Title:	Document Version:
Deliverable D1.1 **Report on fingerprint aliveness detection and fake prevention methods**	1.0

Project Number:	Project Acronym:	Project Title:
IST-2002-001766	BioSec	Biometrics and Security

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
31/05/2004	30/06/2004	R – PP

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other
** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible:	Organization:	Contributing WP:
Davide Maltoni	UNIBO	WP1

Authors (organizations):

Athos Antonelli (UNIBO), Denis Baldisserra (UNIBO), Jean-François Mainguet (ATMEL), Anna Tramonti (BIOK).

Abstract:

This report presents the state-of-the-art of fingerprint aliveness detection and fake prevention methods. Significant experiences and previous studies are surveyed. Well-know techniques for creating artificial fingerprints are introduced and critically reviewed. Aliveness measurements are reported including researches in the medical field. Patent and existing scanners including aliveness detection components are then analyzed. Finally new experiments have been carried out creating new dummy fingers and testing them against some commercial scanners whose producers claim to be able to reject fake fingers.

Keywords:

Biometrics, security, fingerprint scanners, artificial fingerprints, gummy fingers.

© BioSec Consortium

Revision History

The following table describes the main changes done in the document since his creation

Revision	Date	Description	Author (Organization)
v0.1	02/02/2004	First draft	Athos Antonelli (UNIBO), Denis Baldisserra (UNIBO)
v0.2	03/02/2004	Addition from Atmel	Jean-François Mainguet (ATMEL)
v0.2a	04/02/2004	Cleanup of the document	Athos Antonelli (UNIBO)
v0.3	04/02/2004	Additions to chapter 2 and 3	Denis Baldisserra (UNIBO)
v0.4	27/02/2004	Chapter 6, and Section 4.3.1.4, 4.3.1.13	Athos Antonelli (UNIBO)
v0.5	02/04/2004	Chapter 7 and Document review.	Athos Antonelli (UNIBO), Denis Baldisserra (UNIBO) Anna Tramonti (BIOK)
v0.6	12/05/2004	Executive Summary, Conclusions and additions to Section 3.2.	Denis Baldisserra (UNIBO)
v0.7	15/06/2004	Trademarks and additions to Conclusions.	Denis Baldisserra (UNIBO) Athos Antonelli (UNIBO)
V1.0	30/06/2004	Document delivery	Davide Maltoni (UNIBO)

Executive summary

This document discusses the state-of-the-art of fingerprint aliveness detection mechanism applied to on-line fingerprint scanners.

Chapter one introduces the concept of fingerprint scanners spoofing and explains the aim of this research: improve fingerprint scanner security against fake finger attacks.

Chapter two surveys the experiences available in the literature as to fake fingerprint attacks. Particular emphasis is put on two experiences, that can be considered as milestones: the first one conducted by Ton van der Putte, that was able to fool commercially available optical fingerprint scanners using silicone fingers; the second one is due to Matsumoto, that improved previous techniques to fool even solid state fingerprint scanners, using gelatin fingers.

Chapter three explains the techniques used to create a fake fingerprint: 1) with the cooperation of the fingerprint owner or 2) from latent fingerprints.

Chapter four analyzes the measures that can be exploited to prevent fake fingerprint attacks. After a brief introduction dedicated to the desirable characteristics of the aliveness detection methods, several aliveness detection techniques are discussed, stressing their pros and cons.

Chapter five lists the most important patents regarding aliveness detection mechanisms. Each one is explained in detail and commented.

Chapter six describes the experiences we did trying to create new fake fingerprints of different types (silicone, gelatin, etc.) and provides details on the material and process used. We limited our experiences to the duplication with the cooperation of the fingerprint owner.

Finally, chapter seven presents the results we obtained using fake fingers to spoof existing fingerprint scanners. Most of the test have been conducted on scanners whose producers claim to be fake fingerprint resistant.

Trademarks

TS-520 is a registered trademark of Identix.

Checkone is a registered trademark of Fingermetrics.

DermalogKey is a registered trademark of Dermalog.

EFPS110 is a registered trademark of Veridicom.

DFR200 is a registered trademark of Identicator.

Fingsensor is a registered trademark of FUJITSO Ltd.

SystemGuard DT is a registered trademark of Guardware Ltd.

OptiMouse III, EyeD Mouse II and SecuDesktop are registered trademarks of SecuGen.

UareU Personal and UareU Pro are registered trademarks of Digital Persona.

FingerTIP is registered trademark of Infineon Technologies AG.

Siemens ID Mouse and Siemens ID Device Software are registered trademarks of Siemens semiconductors.

Bio-i is a registered trademark of TesTech.

Ethenticator USB 2500 and MS 3000 PC card are a registered trademarks of Ethentica.

AES4000 is a registered trademark of AuthenTec.

Defcon is a registered trademark of Targus.

100 MC is a registered trademark of Precise Biometrics.

TouchChip is a registered trademark of STMicroelectronics.

FingerChip is a registered trademark of Atmel.

All other referenced trade names are trademarks, registered trademarks, or copyrights of their respective holders. Use of a term in this document should not be regarded as affecting the validity of any trademark or registered trademark.

Table of Contents

1. INTRODUCTION

"...
"But is it possible to forge a thumb-print or a finger-print?"
"It is not only possible, but quite easy to do."
"As easy as to forge a signature, for instance ?"
"Much more so, and infinitely more secure. A signature, being written with a pen, requires that the forgery should also be written with a pen, a process demanding very special skill and, after all, never resulting in an absolute facsimile. But a finger-print is a stamped impression- the finger-tip being the stamp; and it is only necessary to obtain a stamp identical in character with the finger-tip, in order to produce an impression which is an absolute facsimile, in every respect, of the original, and totally indistinguishable from it."
..."

R. A. Freeman "The red thumb print", pp. 167, 1907

Every time a new security feature is added to a system, there are always some workarounds that are able to deceive this feature. Fingerprint readers are the new security feature to be added to a system, and spoofing these readers is not a new idea. James Bond in "Diamonds are forever" (1971) was already spoofing Tiffany Case's camera with a thin layer of latex glued on his fingertip, taking the identity of Peter Frank.

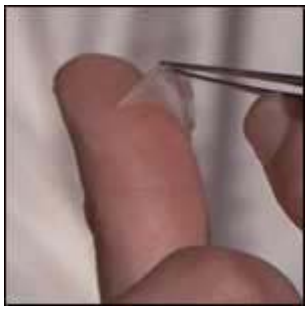


Figure 1: Latex fingerprint

The security of a fingerprint system may be divided into two main areas: electronic security ("Is it an authorized fingerprint system we have at the other end of the wire?") and 'living' security ("Is this finger alive, fake or dead?").

First of all, it is important to remember that absolute security does not exist: given funds, will, and the right technology, nearly any security system can be cracked. Moreover, if you have a gun pointed at your temple (or if you are under any other serious treat), it is likely that you will cooperate whatever the security system is…

But it is possible to make things extremely hard to be cracked.

This document will focus only on the 'living' security. Electronic security is a totally different topic, already studied (e.g. smart cards), and it is not among the document's purposes to check if an enrollment has been properly done (for instance, someone can forge a document with the identity of someone else, but with his own fingerprint template in it).

Aliveness is really a hard task to deal with. How can we say for sure when a finger is dead? Let's simply think when someone cut out his finger: one can put it in ice, run to the hospital and, very likely, the surgeon will be able to mend it.

Nowadays, even the transplant of a whole hand from a deceased donor to another (living) person is possible! Even if we don't have an ultimate solution to this problem, at least we can make things difficult and also select which "security level" we want.

Is it important, in one's application to detect (from the most difficult to the easiest) if:

- A finger belongs to a dead person
- A finger has been cut out (how many hours before?)
- A thin layer of material has been glued to a real finger (be aware: now it is possible to grow skin cells in laboratory for skin replacement, if necessary!)
- A fake finger (made of gelatin, latex, …)
- An image of the fingerprint

Obviously, it is necessary to eliminate any "zero effort" spoofing. Fortunately, and although all the spoofing techniques here described, stealing the fingerprint of someone else is not easy at all; even for forensic professionals is hard to identify people from fingerprints they left in a crime scene.

2. SIGNIFICANT EXPERIENCES ABOUT FINGERPRINTS SCANNERS SPOOFING

Each subsection of this section describes a significant experience of spoofing fingerprint-based systems. The subsection titles are named after the related papers.

2.1 Biometrical Fingerprint Recognition: Don't get your fingers burned. [van der Putte 2000]

In the early 90's Ton van der Putte developed and improved during the following years, a technique to fool all the then available biometrical fingerprint recognition systems. But when he contacted the manufacturers and showed them the security breach in their systems, they thought it was no important the and did nothing to solve it. In 2000 Ton van der Putte and Jeroen Keuning decided to raise people's awareness and published an article "*as a warning to those thinking of using new methods of identification without first examining the technical opportunities for compromising the identification mechanism*".

None of the fingerprint scanners tested by the two Authors (see **Table 1**) was able to perceive the difference between a real finger and a well-made artificial one; still some producers claimed this in their documentation. The Authors described two methods to create artificial fingers, depending on the fingerprint's owner level of cooperation.

- Duplication with cooperation: the two Authors created first a plaster cast of the finger and then filled it with silicone rubber to create a thin silicone dummy of the finger. When the silicone hardened, ready to be used, they carefully removed it and glued it on someone's fingertip as to make it unnoticeable.
- Duplication without cooperation: to obtain a fingerprint, the Authors lifted a latent fingerprint from a glass. The fingerprint was sprinkled with a fine powder then peeled from the glass surface using some scotch tape. The Authors took a photograph of the print and attached the negative to a *PCB* (Prototype Circuit Board) and exposed it to UV light. When the copper was etched, a copy of the print was available. The fingerprint on the PCB was copied by dropping some silicone on the print. It took eight hours to create this type of artificial fingerprint.

Manufacturer	Model	Technology	Date	Difficulty
Identix	TS-520	Optical FTIR	Nov. 1990	First attempt
Fingermatrix	Chekone	Optical FTIR	Mar. 1994	Second attempt
Dermalog	DermalogKey	Optical FTIR	Feb.1996	First attempt
STMicroelectronics	TouchChip	Solid state Capacitive	Mar. 1999	First attempt
Veridicom	FPS110	Solid state Capacitive	Sept.1999	First attempt
Identicator	DFR200	Optical FTIR	Oct. 1999	First attempt

Table 1: Tested Fingerprint sensors

As described before, since 1990 several fingerprint sensors have been tested using dummy fingers. The authors said they fooled the solid state capacitive scanners, for instance, simply moisturizing the silicone finger with some saliva on it. All the sensors tested assumed the dummy finger to be a real one and, almost all, at the first attempt.

