders, either as manufacturer of AFIS, or, in a certain number of recent cases, by offering a complete service as « integrator », manufacturer of AFIS, and producer of secure titles.

It is a developing market segment of approximately 50 to 100 million Dollars per year, with long decision cycles (more than three years). It can be estimated, that over the past ten years the number of contracts signed has concerned almost 275 million people. It is a market segment which is generally structuring: a state which provides itself with a certificate made secure by a biometrics technique, will favour the use of this certificate for other purposes than the simple control of exercising rights. This is, for example, the case of Malaysia with its GMPC project (General Purpose Card) which proposes to manage the driving licence, border crossings, and an electronic purse, all that on a single card made secure by fingerprinting.

Automatic fingerprint processing terminals:

As the first prototypes in the middle of the 1970s, and the first commercial products put on the market at the beginning of the 1980s, these terminals originally addressed the markets of access control and/or time management, their clients being governmental structures (prisons, for example), and more rarely commercial and industrial companies.

At the technical level, the solutions proposed may range from a fingerprint recorder connected to a PC accompanied by a processing software, to the access control box, fulfilling the function of authentication and more rarely of identification. In the latter case, the comparison is carried out with some thousands of fingerprints in a few seconds.

At the industrial level, the sales are often made by the « integrators », the distributors, or by the companies specialised in the vertical market segments (transport, health, etc.). The equipment is often conceived by a myriad (more than 140 in early 2001) of small companies, more or less solid, who only rarely have the capacity of production and performance evaluation of their technology. The years 1998-2001 have seen the start of some consolidation, particularly with the take-over of Identicator by Identix for 43 million Dollars, and the disappearance of Veridicom (a company which had, nevertheless, gathered some significant shareholders, such as, Intel, ATT, and Lucent Technologies); Ethentica (with shareholders, such as Citibank and Philips Electronics) owing its salvation only to the injection of 40 million Dollars and the arrival of HP and Amdhal in its capital. This consolidation should continue and, probably, lead to a dozen actors, as no « lone player » in this market segment is making money.

The historic player on this market is the American company Identix. For the past two years now, Sagem has entered this market by offering technologies tested in the context of the fight against criminality, which are not easily available to traditional companies in this market segment.

Despite its age, it is a still budding market segment, but under rapid development. To the traditional access control sub-segment, we now see the recent addition of a demand for logical access control (PC, Internet and Intranet transactions, etc.) which should be followed by a demand for personal equipment (PDA and telephone).

The market of biometrics terminals is the object of somewhat diverging market analyses. According to certain sources, it was evaluated at between 66 and 196 million Dollars for the year 2000, all technologies included. On the other hand, a consensus exists in recognizing the fact that the technique of fingerprint analysis is the one most frequently retained by the market. A majority of analysts estimate that, with a market share between 37% and 55% and a growth of at least 40% per annum, fingerprinting is the most promising technology among biometrics products.

In the matter of applications, three superior segments are emerging: the historic and mature one of physical access control, which should continue its growth, the one of horizontal applications (telecommunications and IT) which should experience more rapid growth than that of the vertical applications (health, transport, immigration, etc.).

Finally, where the geographic distribution of the market is concerned, there are no surprises. North America keeps its pioneer position with Asia and Europe as followers.

To resume, automatic fingerprint processing represents a market of between 250 and 500 million Dollars, composed of several segments at various stages of maturity.

The various technologies:

In the matter of equipment, the differences lie essentially in the technical characteristics of obtaining the fingerprint image:

Technology of the captor:	optical, « capacitive », ultrasound, « e-field »
Mode of capture:	2D or 1D (sliding the finger along a bar)
Definition:	from 250 to 500 dpi
Acquisition surface:	from 11 x 14 mm ² to 22 x 24 mm ²

All these characteristics have advantages and disadvantages; but in general, for applications needing high performance, the 2D optical captor at 500 dpi with a large acquisition surface remains the best choice at present, at a price which is still remarkably competitive.

In matters of software, it should be noted that the characteristics of the equipment are comparatively much more talked about than the software aspects. There are two different main origins of software: software resulting directly from an expertise in police systems, and other software. Technical problems excepted, the former category is, generally, more tested and more mature. One can distinguish between software that effect recognition according to:

- characteristic points only
- characteristic points and counting of ridges
- characteristic points with other local information

The debate in this matter is to know whether the characteristic points alone are sufficient to identify and/or authenticate prints of a bad quality correctly. Certain people have wanted to compensate for the loss of quality by more information (counting of ridges or other techniques). It generally turns out that seeking more information, when a print is of bad quality, is not a winning choice. The assertion is not obvious and was subject to long internal discussions before we, as from 1983, decided to concentrate our efforts on the characteristic points alone. Apart from the

economy of space in storing the « template », the performances obtained by Sagem during recent comparative tests have always surpassed those of the other technologies in competition. The recent choice by the « American Association of Motor Vehicle Administrators » of retaining, as biometric description standard, a format based on the characteristic points alone is a significant progress and closes the debate.

