Impact of Artificial "Gummy" Fingers on Fingerprint Systems

Tsutomu Matsumoto
Hiroyuki Matsumoto
Koji Yamada
Satoshi Hoshino

Graduate School of Environment and Information Sciences
Yokohama National University
79-7 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan
email: tsutomu@mlab.jks.ynu.ac.jp

ABSTRACT

Potential threats caused by something like real fingers, which are called fake or artificial fingers, should be crucial for authentication based on fingerprint systems. Security evaluation against attacks using such artificial fingers has been rarely disclosed. Only in patent literature, measures, such as "live and well" detection, against fake fingers have been proposed. However, the providers of fingerprint systems usually do not mention whether or not these measures are actually implmented in emerging fingerprint systems for PCs or smart cards or portable terminals, which are expected to enhance the grade of personal authentication necessary for digital transactions. As researchers who are pursuing secure systems, we would like to discuss attacks using artificial fingers and conduct experimental research to clarify the reality. This paper reports that gummy fingers, namely artificial fingers that are easily made of cheap and readily available gelatin, were accepted by extremely high rates by particular fingerprint devices with optical or capacitive sensors. We have used the molds, which we made by pressing our live fingers against them or by processing fingerprint images from prints on glass surfaces, etc. We describe how to make the molds, and then show that the gummy fingers, which are made with these molds, can fool the fingerprint devices.

Keywords: biometrics, fingerprint, live and well detection, artificial finger, fingerprint image.

1. INTRODUCTION

Biometrics is utilized in individual authentication techniques which identify individuals, i.e., living bodies by checking physiological or behavioral characteristics, such as fingerprints, voice, dynamic signatures, etc. Biometric systems are said to be convenient because they need neither something to memorize such as passwords or something to carry about such as ID cards. In spite of that, a user of biometric systems would get into a dangerous situation when her/his biometric data are abused. That is to say, the user cannot frequently replace or change her/his biometric data to prevent the abuse because of limits of biometric data intrinsic to her/himself. Therefore, biometric systems must protect the electronic information for biometrics against abuse, and also prevent fake biometrics.

We have focused on fingerprint systems since they have become widespread as authentication terminals for PCs or smart cards or portable terminals. Some of fingerprint systems may positively utilize artificial fingers as substitutes in order to solve the problem that a legitimate user cannot access, for example, when s/he gets injured on her/his fingertip in an accident.[12] Some other cases include dry fingers, worn fingers, and other fingers with a low-quality fingerprint. However, the users of those systems would run a risk because artificial fingers can be stolen and used by other persons if the systems are utilized for a security application. Except for the above-mentioned cases, fingerprint systems generally must reject artificial fingers. In order to reject them, fingerprint systems should take measures to examine some other features intrinsic to live fingers than those of fingerprints. These measures are called "live and well detection [9, 15, 20, 23, 26]" and have been proposed mainly in patent literature.[13] Although a number of fingerprint systems have come into wide use, it is not clear whether or not these measures are actually implemented in commercial fingerprint systems. Moreover, as far as we know, security evaluation against attacks using fake fingers has been rarely disclosed. In connection, some researchers reported, in 1998, that four of the six fingerprint systems with optical devices accepted silicone fingers.[19] After that, some measures against silicone fingers may have been taken in fingerprint systems. But, someone might object that fingerprint systems with capacitive devices can prevent fake fingers, so they are secure.

Previous to our experiments described in this paper, we made silicone fingers, and then checked fingerprint systems with them. From the results, we ascertained that all the systems with a capacitive sensor and some systems with an optical sensor could reject the silicone fingers. Also, we confirmed that an inked fingerprint on a paper could be accepted by one of fingerprint systems. A series of our preliminary experiments brought up a question whether or not "live and well" functions are actually implemented in commercial fingerprint systems. Finally, we have carried out experiments with artificial fingers to inquire into the fact.[9,16,27-29] In this paper we discuss security evaluation of fingerprint systems, especially for its resistance against artificial fingers. Here, the term "fake fingers" may be widely used to refer fingers which are used to deceive fingerprint systems. However, we use the term "artificial fingers" to refer fingers which are artificially produced because "fake fingers" may include fingers which are modified from live fingers. In addition, we use the term "live fingers" to mean fingers which are part of living bodies.