2.2 Biometrics: yes or no? [Kàkona 2001]

This Paper shows how it is possible to spoof fingerprint sensors without aliveness detection. The following lines describe the procedure proposed by the Author.

1. Take the fingerprint by smearing the fingertip with ink and pressing it on a piece of paper, as usually done in police movies.
2. Acquire the image with a desktop paper scanner.
3. Convert the resulting bitmap into vectors form to exclude imperfections of the fingerprint on the paper. The potential attacker can use several incomplete fingerprints found on various objects to generate one nearly perfect vector fingerprint image. Finally redraw the fingerprint image, paying attention to place the individual part as accurately as possible.
4. Print the resulting image on a laser printer with at least 600 dpi resolution.

Laser printers apply a powder on the paper which agglomerates with it, partly penetrating the paper and partly protruding above its surface. Actually a significant “protrusion effect” can be observed only on same old models of laser printers and photocopy machines.

The printed image of the fingerprint was successfully logged into a system using on optical FTIR sensors. Placing the stamp on the sensor’s surface did not spoof capacitive fingerprint readers, but it was possible to re-activate latent fingerprints on the sensor’s surface by breathing on it. When the authors breathed on the sensor’s surface the traces of sweat became visible and the sensor responded as if a finger had been placed on it again by the authorized person.

2.3 Body Check: Biometric Access Protection Devices and their Programs Put to the Test [Thalheim 2002]

The Authors tested some commercial available fingerprint scanner sensors against fake finger attacks. The recognizing experiments were performed either on solid-state capacitive (Siemens, Cherry, Eutron, Veridicom and Biocentric) and optical FTIR (*Frustrated Total Internal Reflection*) fingerprint sensors from Cherry and Identix.

2.3.1 Solid State Capacitive sensors

The authors demonstrated the feasibility of spoofing the solid state capacitive fingerprint sensors by re-activating the last acquired image breathing on it, using an adhesive film with graphite powder, or placing a thin-walled water-filled plastic bag on the sensor’s surface. Even if, according to the manufacturer's statements, it should have been impossible, the authors were able several times to gain access by reactivating the last acquired image.

The first experiment was to reactivate the last acquired image simply breathing on the sensor surface. They cupped their hands above the scanner and breathed gently within the shell thus formed upon the sensor surface. By doing so, they were able to see the last fingerprint contours reemerging slowly on the biometrically-protected computer screen.

Figure 2: Reactivating the last acquired fingerprint breathing on the sensor surface.

The second experiment was to reactivate a latent fingerprint placing a thin-walled water-filled plastic bag on the sensor surface. As they discovered, the advantage of this technique is that the water allows a smooth pressure on the sensor surface. Even when the security mode was set to its maximum (extended mode), with a good quality latent fingerprint, only a few attempts to access the system were necessary. They noticed also that capacitive sensors are sensitive to humidity: when damp air condenses on the sensor surface, in presence of grease left by a finger, the related dielectric constant on the sensor surface leads to a change in capacitance which the device interprets as a released signal inducing it to undertake a measurement.

Figure 3: Reactivating a latent with a little water in a plastic bag.

The third experiment was to reactivate a latent fingerprint by sprinkling the greasy traces left on the sensor surface with common graphite powder, then placing an adhesive film over the sensor surface with a slight pressure. As they were only occasionally successful using the breathing or the water bag method, their success rate with the adhesive film technique, in presence of good quality latent fingerprints, was almost totally positive.

Figure 4: A fingerprint on adhesive film.

Siemens solid state capacitive scanner was equipped with an algorithm to check whether the currently scanned fingerprint and the last one were the same. This algorithm was introduced to prevent the system from attacks based on latent image reactivation. However, the Authors, using one of the methods described before, were able to re-activate latent fingerprints and access the system.

The fourth experiment was to capture a latent fingerprint from a smooth surface, a glass or a CD for instance, using a police fingerprinting kit. They sprinkled prints with graphite powder, peeled them from the surface using adhesive film and placed them on a scanner applying a gentle pressure. The success rate with this approach was very high, regardless whether the system was in normal or in extended security mode.

2.3.2 Optical FTIR sensors

To fool optical scanners, the Authors forged a fake fingerprint using the wax of small tea-warming candles as mold and silicone. Wicks removed, they pressed their fingertips into the warm wax and filled the mold with commercially available silicone. This artificial fingerprint was successfully used during authentication and enrollment phase.

The Authors noticed how was also possible to deceive the sensor using graphite powder and scotch tape, holding an halogen lamp from a distance of about 30 centimeters. They observed that an intense back-lighting, while enhancing the contrastive properties of graphite powder, was also inducing a sort of blindness in the sensor.

2.3.3 Solid-state thermal sensors

Only with silicone copies of an authentic fingerprint the Authors were able to obtain some results. They said that with a little bit of practice, it would have been possible to use silicone copies during enrolments and verification as well.

2.4 Impact of Artificial Gummy fingers on Fingerprint Systems [Matsumoto 2002]

The Authors focused their attention on whether a fingerprint systems can be spoofed or not in accepting an artificial finger as a substitute of a real one. Prior to this paper they made silicone fingers and tested fingerprint system with them. From the results that they obtained by testing several scanners they concluded that systems with capacitive sensors and some with optical sensors could reject silicone fingers. In order to investigate this, they carried out experiments with a new kind of material: gelatin.

The experiments involved eleven commercial available fingerprint sensors, both optical and capacitive (see **Table 2**). The sensors produced by Sony were equipped with an aliveness detection mechanism that claimed to be able to recognize a live finger from an artificial one.

Device	Manufacturer	Product Name	Technology
A	Compaq Computer Corp.	Standalone Fingerprint Identification	Optical FTIR
B	Mitsubishi Electric Corp.	Fingerprint Recogniser	Optical FTIR
C	NEC Corp.	Fingerprint Identification Unit	Optical Sheet Prism
D	OMRON Corp.	Fingerprint Recognition Sensor	Optical FTIR
E	Sony Corp.	Fingerprint Identification Unit	Optical FTIR
F	FUJITSU ltd.	Fingsensor	Solid State Capacitive
G	NEC Corp.	Fingerprint Identification Unit	Solid State Capacitive
H	Siemens AG	FingerTIP Evaluation Kit	Solid State Capacitive
I	Sony Corp.	Fingerprint Identification Unit	Solid State Capacitive
J	SecuGen Corp.	EyeD Mouse II	Optical FTIR
K	Ethentica Inc.	Ethenticator MS 3000 PC Card	Optical Electro-optical

Table 2: The list of fingerprint devices

The Authors tempted an one-to-one verification one hundred times and counted the times that the sensor recognize the finger presented as a real finger. The types of experiments that were carried out are presented in the following table (see **Table 3**).

Experiment	Enrollment	Verification
L - L	Live Finger	Live Finger
L – A	Live Finger	Artificial Finger
A – L	Artificial Finger	Live Finger
A - A	Artificial Finger	Artificial Finger

Table 3: Types of experiments

Two different methods were used to forge the prints:

- Co-operative: They filled the mold left by pressing a live finger into a soft plastic material with a jelly solution (gelatin and water in a 50% solution heated to its melting point) as to create an artificial finger.

- Non co-operative: A fingerprint image was captured from a residual fingerprint with a digital microscope and used to make a mold. This fingerprint was created by pressing a finger against a glass to have a residual fingerprint that was captured with a digital microscopic camera. The acquired image was enhanced and printed on a transparent sheet to make a mask for a photo sensitive PCB. When the PCB had been processed the remaining copper had the form of the fingerprint and was used as a mold to create an artificial finger. The fake finger was obtained dropping a jelly solution (gelatin 40% and water in a solution heated to its melting point) on the PCB.

All the fake fingerprints forged with their owner cooperation were enrolled and positively verified by the system with a rate varying between 68% and 100% (see **Figure 5**). All the fake fingerprints forged without cooperation were enrolled and positively verified by the system with a rate of more than 67% (see **Figure 6**).

The experiments were performed on 5 subjects for the artificial fingers cloned with molds (method 1) and 1 subject for artificial fingers created from residual fingerprints (method 2). The authors tested 11 fingerprint readers.

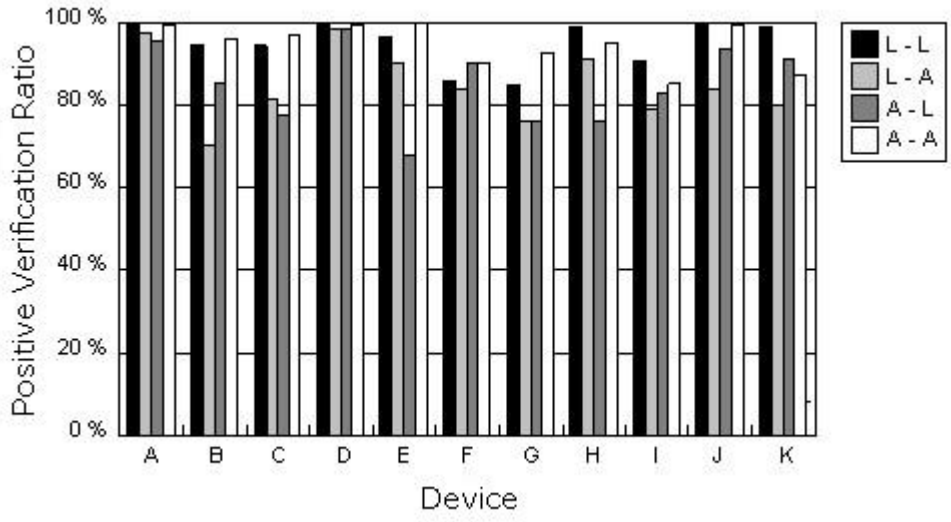


Figure 5: Positive verification ratio for gummy fingers made from live finger.