The ability to identify - versus simply to authenticate - is a relatively recent criterion, and differs greatly in matters of software. Such a function allows, in certain security and comfort applications, the suppression of badges. Obtaining good performances in identification is considerably more difficult than in authentication, therefore, very few companies offer efficient identification functions.

Concerning performance and costs:

Some fifteen years ago the international press echoed some unfortunate biometric experiences. Despite this lack of success which has certainly been harmful to the development of this technology, we have to note, that most of the companies have adopted a policy essentially centred on the reduction of prices, with a soothing and identical message concerning the performances. The sales prices have, in fact, these past few years gone down from more than 1000 Dollars down to 100/200 Dollars. Projects at some tens of Dollars are currently in the plans of numerous companies. But in terms of performance, the discussion remains commercial, and extremely few biometrics systems respect the performances they announce. This ambiguous situation is continuing, because it is particularly difficult for a company to appreciate the real performances while biometrics systems are implemented: the false rejects are immediately noticed by the users, whereas, the false acceptances are much more difficult to measure.

At another level, assessment criteria have slowly evolved for some years, probably with the maturity of the market. As the purchase price is less and less differentiating, we have moved slowly from the « sales price » criterion to the criteria of « ease of implementation, functionalities, convergence with the public key management tools (PKI), etc. », still leaving aside one of the most fundamental aspects: security.

It should be expected that some projects will experience cruel disillusion during their operational phase.

What future for biometrics:

If there were only one message to remember it would probably be: « Biometrics is developing much more rapidly than some European players think ». It is reasonable to assume that this technology will experience massive and generalized development, probably within the next five years, and certainly within the next ten years.

Its more or less rapid development will be conditioned, firstly, by the implementation of standards, and the acceptance by users; these two points represent more than 51% of the reasons why the development of biometrics is slowing down, according to « Biometrics in Human Services User Groups ».

In a more exhaustive manner, one can retain as the conditions for the construction of a biometrics industry:

1. Definitions of rules of use specified by the organisms of protection of data and individual liberties. On this subject, faced with the accelerated development of different technical approaches, identification versus authentication, or, even more basically, techniques which in use are

imperceptible to the user (voice and face recognition in particular), the case by case authorisations of biometrics applications should probably give way to a legal body to define the conditions under which the judiciary may use such information.

2. Where it concerns the acceptability of the technique by users, it is useful to note, that even if there is some reticence by users before adopting a biometrics solution, this changes with use in more than 98% of the cases due to the comfort and the advantages of biometrics solutions. The prior reluctance should, therefore, disappear with the adoption of pilot operations.

3. The too great number of different standards should lead to industrial consensus:

BioApi retained by the US Army,

Bapi chosen by Microsoft,

BIR format of the BioApi template description,

CBEFF referring to a format for exchange of data,

AAMVA with its standard for describing the characteristic points,

ANSI X9.84 standardising the use of biometrics for financial applications,

Common biometrics criteria sponsored by the UK Biometric Working Group and the German Information Security Agency,

ISO SC17 concerning the use of biometrics on cards,

and, it is certain that some key industrial players - not to mention, notably, Microsoft - will have some responsibility in the matter. The interoperability of « templates » is a topic that must be dealt with in order to see a large scale world-wide use of this technology emerge.

4. Implementing standards of performance and evaluation services, led by truly independent third party bodies, should allow the market to better understand what it is buying, e.g., either security or comfort. Positive points should be attributed for the continuous efforts of the National Biometric Test Center of San José University, to the University of Bologna for conducting the first competitive test of algorithms in automatic fingerprint processing, and to the works by the UK Biometric Working Group and the German Information Security Agency. On this subject, we can regret, on the other hand, the few positive operational repercussions - not to say the failure- of the interesting European biometrics project BIOTEST, which it would be interesting to revive on a different basis. At a more local level, there are for the moment no governmental projects in France on this subject, in contrast with what is being done in the UK under the aegis of the « Communication Electronic Security Group » of the Ministry of Defence (Biometric Working Group), or in Germany (German Security Agency), in Japan with the MITI (National Project of Test and Evaluation for Biometrics Technologies), or in Hong Kong (The Biometrics Technology Center).

5. At the technical level, with the development of the market and the evolution of values (financial transactions, access to the home, to the car, etc.) being the object of biometric protection, industrials should begin the classic technological pursuit against the new attempts at fraud, which will not fail to appear.

6. Finally, a consolidation of the sector, which has already begun, should give rise to a real biometrics industry that would develop quality products at a competitive price. It is to be feared, however, that only those players will succeed which have real competence in the matter and which can back up their biometrics activity with other, more lucrative, activities.