2. FINGERPRINT SYSTEMS

2.1 Fingerprint Systems

The principle of fingerprint systems is schematically illustrated in **Fig. 2.1**. In an enrollment process, the system captures finger data from an enrollee with sensing devices, extracts features from the *finger data*, and then record them as template with a personal information, e.g. a personal identification number (PIN), of the enrollee into a database. We are using the word "*finger data*" to mean not only features of the fingerprint but also other features of the finger, such as "live and well" features. In an identification (or verification) process, the system captures *finger data* from a finger with sensing devices, extracts features, identifies (or verifies) the features by comparing with templates in the database, and then outputs a result as "Acceptance" only when the features correspond to one of the templates.

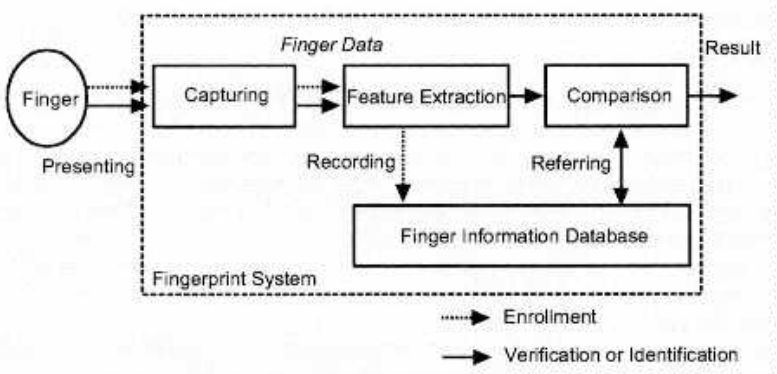


Figure 2.1 Typical structure of a fingerprint system

Most of fingerprint systems utilize optical or capacitive sensors for capturing fingerprints.[3, 10, 14, 22] These sensors detect difference between ridges and valleys of fingerprints. Optical sensors detect difference in reflection. Capacitive sensors, by contrast, detect difference in capacitance. Some systems utilize other types of sensors, such as thermal sensors, ultrasound sensors.[6, 15, 24] In this paper we examine fingerprint systems which utilize optical or capacitive sensors.

2.2 A Risk Analysis for Fingerprint Systems

Generally, fingerprint systems capture images of fingerprints, extract features from the images, encrypt the features, transmit them on communication lines, and then store them as templates into their database. Some systems encrypt templates with a secure cryptographic scheme and manage not whole original images but compressed images. Therefore, it is said to be difficult to reproduce valid fingerprints by using the templates. Some systems are secured against a so-called replay attack in which an attacker copies a data stream from a fingerprint scanner to a server and later replays it, with an one time protocol or a random challenge response device. We are here not concerned with the security for the communication and database of fingerprint systems, assuming that they are secure enough by being protected with some encryption schemes. In this section, we would like to address security of fingerprint scanners.

When a legitimate user has registered her/his live finger with a fingerprint system, there would be several ways to deceive the system. In order to deceive the fingerprint system, an attacker may present the following things to its fingerprint scanner.

(1) ***The registered finger:*** The highest risk is being forced to press the live finger against the scanner by an armed criminal, or under duress. Another risk is being compelled the legitimate user to fall asleep with a sleeping drug, in order to make free use of her/his live finger. There are some deterrent techniques against these crimes. Combination with another authentication method, such as by PINs, passwords, or ID cards, would be helpful to deter the crimes.[20] Furthermore, a duress control enables the users to alarm "as under duress" with a secret code or manner, which is different with a PIN or usual manner respectively. Combining a duress control with a fingerprint system would provide a helpful measure to apply to someone for protection. Similarly, a two persons control, namely a two persons rule, where the authentication process requires two persons properties, i.e., fingerprints, or would be helpful to deter the crimes.