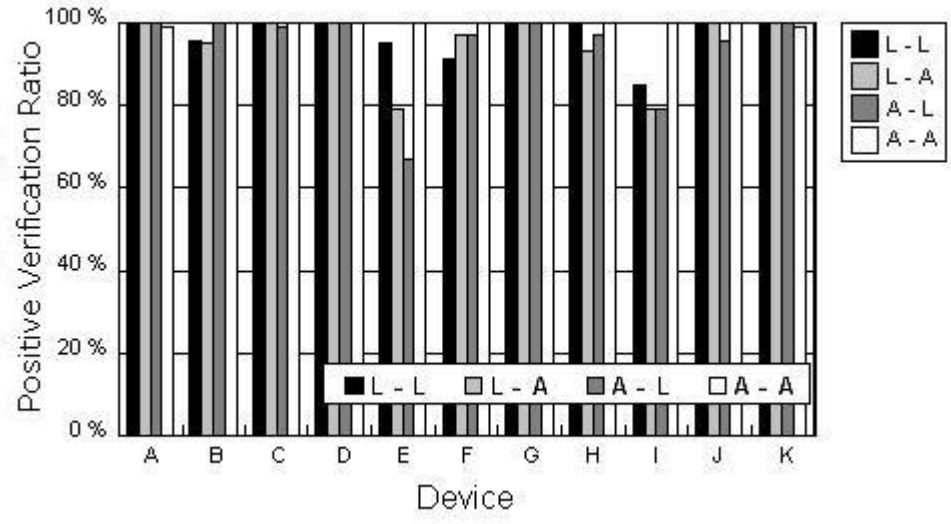


Figure 6: Positive verification ratio for gummy fingers made from residual fingerprint.

The authors demonstrated that artificial fingers can spoof commercial fingerprint systems and that it was possible to forge artificial fingers out of other materials than silicone

2.5 A Study on Performance Evaluation of the Aliveness Detection for Various Fingerprint Sensor Modules [Kang 2003]

This study extended the previous researches ([Matsumoto 2002] and [van der Putte 2000]) by testing more fingerprint sensors (see **Table 4**) and evaluating their aliveness detection capability in a quantitative way.

	Optical		Solid State	
	FTIR	Electro-optical	Capacitive	Thermal
Device	A	C	B	D
DPI	500	403	250	500
Aliveness Detection	YES	YES	NO	YES
Sensor				

Table 4: Sensors involved in the experiments.

This study focused on performance evaluation of fingerprint sensors based on different sensing mechanisms such as optical FTIR, capacitive, thermal and electro-optical [Maltoni 2002]. The artificial fingerprints used for this research were made of gummy as well as silicone rubber. Each fingerprint sensor was tested in terms of positive verification ratio and score distributions obtained with a fingerprint matching algorithm developed by the Authors.

The experiments carried out with silicone-rubber fingerprints showed that the optical FTIR, the capacitive and the electro-optical sensors can not be spoofed with this kind of artificial fingerprints (see **Figure 7**). The optical FTIR sensor had a software-based aliveness detecting capability based on skin color. The capacitive sensor did not work with silicone fingerprints because silicone is not a conductive material. The authors says that electro-optical sensor failed to acquire image from a silicone finger because the light is absorbed by the black rubber surface but the thermal sensor can be spoofed by silicone rubber fingers.

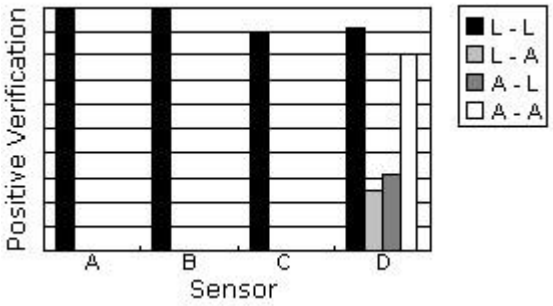


Figure 7: Experimental results by silicone fingers

The Authors reported that the optical FTIR sensor was easy to spoof with a gelatin fingers, regardless of the level of security. To demonstrate this statement, they tried to spoof the sensor varying the security level. The experiment results are shown below (see **Figure 8**).

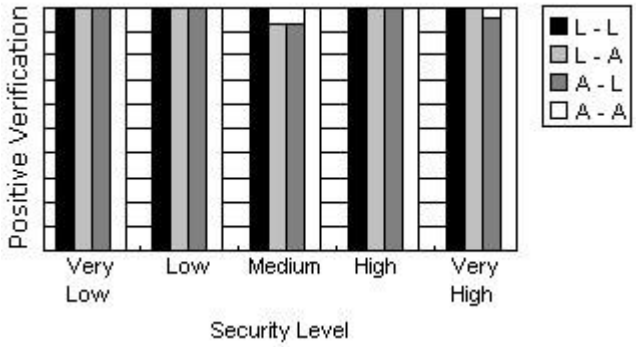
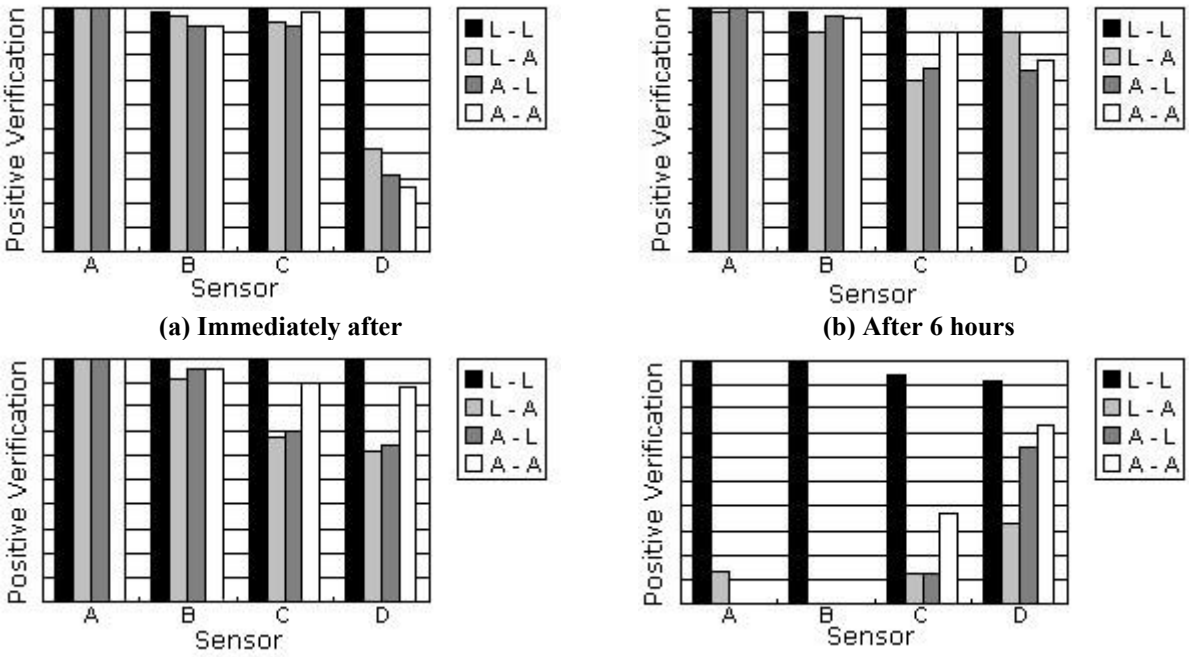


Figure 8: Evaluating aliveness detection varying security level.

As gelatin hardness may vary, due to loss of water as time passes, the Authors decided to test if and how this loss affects aliveness detection rate. So the positive verification ratio was measured 100 times immediately after, 6 hours after, 12 hours after and 24 hours after the gelatin finger was made (see **Figure 9**). All of the sensors showed low positive verification ratio after 24 hours when the gelatin became useless because it has dried. As silicone physical properties do not change significantly on time the same test was not performed on silicone fingers



(a) Immediately after **(b) After 6 hours**

(c) After 12 hours **(d) After 24 hours**

Figure 9: Results of verification tests using gummy fingers as time passes

Concluding, the Authors observed that fingerprint aliveness detection mechanisms included in some commercial fingerprint sensors are able to reject fingerprints made of non conductive material, like silicone rubber, but are not resistant to conductive material, like gelatin. Gelatin is more difficult to maintain than silicone and tend to become useless short after its creation.

2.6 Evaluation of Biometric Security Systems Against Artificial Fingers [Blommè 2003]

This report examined fingerprint readers' capability to withstand an artificial finger attack. The method used for experiments was based on Ton van der Putte & Jeroen Keuning [van der Putte] and Tsutomu Matsumoto's experiments [Matsumoto].

Experiment	Enrollment	Verification
L - L	Live Finger	Live Finger
L – A	Live Finger	Artificial Finger

Table 5: Experiment Types

The artificial fingers in this report were forged in a mold obtained from a real finger. The molding material chosen for these experiments was a two components silicone-paste that vulcanize at room temperature. The authors rolled the paste into a ball and gently pressed the finger into the paste until it cloned the fingertip.

As demonstrated in the previous experiments, to obtain a fake finger, a jelly solution was dropped into the mold as to fully cover the print left previously.

In this report three fingerprint sensors have been tested: the one produced by Targus, the one by Identrix and the one by Precise, each one with its own software. Both Precise and Targus use the same sensor, AES 4000, a solid state one based on electric field [Maltoni 2002], whereas Identrix uses an optical sensor. The experiments showed that all tested sensors were spoofed by artificial fingers made of gelatin, with different easiness depending on sensor and software characteristics.

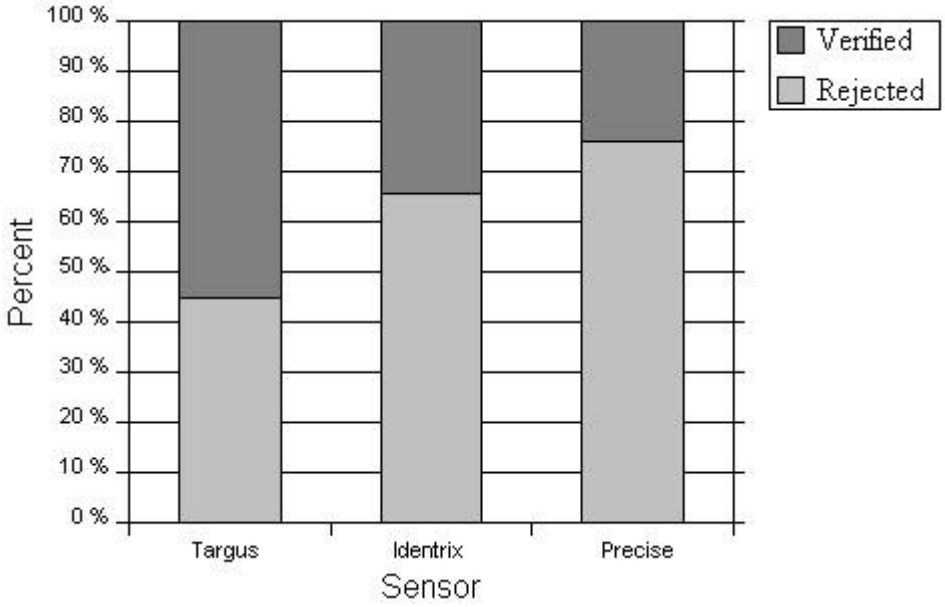


Figure 10: Positive verification for each sensor.

The test results with the artificial fingers showed that the fingerprint scanners were not able to cope with artificial copies.

3. MAKING A FAKE FINGERPRINT

> *"...*
> *A mould would be made by pressing the finger into some plastic material, such as fine modeling clay or hot sealing wax, and then, by pouring a warm solution of gelatin into the mould and allowing it to cool and solidify, a cast would be produced which would yield very perfect finger-prints*
> *..."*
>
> *R. A. Freeman "The red thumb print", pp. 167, 1907*

In this section the process of creating fake fingerprint is discussed, starting from van der Putte and Matsumoto's experiences, and critically reviewed.

There are different ways to make an artificial finger from a given alive one. We can obtain the impression from a live finger with the cooperation of the finger owner. By pressing the live finger against a soft material we obtain a fingerprint image that can be used as a mold to forge an artificial finger.

Otherwise, a latent fingerprint could be captured thanks to a digital camera and a special illumination, eventually after enhancing it with special powders; it may be horizontally mirrored by image processing software, and then printed on a material to produce an artificial finger.

3.1 Duplication with cooperation

Duplicate a fingerprint with the co-operation of its owner is the easiest method ever, being possible to compare the resulting dummy fingerprint with the original one and adapt/improve it accordingly.

In the early 90's Ton van der Putte described how to create artificial fingerprints and he was able to spoof some commercial fingerprint sensors. The following lines describe, step by step, how to create a silicone fingerprint with the cooperation of the finger owner. With the right materials and procedure, the method requires only a few hours.

1. Beforehand, the finger should be washed with soap, to make plaster flow more easily through the valleys of the print.
2. Using modelling-wax a kind of bowl is formed at the nail side of the finger and around the tip of the finger. This bowl is filled with plaster to obtain a print of the finger. Preferably the plaster should be of a good quality (such the one used by dental technicians).
3. The dried plaster is a bowl with a perfect fingerprint inside. In order to make a very thin dummy, a pounder that fits the mould (apart from a 1 mm distance for the dummy) can be created using plaster.
4. Silicone waterproof cement or liquid silicone rubber is placed in the mould and the pounder is pressed firmly on top of this layer.
5. When the silicone has hardened, the dummy should be very carefully removed and is ready

Figure 11: A wafer thin-silicone dummy of a fingerprint.

In 2002, Tsutomu Matsumoto used free molding plastic for the mould and solid gelatin sheet for the artificial finger, that he called gummy finger. While silicone is an insulating material, the moisture and electric resistance of a gummy fingers are quite close to those of a real finger (see **Table 6)**.

	Moisture	Electric Resistance
Live Finger	16%	16 Mohms/cm
Gummy Finger	23%	20 Mohms/cm
Silicone Finger	Impossible to measure	Impossible to measure

Table 6: Characteristics of finger.

The following lines describe, step by step, how to create a gelatin fingerprint with the cooperation of the finger owner. Again, given the right materials and practice, this method requires a limited amount of time:

1. Put the free molding plastic into hot water, whose temperature is around 60°C, to soften it, and then take it out.
2. Wait until the plastic will get a little cooler, and then make it round as a small ball.
3. Press the finger against the plastic ball to make the fingerprint mould, applying the same pressure as it has to be scanned by a fingerprint device.
4. Wait till the plastic hardens, and then remove the fingertip from the mould. It takes around ten minutes.

(a) Put the plastic into the water to soften it.

(b) Press a live finger against it.

(c) The mold.

Figure 12: How to make a mold

When the mould is ready to use, it is possible to prepare the gelatin, following this procedure:

1. Add boiling water (30 cc) to solid gelatin (30 grams) in a bottle and stir them. Cap the bottle and wait till the mixture forms a gel as it cools. Then melt it to form a solution heating it in a microwave oven. After that, cool down to form a gel and heat up to form a solution several times to reduce bubbles, if necessary. As a result of this procedure you will have a jelly liquid.


(a) Add gelatin to boiling water


(b) Mix up the solution


(c) Gelatin.

Figure 13: How to prepare gelatin.

2. Pour the liquid into a mold. Remove carefully eventual bubbles around the mold base, if necessary.
3. Put this mold into a refrigerator to cool, and wait for about ten minutes


(a) Pour the solution into the mold.


(b) Put it into refrigerator to cool.


(c) The gummy finger.

Figure 14: How to make a gummy finger.

3.2 Duplication without cooperation

For duplication without cooperation, it is necessary to get a latent fingerprint of a good quality left on a surface. There are many ways used by scientific police to get latent prints which are quite difficult to perform and need knowledge from such fields as applied chemistry, forensics and computer sciences. [Lee 2001].

Anyhow, to do this, you need to be physically close from your target, and make sure that you get the right fingerprint. This is generally very difficult to achieve (try yourself to get the fingerprint of someone randomly chosen in the street), and there are very few situations where it is possible to collect the fingerprint. The fingerprint scanner itself is probably the best way, excepted in the case of a sweep sensor. If the scanner is cleaned before someone uses it, a good quality print is left on the scanner surface. However, scanner surfaces are normally dirty and the chances to find a neat print are low.

Special skills are required to create a dummy from a latent fingerprint. The following method was developed by Ton van der Putte, in the early 90's. Obviously, dummies can not be better than the print itself; therefore to forge a good dummy, a good print is required.

1. First, it is necessary to lift the print from the surface where it lays. An enhancing powder (like the one used by the police) is applied with a brush, then the print is peeled off using some scotch tape.

2. A photo of the print is taken (with a standard camera) placing the tape on the photosensitive side of the film and making a picture of a diffused light source.
3. Then the negative is attached to a photosensitive PCB and exposed to UV light; negative removed, the PCB is developed in an etching bath: the parts of the PCB that were exposed to the UV light are washed away. A final etching bath (sour) etches the copper layer. The result is a very slim profile (about 35 micron) that is an exact copy of print, copied in step 1.
4. After deepening the profile to resemble the depth of a regular fingerprint, a silicone waterproof cement stamp can be created.

The procedure takes about eight hours.

Figure 15: A stamp type dummy of a fingerprint.

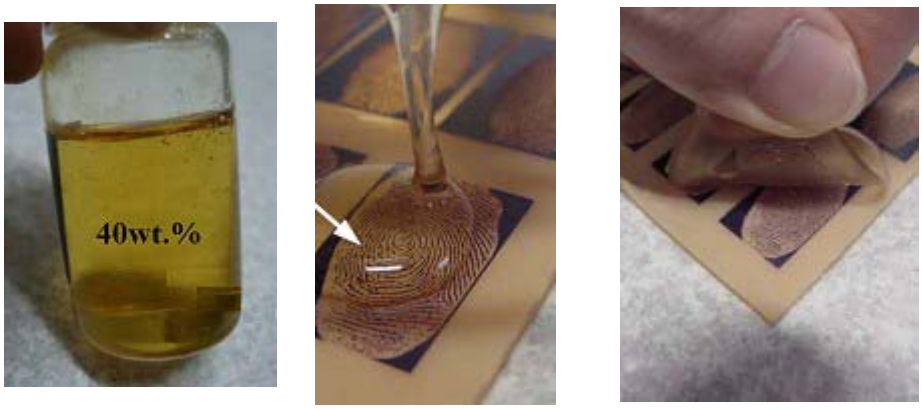
Matsumoto's approach is quite similar: starting from a latent print left on a glass plate he used a photo sensitive coated PCB to make the mold and a solid gelatin sheet to forge the artificial fingerprint

1. A cyanoacrylate adhesive was placed on a latent fingerprint to enhance it. Matsumoto noticed that keeping for a little while the glass plate in an airtight container, the fingerprint was outlined more clearly.
2. A fingerprint image was taken with a digital microscopic camera and set right side left. A better contrast was obtained with an image processing software.
3. The fingerprint image was then printed on a transparent sheet with an inkjet printer to obtain a sort of mask

Once the fingerprint image was acquired, it was possible to make the mold.

1. He fixed the printed side of the mask on a photo sensitive coated PCB and exposed it under an UV light source for 6 minutes to copy the mask on the photo resist layer of the PCB.
2. Develop the PCB to remove all the unnecessary photo resist, and expose the unnecessary copper.
3. Etch the developed PCB to remove all the unnecessary copper, and get only the fingerprint. Finally, the mould for artificial fingers can be obtained.

To create a fingerprint using the mould follow the procedure described in previous section.



(a) Gelatin **(b) Drop the liquid in the mold** **(c) Put this mold into a refrigerator and then peel carefully.**

Figure 16: How to make an artificial fingerprint without co-operation.

4. ALIVENESS MEASUREMENT

To be able to detect a fake, firstly we must answer to this question: what a live finger is like?

The activities related to liveliness are:

- The cellular metabolism with material transformation (protein…)
- The movement
- The heat production (which is sub-product in fact)
- Blood circulation for material delivery and heat transportation (regulation)

This activity has a lot of signatures: physical, chemical, mechanical, nervous, geometrical… and moreover, signification changes with the observation scale.

Medical techniques to monitor patients exist for a long time, so it is natural to check what are the usual methods used in hospitals. At first sight, it should be a little bit easier just to test for liveliness than trying to detect a disease.

4.1 Constraints

But the problem is a little bit more complicated, because we have more constraints. Aliveness detection must be:

- Non invasive: it is not allowed to make a "hole" in the skin to see if there is some blood inside...
- No nociceptive methods: we must not have a bad feeling such as surprise, harm, pain…, it must be friendly
- No dangerous chemical involved: it is not possible to use any acids, radioactive or biohazard products…
- No allergenic reactions
- Short measuring time: it is not possible to ask the user to give his/her finger more than a few seconds.
- Low cost

4.2 What is a finger?

A finger is:

- A structure from 1 to 10 cm^3, containing cells, bones, nail, no muscle (so electrical activity linked to muscle comes from other areas).
- Arterial blood brings all the chemicals and oxygen necessary to the cells, heat. Blood returns to the body in veins.
- About 2 watts/kg is spent in the body so it is about 10 mW for one finger, (just to give an idea of the energetic level for comparison with techniques that inject energy).