(2) ***An unregistered finger (an imposter's finger):*** An attack against authentication systems by an imposter with his own biometrics is referred to as non-effort forgery.[26] Commonly, accuracy of authentication of fingerprint systems are evaluated by the false rejection rate (FRR) and the false acceptance rate (FAR).[1, 2] The FAR is important indicator for the security against such a method as with an unregistered finger. Moreover, fingerprints are usually categorized as "loops," "whorls," "arches," and others. If an attacker knows what category of the registered finger is, an unregistered finger of which pattern is similar to the registered one would be presented to the scanner. In this case, the probability of the acceptance may be different from the ordinary FAR. From this point of view, the accuracy of authentication for the system should be evaluated not only, as usual, for fingers throughout the categories of fingerprints but also for fingers within each category. Another attacker may modify his fingerprint by painting, cutting, or injuring his own fingertip. However, it is thought to be very difficult to deceive the fingerprint

system with such a modified finger. The reason for this is that fingerprints are so random the attacker cannot identify which patterns should be modified. Ordinarily, ten-odd features, such as ridge's and valley's distinctive patterns are used for the authentication.

(3) ***A severed fingertip from the registered finger:*** A horrible attack may be performed with the finger which is severed from the legitimate user's hand. Even if the finger severed from the user's half-decomposed corpse, the attacker may use, for the wrong purpose, a scientific crime detection technique to clarify its fingerprint.[6] In the same way as the above-mentioned registered finger, combination with another authentication method, or a duress/two-persons control would be helpful to deter these crimes. The detection whether the finger is alive or not would be helpful as well.

(4) ***A genetic clone of the registered finger:*** In general, it is said that identical twins do not have the same fingerprint, and neither would clones. The reason is that fingerprints are not entirely genetically determined, and rather determined in part by its pattern of nerve growth into the skin. As a result, this is not exactly the same even in identical twins. However, it is also said that fingerprints are different in identical twins, but only slightly different. If the genetic clone's fingerprint is similar to the registered finger's, an attacker may try to deceive fingerprint systems by using it. Now is the time when we must keep a close watch on such possibility with genetic engineering,

(5) ***An artificial clone of the registered finger:*** More casual attacks against fingerprint systems may use an artificial finger. An artificial finger can be produced as a printed fingerprint with a copier or a desk top publishing (DTP) technique as well as forged documents. If an attacker can make a mold of the registered finger directly modeling it, s/he can produce an artificial finger with some materials. Even if not, s/he may make a mold of the registered finger modeling its residual fingerprint at second hand, so as to produce an artificial finger. And, if an attacker can make an artificial finger which can deceive a fingerprint system, one of countermeasures against the attack obviously is the detection whether or not the finger is alive. Again, combination with another authentication method, or two-persons control would be also helpful to deter the crimes.

(6) ***The others:*** In some fingerprint systems, an error in authentication may be caused by making noise or flashing a light against the fingerprint scanner, or by heating up, cooling down, humidifying, impacting on, or vibrating the scanner outside its environmental tolerances. Some attackers may use the error to deceive the system. This method is well-known as a "fault based attack," and may be carried out with above-mentioned attacks. Furthermore, a fingerprint image may be stood out in strong relief against the scanner surface, if we spray some materials on the surface. The image would be the residual fingerprint of a registered finger. In this case, a bald thing or finger, regardless of alive or not, which are pressed on the surface, may be accepted by the fingerprint system.

As fingerprint systems come into wide use, they are still more exposed themselves to a risk of casual attacks. Apart from duress or other crimes, our great concern, in this paper, is the possibilities of attacks with artificial fingers.