Skin is composed of several layers:

- The stratum corneum about 100 micron thick, made of dead cells, more or less hydrated.
- The blood-free epidermis: 0.05 to 1 mm thick made of proteins, lipids and melanin-forming cells, making the characteristic brown color of the skin.
- The dermis, which consists of dense connective tissues, sweat glands, capillaries…
- The hypodermis

4.3 Detection methods

Here is an extensive list of possible effects to use to detect life. Remember that it is not possible to be absolutely sure to have scanned all possibilities to detect the liveliness of a finger, and new technologies may be later found.

4.3.1 Skin / flesh

4.3.1.1 Thermal measurements

- Temperature of a normal finger is around 33ºC, but may vary between 10ºC and 40ºC, so this is not a reliable characteristics. Moreover, spoofing a thermometer requires no effort (just put your cut finger in your armpit or mouth).
- Thermal conductivity measurement necessitates a very good thermal contact, which is not so easy to achieve, and takes about 15 to 20 seconds. Moreover, it is quite easy to find out some material that exhibits almost the same thermal characteristics than the skin.

4.3.1.2 Microwaves

Excepted temperature measurement, microwave is not usable as liveliness detection.

It is also too linked to cooking devices, so it is likely to be rejected by users. In any case, we cannot send more than a few mW in the finger!

4.3.1.3 Ultrasonic measurements

Ultrascan and Optel are working on fingerprint readers using ultrasound. One difficulty is the cost and the size of the ultrasound emitter/receiver,

Echography is a common non-invasive method in medical area to study the internal organs of the body, and as air is a bad ultrasound transmitter, it generally requires some gel to get a good picture. It is possible to get a good picture of the skin layers, it is even possible to read the blood flow by Doppler effect.

Unfortunately, it seems too difficult to achieve an automatic good liveliness detection, it always requires some human analysis.

4.3.1.4 Flexibility measurements

Skin is flexible, and this property can be measured using some specific vibrating material, which is not enough robust for everyday usage.

It has also been proposed to measure the skin color which changes when the blood is rejected because of the applied pressure (the finger is becoming white), which is not an easy feature to control.

By noting that the finger pressure against the sensor surface is not uniform but decreases from the center toward the borders, Cappelli, Maio and Maltoni [Cappelli 2001] defined a skin-distortion model with three distinct regions:

- An inner region in close contact with the surface, where the pressure do not allow any skin slippage;
- An external region where the light pressure allow the skin to freely follow the finger movements;
- An intermediate region between the above mentioned two regions, where skin compression and stretching take place.

The user can be instructed to move the finger while pressing it on the scanner surface. By rotating or translating the finger the elasticity of the skin can be measured.

It is likely that we can find some material quite similar to the skin, and it does not prove that the finger is living. But this is an additional test at practically no cost, so it will be more difficult to spoof.

4.3.1.5 Electrical measurements

- Skin conductivity: this is the most common system to detect liveliness, and it has showed not to be reliable, because the stratum corneum (the last layer of the skin) is made of dead cells which are more or less hydrated, so the skin conductivity varies too much.
- Skin impedance: this is an analysis of the returned signal when using several excitation frequencies. It can be seen as a more sophisticated measurement than conductivity. With this method, it is possible to measure the fat percentage. This is one of the most studied area for liveliness detection because it requires very few material, so it is quite cheap. But it is quite hard to get reliable measurements.
- Impedance plethysmography
- Biomagnetism : there is no magnetic activity in the flesh, and trying to measure the magnetic activity of the hydrogen atoms to identify typical molecules of the flesh is just not reasonable.

4.3.1.6 Light measurements

Light (by extension any electromagnetic radiation) is one of the best medium to measure a liveliness signature, because it is very often very fast and reliable. There is two ways to use light:

- Transillumination: consists of sending some light from one side, and reading the remaining light at the opposite side.
- Reflection: consists of sending some light on one side, and collecting the reflected light on the same side. Generally, there is less signal and information, but this is more practical to use.

You will find later the measurements related to the cardiac pulse, only skin is studied in this section.

4.3.1.7 Skin reflectance, absorption.

The spectra of the reflected/transmitted light by the skin is quite characteristic, mainly linked to the hemoglobin properties.

Measuring a spectra requires a light source and a spectrometer which are large and expensive material. The reflected light only is probably not enough as some material will probably fake the skin spectra quite easily.

Lumidigm is working on recognition using the light transmission in the skin.

4.3.1.8 Fluorescence spectroscopy

Some biological molecules exhibit fluorescence, that is re-emit incident light under another wavelength. For instance, if you send an UV pulse @290nm you obtain a resulting signal in the @320-340nm from the stratum corneum thanks to the tryptophan.

The main problem of this technology is the large expensive material (pumped laser…) to perform this measurement.

4.3.1.9 Raman spectroscopy

Raman spectroscopy is a spectral measurements on molecular media based on inelastic scattering of monochromatic radiation. This is a very precise technology to measure molecules, but necessitate quite an expensive an large material (laser, spectrometer…).

Take care that "fingerprint Raman" is a common wording to speak of Raman spectra, and has nothing to do with fingerprint recognition.

4.3.1.10 Optical coherence tomography

Optical coherence tomography uses "echoes of light", more or less like ultrasound, but with an order of magnitude better. It requires a Michelson interferometer with a broadband light source, so again, this is not a reasonable technology for us.

Associated with Doppler effect, it is even possible to perform vessel imaging!

4.3.1.11 UV, X-ray, radioactivity

Ultraviolet light is stopped by the melanin, so the resulting signal is quite weak. It may be used just to detect non-absorbing UV material, making sure we have no skin in that case, but this is not enough to make sure we have a live finger. Moreover, UV sources are still quite expensive.

X-ray and radioactivity cannot be used in our scope for obvious reasons.

4.3.1.12 Chemical measurements

Using a specific chemical reaction of the skin is almost impossible to use, because:

- we cannot refuel the sensor with the necessary chemicals
- it always requires very clean material
- it is likely that we'll have some allergenic reactions
- sweat is corroding…

DNA detection is beyond actual technical possibilities, and even if it was existing, it would be too easy to fake.

pH detection is too easy to spoof, and not reliable in the context of the finger.

4.3.1.13 Odour

On the skin it is possible to find over 300 volatile compounds [Bernier] which can be used to discriminate between human skin and silicone replicas. An electronic nose can be coupled with a fingerprint scanner to sniff the skin of the finger and recognize a real finger.

Nowadays CMOS odor-sensing devices are quite cheap, and used in different application to work as a natural nose (for example for discriminating between two different tea blends), or to recognize a volatile chemical like no humans can do (to measure air pollution).

Integration of this sensors into a fingerprint scanner is not a trivial task, but it is worth trying to do it.

4.3.1.14 Perspiration

CiTER [Schuckers 2003] is working on fake detection using perspiration. It is likely to be very sensitive to external conditions, as humidity and temperature, and on the skin state. In particular it requires the fingerprint surface to be perfectly dry when the finger get in contact with the scanner.

4.3.2 Nervous activity

4.3.2.1 Electroencephalography (EEG)

EEG measures the electrical activity of the brain, which is certainly a good liveliness signature. Most of the time, we would like to say "I'm the person I claim I am, and I agree to the transaction".

EEG is not feasible in our context: there is almost no remaining electrical signal coming from the brain up to the fingertip.

4.3.2.2 Electromyography (EMG).

Electromyography consist of measuring the electrical activity linked to the muscle activity. Note that heart activity (Electrocardiography) is studied in a separate chapter.

As there is no muscle in the finger, there is almost no electrical activity we can reliably detect. At best, this is coming from the only muscle in the hand, or the forearm, and it necessitates very good (large) electrodes, using gel, to compensate the bad conductivity of the stratum corneum. Moreover, this is very sensitive to the noise environmental.

4.3.2.3 Nervous stimulation

It would be nice to send a nervous stimulation to the finger, and measure the reaction, because in that case, we are pretty sure that the signal went up to the nervous centers or brain of the owner, so we are sure that the subject is alive.

Unfortunately, it is generally not acceptable to use this method, people will naturally reject such kind of system because if it reach the brain, then you really feel it. Imagine if we send an electrical shock, even small! An automatic nervous reaction, not reaching the consciousness, seems to be the only acceptable method, but well, no automated measurement like that exists at the moment, and it is hard to imagine at the fingertip, which is one of the most sensitive part of the body.

4.3.3 Blood pulse / cardiac pulse

The heart is one of the best candidate to make a liveliness test. It has a lot of impact everywhere in the body, and if we are able to capture a signature typical from the heart, we are pretty sure to have a live person.

4.3.3.1 Sound

The noise of the heart cannot be monitored at the fingertip, even if bones are well-known to conduct sounds.

4.3.3.2 Ultrasound

Blood circulation can be (hardly) measured thanks to the Doppler effect using ultrasound. It seems extremely difficult to automate such measurement.

4.3.3.3 Sphygmomanometer

Blood pressure refers to the pressure of blood on the walls of the blood vessels of the body. Applying pressure on an artery at the fingertip is not an easy task to automatically make at the fingertip, an air pressure chamber is necessary. Some medical device exists, but they are quite expensive, and requires the user to put his/her fingertip inside a hole for the measurement (so not user-friendly).

4.3.3.4 Piezoelectricity

It is possible to "glue" some quite large piece of piezoelectric material on the arm to measure the cardiac pulse, but unfortunately the signal is too weak at the fingertip.

4.3.3.5 Plethysmography, photoplethysmography, impedance plethysmography

Plethysmography consists in measuring the volume change linked to the cardiac pulse using pressure. This is usable on the arm or the leg, but not on the fingertip.

Photoplethysmography is the same using light, as the blood volume changes, the transmitted light varies as well. Pulse oxymetry (see further) is an enhanced version of this.

At least one company (Tarian) tried to perform recognition using the shape of the blood pulse, measured with light.

Impedance plethysmography uses the electrical impedance changes also linked to the blood volume changes. It is used only with the legs to our best knowledge, and requires quite large electrodes well connected to the skin (conductive gel).

4.3.3.6 Electrocardiography (ECG)

ECG (or EKG from the german root) is an attractive method, as the heart has a powerful electrical activity. Regular ECG uses several electrodes (12) directly near the heart, but it is possible to make measurement from the hands and feet.

One important thing is to make a loop: if you try to read the electrical signal just at the end of one fingertip, there is almost no signal. So you absolutely need to have one finger connected to one electrode, and the other hand connected to the other electrode, which is not that easy to achieve from an ergonomic point of view.

3M made in the past an optical fingerprint reader with blood pulse measurement as well as ECG, but it was too expensive.

4.3.3.7 Oxymetry

Pulse oxymetry is a very common and well-know measurement of the blood oxygenation, that is the percentage of oxyhemoglobin compared to deoxyhemoglobin. This is measured thanks to infrared LEDs at the end of the finger and is a good candidate for liveliness detection, especially for cut fingers.

Its main defect is the fact that you need to wait several cardiac pulses to perform the measurement, so it is quite long. Existing devices are quite expensive, but it is likely that a "degraded" version just to detect liveliness would be less expensive, as we don't need to know the exact percentage of oxygen in the blood, so calibration is less a problem.

4.3.3.8 Doppler-laser

A laser can read the blood flow using Doppler effect. This is quite a difficult measurement as you need to precisely find an artery or a vein, and requires a laser.

4.3.3.9 Infrared imaging

PosID proposes to take a infrared picture of the finger to map the temperature. Requires an (expensive) infrared camera.

4.3.3.10 Sound

It is almost impossible to "hear" any body noise (mainly the heart and respiration) at the fingertip. Anyhow, spoofing a microphone with a record is too easy to achieve.

5. PATENTS AND SCANNERS WITH ALIVENESS DETECTION

Several patents have been issued to protect methods and techniques for aliveness detection in fingerprint acquisition devices. Most of them exploits measurements and/or concepts introduced in section 4.

- WO 01/10296 : piezoelectric film (PVDF), uses acoustic reflections. May detect blood circulation using Doppler effect, or bones.
- WO 01/124700: (Veridicom) image analysis
- US 2002/0076089: visible and infrared images
- US 2003/0044051: finger color detection
- US 2003/0025897: red & green LED, then difference
- US 2002/0131624: two lights
- US 6597945: (Infineon Technologies AG) measure of the impedance of the skin
- US 6373967: (CalTech) secret finger sequence
- US 6327376: (Philips) electrodes on optical device
- US 6326644: (TesTech) Contact light emitting device
- US 6292576: (Digital Persona) uses two orthogonal lights
- US 6259804 & 6088471: (AuthenTec) gain control features and anisotropic dielectric coating
- US 6181808: (NEC) electrical activity of muscles
- US 6180868 & 6144747: (NEC) using electrodes
- US 6175641: (Guardware Systems) electric measurements of the dielectric constant of the skin
- US 6064753: (IBM) measure applied force
- US 5180901: with pressure, the finger becomes white
- US 2003/0039382 & US 5982914: count the number of pores

Some of the above patents are being implemented in commercially available scanners; the following list includes commercially available scanners whose manufacturers claim to be fake finger proof:

Manufacturer	**Product**	**Aliveness Measurement**
Guardware System	SystemGuard	Electric measurements of the skin.
Secugen	OptiMouse III	Software level.
Digital Persona	U.areU. Pro	Check the reflection ratio of the finger.
Testech	Bio-i	Conductivity of the skin
Ethentica	Ethenticator USB2500	Conductivity of the skin
Authentec	AES4000	Electric Field
Infineon Technologies AG	FingerTip	Skin Impedance

5.1 Guardware Systems

http://www.guardwaresystems.com

Guardware Systems (Budapest, Hungary) produces the "System Guard" line of fingerprint scanners, as a stand-alone solution (DT model), embedded solution (PL model in a 5.25" rack) or integrated on a keyboard (KB model).

According to our analysis, the core of the system is the BioSensor which is equipped with a 'aliveness check'. The manufacturers state that their aliveness check "*...performs static and dynamic measurements, and blocks the authentication process if presented with a fake (e.g., silicone, rubber, or gelatin) finger*" [Guardware 2003]

They also claim of being aware of the tests made in [Matsumoto] and [van der Putte]: "*...Really high security applications of fingerprint systems demand a vital feature: live finger detection. Most of the currently available fingerprint scanners are still facing the problem of being easily fooled with three-dimensional finger replicas made of silicone, rubber or gelatin. Guardware has developed the solution for detecting and rejecting all kinds of finger surrogates. With the implementation of the patented biosensor – a live finger detector – the integrity of the fingerprint recognition system is ensured.*"

Some details are provided to explain the technology underlying the 'aliveness check':

"*Several dynamic measurements are made in every tenth of a second while the finger is being placed on the scanner and the finger surface gets completely spread. When the finger is on the sensor, the static parameters are constantly being measured. If the already stable static value changes to an unacceptable extent, the biosensor rejects the finger immediately*"

Looking at the Patent US #6,175,641 "Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus" more details can be understood.

The Guardware BioSensor is an optical FTIR sensor equipped with transparent electrodes on the acquisition surface that measure the dielectric constant of the skin (that has a range of 60-90, far from silicone dielectric constant that is 5-30). It also measures the impedance of the finger. The system does not only measure static values, but also tracks down variation on skin surface electrical properties as a function of the time, while the finger is touching the sensor. The verification time is typically below 0.6 seconds.

5.2 SecuGen

http://www.secugen.com

SecuGen produces a mouse with an embedded optical finger sensor. Matsumoto tested (and fooled) the SecuGen EyeD Mouse II with SecuDesktop v.1.55 in [Matsumoto 2002]. SecuGen tried to reply to this attack with the release of an improved version (both hardware and software were modified) called OptiMouse III with SecuDesktop2000.

As Won Lee, Chief Technical Officer, said: "*To defeat spoofing techniques, we have combined a proprietary algorithm with physical changes to the optical sensor to detect all known methods of defeating a fingerprint biometric system.*"

Instead of a detection based on physical characteristics of the finger as temperature, transparency, pulse or electrical characteristics, they have a different approach detecting some basic characteristics of the spoofing methods itself. Unfortunately, no further details are provided, but they also claim: "*While other fingerprint systems, including those using 'live finger detection', are fooled 75% to 100% of the time by a 3D gelatin mold recently referred to as a 'gummy finger', the new SecuGen system consistently rejects such a mold.*" [SecuGen 2002]

5.3 Digital Persona

http://digitalpersona.com

The Digital Persona U.are.U Personal has been tested in the 2002 and easily spoofed by the reviewer [Dan 2002].

The U.are.U Pro includes an advanced method to detect a fake finger: it uses two orthogonal lights, then two images are acquired and a mathematical computation enables to discriminate between a real or an artificial finger. The idea is protected by the patent US #6,292,576.

5.4 Infineon Technologies AG

http://www.infineon.com/fingertip

Infineon's FingerTIP, formerly known as Siemens Semiconductors, is a capacitive solid-state scanner that senses an image by measuring the distances between the sensor surface and the ridges/valleys which constitute the fingerprint.

It is interesting to note that this chip was fooled in [Matsumoto] and was easily fooled with the gelatin finger, but Matsumoto tested an evaluation kit, using the Software Development Kit in beta release (v0.90 Beta 3)

At the moment, this sensor is mounted in the Siemens ID Mouse, and is driven by a new software (Siemens ID device software release 5) that, according to the manufacturer claims, includes an "Improved fake protection" [Ligon 2002]. As happened to the SecuGen scanner, we can suppose that Infineon developed a software method which try to discriminate between a live and a gummy finger.

In January 2001 Infineon submitted a patent with title: "Method for detecting living human skin" (US #6,597,945) describing how to use a measure of the impedance of the skin to test the liveness of the finger. We do not know if they have tested this method with gummy fingers, and if they have plans to implement this technology in the FingerTIP sensor.

5.5 Testech

http://www.testech.co.kr

The TesTech "Bio-i" is an electro-optical fingerprint reader based on Light-Emitting polymer CMOS Sensor. The manufacturer claims: "*U.S patent TesTech LE Sensor Tech Guarantee Highest Security Disable Fake Finger Trials*" and they can "*Distinguishes live Finger from copied or any other forged fingerprints using U.S. Patented Contact Light Emitting Sensor*"

The technology behind this sensor is patented:

- US #6,326,644: "Contact light emitting device" which is a sensor that emits light when a finger (acting as a ground contact) touches it (December 4, 2001);
- US #20020054696: "Fingerprint recognizing device having patterned floating electrodes and fabricating method therefore" (patent pending);
- US #20020027605: "Fingerprint recognition sensor and manufacturing method thereof" (patent pending);
- US #20020018252: "Contact imaging system"(patent pending);

Since the patent was submitted before the test of Matsumoto, we do not know if it can reject a gummy finger.

5.6 Ethentica

http://www.securityfirstcorp.com

Ethentica, formerly known as WhoVision, is the Biometrics division within Security First Corp. They developed the Ethenticator USB 2500, an optical electro-optical scanner based on a Tactile-Sense technology that use a polymer based sensor.

The manufacturers claim their system is secure against fake replicas: "*By using your finger's electrical field, it senses a live finger, so it is not possible to use a replica of a fingerprint or a latent image left on the sensor, like optical or CMOS chip sensors*".

As they say in the description of their sensor [Ethentica 2002] it is sensitive to the conductivity of the finger, and it is possible to spoof it with a fake conductive finger [Matsumoto 2002].

5.7 AuthenTec

http://www.authentec.com

AuthenTec is a manufacturer of a family of solid-state electric field sensors. These sensors, and in particular the AES4000, with a resolution of 250dpi, are mounted on several commercial devices, like the Targus "Defcon" and the Precise Biometrix "100MC".

The manufacturer claims: "*TruePrint® technology sensors can capture images from beneath the surface of the skin where the ridge-and-valley pattern suffers less damage from day-to-day living*", and also "*TruePrint® Technology uses a patented radio frequency (RF) imaging technique that allows the sensor to generate an image of the shape of the live layer of the skin that is buried beneath the surface of the finger. This live subsurface layer has the shape of the fingerprint ridge and valley pattern, in fact it is the source of the fingerprint pattern, and it is rarely affected by damage or wear to the finger surface. It is this protected subsurface "true print" that TruePrint® technology captures in its images*" [Authentec].

The live subsurface has a better conductivity than the superficial skin, that act as a dielectric. The related patents are:

- US #6,259,804: "Fingerprint sensor with gain control features and associated methods";
- US #6,088,471: "Fingerprint sensor including an anisotropic dielectric coating and associated";

Some vendors (i.e. Targus and Precise Biometrics) stress on security of their systems, and also Intel released a paper describing the TruePrint technology in conjunction with the AES3400 (500dpi) as an effective anti-spoof method [Intel 2003]. But the Targus "Defcon" and the Precise "100MC" have been fooled by a gelatin fingerprint in a comparative study made at the Swedish University of Linköpings [Blommé 2003].

We believe that a better resolution (such as 500 dpi) does not change the result, and that the TruePrint technology can discriminate a live finger from a silicone one, but can do nothing against a gummy finger.

5.8 Additional manufacturers

Other companies are claiming to have a fake finger detection mechanisms:

- Optel: (http://www.optel.com.pl/article/english/livetest.htm) they are developing an Ultrasonic Fingerprint scanner.
- Cross Match: (http://www.crossmatch.com/industries_commercial.html) ID 1000 live scan, they speak about "Blood Flow".
- Lumidigm: (http://www.lumidigm.com/LumiSure.html) they are developing a LumiSure sensor that elaborates the light reflected from the skin to recognize a living finger.
- Sony: were claiming to have a fake detection, for their optical unit. Seems to have disappeared from their web site.
- Delsy: (http://www.delsy.de/english/2000/2200/22_02/index.html) just talking of having fake detection.
- Idex: (http://www.idex.no/x/Default.asp?page=TechWeb\livefinger\live%20finger.htm)
- ST Microelectronics: some patents using impedance.
- Tarian: is a company trying to recognize people using the blood pulse shape. Low information about them, they are trying to get funds.
- PosID & Hitachi: are trying to perform recognition using an infrared camera: (http://www.photonics.com/spectra/applications/XQ/ASP/aoaid.266/QX/read.htm)

6. FURTHER TESTS ON THE DEVELOPMENT OF FAKE FINGERPRINTS

This section discusses some experiences made by BioSec partners (UNIBO, BIOK and ATMEL) in creating fake fingerprints.

6.1 Casting a mold

We worked under the assumption of duplication with cooperation.

To cast a mold of a real finger we tried some different materials, available on the market:

- Wax;
- Bi-component Dental material usually used to cast a dental prosthesis;
- A modeling material (Green Stuff);
- A kind of stucco (Milliput);
- Room Temperature Vulcanizing Silicone (Prochima RTV 530);

Characteristics of the desirable mould are:

1. Time stability and durability;
2. Does not worn out when used;
3. High reproduction accuracy;
4. A forger does not have to apply a high pressure to leave a fingerprint.

A first attempt has been made using warm wax because it is suitable to be easily poured on a flat surface. The harder bit is wait for the temperature: not too hot to burn the finger, not too cold to not get the fingerprint details. A wax mold can be very thin (this is wax's advantage) and highly detailed, but it can be easily damaged by pouring some hot liquid on it: it lacks, then, the characteristic number 2.

Then we get a sample of a bi-component dental material (very expensive): the two component need to be mixed very quickly (the compounds sets in a few minutes) and accurately. As this material is really sticky, it is better to soap the finger before making the mold. The resulting mold is highly detailed and re-usable.

Looking for a material cheaper than the dental one, we found two bi-components used by figurine molders: the Green Stuff (€ 6,50) and the Milliput (€ 9,15). As they are very hard (you need to apply a high pressure with the finger to leave the fingerprint) the resulting fingerprint, once hardened, won't be flat enough to be use on the scanner surface. Moreover, the Milliput does not have a good reproduction accuracy.

Finally we used a dual-compound silicone available in modeling shops: the Prochima RTV 530 (€ 27,00 for 500g). This silicone vulcanizes at room temperature in 3 minutes and is skin compatible, since it is used in artistic reproduction of anatomical parts. This product is similar to the dental one for the mold quality, but cheaper and it is not adhesive and does not stick to the finger.

6.2 Casting a fake fingerprint

When the mold is ready we need to fill it to have a fingerprint. The right compound has to be liquid at the starting stage, and has to become more solid as time passes, up to a gummy consistency.

6.2.1 Liquid Silicone

Liquid silicone tends to be adhesive to the mold, it usually releases harmful solvents in the air, it requires a lot of time to vulcanize. The resulting fingerprint is very definite and elastic, but not conductive.

6.2.2 Natural Rubber Latex

The natural rubber latex is a white liquid, derived from the rubber tree. It is possible to find it in artistic shop at a low cost: 1 kg package for € 7,23. It is easy to pour it into the mold but it needs several hours to dry up. Latex is cheaper than silicone but the final result is not as good as the silicone one.

6.2.3 Gelatin

To repeat the experiments made by [Matsumoto] with a conductive fingerprint, we tried several gelatins:

- Animal derived gelatin (usually made from pigs) in powder and sheets;
- Pectine powder, a vegetal gelatin;
- Agar-agar, that is a dried alga with high gelling power.

Vegetal gelatin are not well suited for this job, because they tend to remain a bit coarse and do not get the ridge with the required accuracy.

Even the gelatin powder has to be discarded because it is more difficult to melt it in so little water as required by the experiment: we need to melt 1 g of gelatin in 1 ml of water. Usually gelatin can absorb up to 10 times its weight of water, and fine particles swell very fast in hot water, so that insufficient water is available for all the gelatin: this can lead to the formation of lumps that are difficult to dissolve.

Since we want to stir the gelatin and have control on the full process, we did not use a microwave oven, but we tried with a free flame. Given the low amount of water to heat up, we did not use a gas cooker, but we used a candle and a small aluminum saucepan. It takes from 3 to 4 minutes to melt 1 g of gelatin in 1 ml of water, and the resulting compound can be used for no more than one fingerprint.

At the end of the cooking process the compound is quite sticky and a small spatula is needed to spread a layer of melted gelatin on the mold. After 15 minutes the fake fingerprint is ready to use.

An important problem using gelatin is that it dehydrates very quickly so the fake is usable only for a couple of hours. After that it becomes too hard and the ridges are not viewable by the scanner. To solve this problem we added 0,2-0,3 ml of glycerol (also known as glycerin) to the final compound. The glycerol, available in pharmacies, is obtained from natural fats and used in cosmetics as a skin emollient. It is hygroscopic, so it retains the water released by gelatin dehydration. It can not be used in great quantity because it gets water from the air humidity and can moisturize the fingerprint too much.

Adding glycerol extends the fingerprint life up to 12 hours. If properly wrapped with cling film it can be used again after a week, and up to a month if kept it in the fridge.

When a gelatin fingerprint is too dry, it is possible to moisten it by breathing on its surface. This can trick even a conductive fingerprint scanner.

7. TEST OF EXISTENT FINGERPRINT SCANNERS

After developing a good fake fingerprints, we checked them against some fingerprint scanners. We selected the scanners (see **Table 7**) according to the two following criteria:

- Not tested in previous studies
- Including "aliveness detection" mechanism, that, according to the manufacturer, make them resistant to fake finger attacks.

Manufacturer	Product	Technology	Aliveness Detection
Guardware Systems	SystemGuard DT	Optical FTIR	Dielectric measure.
Digital Persona	U.areU. 4000 Pro	Optical FTIR	Software computation.
Ethentica	Ethenticator 2500	Optical Electro-optical	TactileSense technology.
Testech	Bio-i	Optical Electro-optical	Light Emitting Sensor .
AuthenTec	AES 4000	Solid-state Electric Field	TruePrint technology

Table 7: List of the tested fingerprint scanners.

To have a more complete test including all the available sensing technology, we also tested a classic capacitive scanner (the TouchChip of STMicroelectronics) and a thermal sweep sensor (the FingerChip of ATMEL).

7.1 SystemGuard DT (Guardware Systems)

The SystemGuard DT is the desktop version of the Guardware scanner. The package includes the software for enrollment and authentication. The acquisition image process is driven by a red light that illuminates the finger when the user touches the glass surface. If the finger is not recognized as a real finger, the light begins to flash: this is supposed to help the user to place correctly the finger on the sensor surface, but it is also a good feedback for a forger to hack the system.

There are two different security settings. The first one, common to all user, sets the security level of aliveness detection. There are four different levels: low, normal, high and extreme; when set at "extreme" level the scanner easily rejects even a real finger. At "high" level, often a user has to be very well trained before his fingerprint is recognized as a real one. If in the user group there is someone with an intrinsic bad quality or dry fingerprint, the system has to be configured at "normal" level, increasing the probability that the system accepts a fake finger. The second security level measure is the percentage of minutiae that the system needs to accept a finger. This level is variable in a range from zero to nine (where 0 is the lowest and 9 the highest) but manufacturers advise against setting it to a level lower than five. It is possible to set this security level differently from user to user and also finger from finger for the same user.

In our test we set aliveness detection security level to "high" and searched security level to "seven" for all users.

With this settings, to enroll a gelatin fingerprint is quite hard but possible with some practice (see **Figure 17.b**). If a non-conductive material is used, like silicone or latex, the fingerprint scanner rejects every attempt, because the aliveness test measures the dielectric constant of the finger.

Nevertheless, it is possible to use a latex or silicone fingerprint to enroll a new user and authenticate someone as someone else. The replica has to be glued to the real finger and moistened breathing on it and it must be smaller than the finger area, to let the real skin touch the scanner surface. In this way the aliveness detection system is deceived because the surrounding live skin touches the electrodes that perform dielectric measures, while the identification process is cheated by the latex core (see **Figure 17.c**)..

a) Real finger **b) Gelatin fingerprint** **c) Latex fingerprint**

Figure 17: Images acquired with the Guardware SystemGuard DT

Using a small patch of gelatin someone can try to be misidentified as another user, even if the patch is very small (see **Figure 18**). These images are clearly a fake for the human eye but they can fool the scanner, so it is also possible to deceive this scanner with a small fingerprint, like those obtained from a latent fingerprint.

a) Gelatin fingerprint **b) Partial gelatin fingerprint** **c) Partial gelatin fingerprint (smaller)**

Figure 18: Partial fake fingerprint glued on a real finger

7.2 U.are.U 4000 Pro (Digital Persona)

The U.are.U Pro is a slim optical scanner that includes a software for enrollment and authentication of new users. To enroll a new user both the index fingers are registered. During the enrollment phase each finger is acquired four times to reduce the error ratio during future authentications.

The sensor was easily spoofed by a fake finger made of gelatin, latex or silicone (see **Figure 19**): it has been possible to enroll a fake finger and then to authenticate with the real one and vice versa.

a) Real finger **b) Latex finger** **b) Gelatin finger**

Figure 19: Images acquired with the Digital Persona U.are.U Pro

7.3 Bio-i (Testech)

This fingerprint scanner is based on an electro-optical technology called “Light Emitting Sensor” that, according to Testech, can discriminate a live finger from a false or a dead one. The tested package does not contain a software to enroll and authenticate, so it is not possible to evaluate the performance of this fingerprint scanner in terms of accuracy.

The sensor does not accept silicone or latex fingers because these are not conductive materials but it is possible to acquire a fingerprint image by using a gelatin finger like the live one, in spite of the manufacturer statement. The image of a gelatin fingerprint is very similar to the real one (see **Figure 20**).

a) Real finger **b) Gelatin finger**

Figure 20: Images acquired with the TesTech Bio-i

7.4 Ethenticator 2500 (Ethentica)

This scanner is based on an electro-optical technology called TactileSense. The Manufacturer states that it is not possible to use a replica of a fingerprint for enrollment and verification . The package contains a software that realize enrollment and verification, a match one to one of a fingerprint. During the enrollment phase the scanner collects a series of consecutive acquisition to create an image of the finger.

Latex and silicone fingers are not recognized as live finger but it is possible to enroll and verify gelatin fingers (see **Figure 21**).

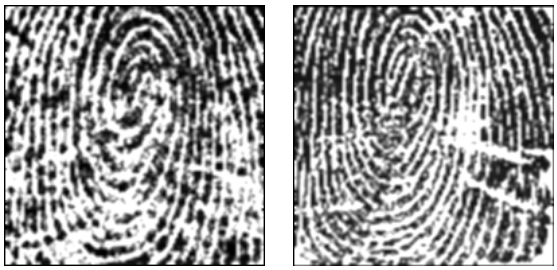
a) Real finger **b) Gelatin finger**

Figure 21: Images acquired with the Ethentica Ethenticator 2500

7.5 AES4000 (AuthenTec)

According the vendor's press releases, AuthenTec sold over two million of TruePrint technology based fingerprint sensors all over the world. TruePrint technology received important reviews from biometric magazines, the last one it has been a "2004 Disrupter Award", in Fast Company Magazine: "*for having successfully developed a viable biometrics technology that today offers consumers and businesses the convenience of a fingerprint security solution for minimum cost*".

The evaluation kit package includes a software to enroll and identify users. To enroll a new user it is necessary to insert a name, select the finger one wants to enroll and acquire the selected finger three times. After the enrolling, the user can be identified simply placing his registered finger on the scanner surface. There is a parameter that allows to set the security level of aliveness detection methods; by default this parameter is not enabled, we enabled it for our tests. This sensor rejects latex or silicone fingers, because these material are not conductive, and it is impossible to visualize a silicone finger. It is possible to fool the scanner using gelatin, whose conductivity is similar to human skin. With a gelatin finger the image was acquired and it has been possible to enroll a new user or to impersonate a registered user (see **Figure 21**).



a) Real finger **b) Gelatin finger**

Figure 21: Images acquired with the AuthenTec AES4000

7.6 TouchChip (ST Microelectronics)

This scanner is based on capacitive sensor technology that allows to reject all the fake fingers made of non-conductive materials, for example silicone or latex. Using gelatin is possible to spoof this sensors, because its conductivity is similar to human skin, so the scanner acquires the fake finger.

The tested package includes a software that acquires the fingerprint image but does not provide enroll and authentication. The images acquired from a real and a fake finger (see **Figure 22**) shows that the results are very similar, so we can suppose that an acquisition software cannot sense a fake finger from the real one.

a) Real finger **b) Gelatin finger**

Figure 22: Images acquired with the STMicroelectronics TouchChip

7.7 FingerChip

FingerChip is a very little scanner based on a sweeping thermal sensor, whose matrix have few rows of pixels. When the user sweeps his finger on the sensor surface, the image is acquired slice by slice and then reconstructed. The tested package does not include a software for enrollment or authentication, so it is not possible to evaluate the performance of this sensor with fake fingers.

Referring to traditional sensors in this case it is harder to use a fake finger because it is not easy to move correctly the fake finger along the sensor surface. Anyway, using silicone, latex or gelatin the image can be acquired; However obtaining a good quality image requires some practice. The images acquired by the ATMEL sweeping sensor, with a real finger and a fake as well, look very similar (see **Figure 23**).

a) Real finger **b) Gelatin finger**

Figure 23: Images acquired with the ATMEL FingerChip

8. CONCLUSIONS

This study focuses on aliveness detection mechanisms against fake fingerprint attacks. From the critical review of the related bibliography and from the experiences we did by creating new fake fingerprints and using them to spoof existing fingerprint scanners we can conclude that:

- to forge a fake finger is not so easy as some authors claim, even when the person whose finger has to be cloned is cooperative. It is necessary to find the right materials to mold and cast, learn the right process and handle the artificial finger created with care. Duplicating a key, observing or guessing a simple password is definitely simpler.

- if the fingerprint owner is non cooperative, to create a fake fingerprint from a latent one is significantly more difficult, unless you are a forensic expert with the appropriate instrumentation.

- at the best of our knowledge and from the experience gained testing several recent scanners including aliveness detection mechanisms (see sections 6 and 7), nowadays none of the commercial fingerprint scanner is really resistant to fake fingerprints.

- some of the measures proposed to perform aliveness detection methods, require sampling a biomedical feature (blood pressure, electrocardiography, etc) that may reveal an illness of the subject. There are legal and privacy issues related to the collection of these personal data, that can be an obstacle to the use of such methods in aliveness detection.

- the lack of satisfactory solutions to reject fake fingerprints, shows that there are a lot of challenges in aliveness detection and the commercial products that claim to have solved the problem are far from perfect. This justifies BioSec work on fingerprint aliveness detection methods very nicely.

- depending on the application, fake finger detection may not always be a requirement. Certain implementations of a fingerprint based biometric system and/or of related management procedures (e.g., storing the template in a smart card owned by the user, supervising the authentications attempts, using multi-biometrics) provide effective alternatives to combat fake finger attacks.

9. BIBLIOGRAPHY

[Authentec] Authentec Inc. “Why TruePrint technology”. (http://www.authentec.com/finalInteg/WhyTruePrint.htm)

[Bernier 2000] U. R. Bernier, D. L. Kline, D. R. Barnard, C. E. Schreck and R. A. Yost, “Analysis of Human Skin Emanation by Gas Chromatography/Mass Spectrometry. 2. Identification of Volatile Compounds That Are Candidate Attractants for the Yellow Fever Mosquito (*Aedes aegypti*)” Analytical Chemistry, vol. 72, No. 4, pp. 747-756, 2000.

[Blommé 2003] J. Blommé, “Evaluation of biometric security systems against artificial fingers”. (http://www.ep.liu.se/exjobb/isy/2003/3514/exjobb.pdf)

[Cappelli 2001] R. Cappelli, D. Maio and D. Maltoni, “Modelling Plastic Distortion in Fingerprint Images”, in proceedings on International Conference on Advances in Pattern Recognition (2nd), pp. 369-376, 2001.

[Dan 2002] “Digital Persona U.areU. Personal Fingerprint Scanner” July 2002. (http://www.dansdata.com/uareu.htm)

[Ethentica 2002] Security First Corp. “Tactile Sense White Paper: a Breakthrough in fingerprint Authentication”, June 2002. (http://www.securityfirstcorp.com/tactwhtpr.pdf)

[Freeman 1907] R. A. Freeman, "The Red Thumb Mark", 1907.

[Guardware 2003] Guardware Systems Ltd. “SystemsGuard DT: Logical Access Control”,2003 (http://www.guardwaresystems.com/images/SystemsGuard_DT.pdf)

[Intel 2003] Intel Corp. “Biometric User Authentication: Fingerprint Sensor Product Evaluation Summary”, November 2003. (http://www.intel.com/design/mobile/platform/downloads/FingerprintDeviceProductEvaluationSummary.pdf)

[Kàkona 2001] M. Kàkona, “Biometrics: yes or no?” (http://home.i.cz/kakl/biometrics/Biometricsyesorno.htm)

[Kang 2003] H. Kang, B. Lee, H. Kim, D. Shin and J. Kim, “A Study on Performance Evaluation of the Liveness Detection for Various Fingerprint Sensor Modules”. (http://www.springerlink.com/media/fl9xa52kwm4xyj8xcd4p/Contributions/0/N/9/X/0N9XYEH420D733BL.pdf)

[Lee 2001] H. C. Lee and R. E. Gaenslen, “Advances in Fingerprint Technology, Second Edition” , June 2001.

[Ligon 2002] A. Ligon “An Investigation Into the Vulnerability of the Siemens ID Mouse Professional Version 4”, September 2002. (http://www.bromba.com/tdidd50e.htm)

[Maltoni 2002] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, "Handbook of Fingerprint Recognition", 2002.

[Matsumoto 2002] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," Proceedings of SPIE Vol. #4677, *Optical Security and Counterfeit Deterrence Techniques IV*, 2002.
(http://cryptome.org/gummy.htm)

[Schuckers 2003] S. T. V. Parthasaradhi, R. Derakshani, L. A. Hornak, S. Schuckers, "Time Series Detection of Perspiration as a Liveness Testing in Fingerprint Devices", submitted to: *IEEE Systems Man, and Cybernetics Society, Part C: Application and Reviews*, 2003.

[SecuGen 2002] Secugen Corp. "SecuGen announces new technology to detect spoofing of fingerprint biometric systems", press release May 2002.
(http://www.secugen.com/company/pr/20020530detection.htm)

[Thalheim 2002] L. Thalheim, J. Krissler, P. M. Ziegler, "Body Check: Biometric Access Protection Devices and their Programs Put to the Test" .
(http://www.heise.de/ct/english/02/11/114/**)**

[Testech 2003] Testech. "Bio-i Net Access"
(http://www.testech.co.kr/user/english/img/product/images/netaccess.zip)

[van der Putte 2000] T. van der Putte, J. Keuning, "Biometrical Fingerprint Recognition Don't Get Your Fingers Burned" proceedings of: IFIP TC8/WG8.8 *Fourth Working Conference on Smart Card Research and Advanced Applications*, pages 289-303, Kluwer Academic Publishers, 2000.
(http://cryptome.org/fake-prints.htm)