2.3 Dishonest Acts with Artiflcial Fingers

In this section, on the assumption that artificial fingers can be accepted by fingerprint systems, we discuss dishonest acts against the system with the artificial fingers. Several patterns of dishonest acts, with artificial fingers, in a fingerprint system are shown in **Table 2.1**. In this table, L(X) and L(Y) denote live fingers of persons X and Y respectively. A(X) and A(Y) denote artificial fingers which are molded after L(X) and L(Y) respectively. A(Z) denotes artificial fingers which are created artificially without being molded after live fingers. There may be at the total of 25 possible combinations because we can enroll and verify each of L(X), L(Y), A(X), A(Y) and A(Z) in the system. However, we show 15 in 25 combinations and focus on 5 combinations, from (1) to (5), in the table on the following assumptions;

Table 2.1 Several patterns of dishonest acts with artifical fingers in a fingerprint system

	Verification / Identification				
Enrollment	**L(X)**	**A(X)**	**L(Y)**	**A(Y)**	**A(Z)**
L(X)	(1)	(2)	- *	-	-
A(Y)	-	-	(3)	(4)	-
A(Z)	-	-	-	-	(5)

- Only X can enroll fingers in the system,
- but X cannot enroll Y's live finger L(Y),
- the fingers must be enrolled with a genuine X's PIN,

- and X can obtain and enroll A(Y) and A(Z) in the system.

The case (1) is the proper way in the system. The case (2) or (5) is also the proper way in some systems which positively utilize artificial fingers. However, we discuss dishonest acts of artificial fingers regarding the cases from (2) to (5) as dishonest ways. The possible dishonest acts are:

- Some other persons than X can pretend, in the system, to be X by presenting artificial fingers in all the cases of (2), (4) and (5), and
- Y can pretend, in the system, to be X by presenting her/his own fingers L(Y) in the case (3).

In addition, X can deny the participation showing by means of evidence that her/his own live fingers cannot be accepted by the system, when the dishonest act was detected in the cases (3), (4) and (5).

Most discussion on dishonest acts with artificial fingers have mainly focused on the case (2). However, it should be noted that the dishonest acts, which correspond to the cases (4) and (5), can be done if artificial fingers are accepted by the system. The cases (3), (4) and (5) can be probably prevented by a practical measure that enrollment is closely watched to prevent using artificial fingers. Moreover, dishonest acts which correspond to the cases, from (2) to (5), never occur if the system can successfully reject artificial fingers.

Accuracy of authentication of fingerprint systems are commonly evaluated by the false rejection rate (FRR) and the false acceptance rate (FAR).[1, 2] In Table 2.1, the case (1) and the case indicated by the sign '*' correspond to those which are commonly evaluated by the FRR and FAR in its ordinary performance test for live finger samples, respectively. It is important that the acceptance rate for the cases from (2) to (5) should be evaluated if the system cannot perfectly reject artificial fingers.

3. EXPERIMENTS

3.1 How to make Artificial Fingers

There are several major ways to make an artificial finger of a given live finger, as shown in **Fig. 3.1**. First of all, an impression must be obtained from the live finger. The fingerprint image of the impression is mostly the lateral reversal, i.e., transposed from left to right as in a mirror reflection, of the original. This impression may be used as an artificial finger to deceive the system, if an attacker can make an impression without being lateral reversal. However, most of the impressions have a lateral reversal fingerprint image. When a live finger was pressed on an impression material, a fingerprint image on the impression may be used as a mold of an artificial finger. If an impression was captured with a digital camera as an electronic fingerprint image, it may be set right side left by an image processing software, and then printed on a material to make an artificial finger. This electronic fingerprint image also can be used to make a mold, as it is. The impression may be a residual or inked fingerprint. Even if the fingerprint image is latent, some techniques for scientific crime detection can enhance it with some material, e.g. aluminum powder, a ninhydrin solution, a cyanoacrylate adhesive,[6, 18] then producing the artificial finger with them. Besides these, we can, without original live fingers, create an artificial finger with a fictitious fingerprint, such as, using a so-called fingerprint generator.

In our experiments, we make artificial fingers by the following two ways, which are; (1) we make an impression directly pressing a live finger to plastic material, and then mold an artificial finger with it, and (2) we wapture an fingerprint image from a residual fingerprint with a digital microscope, and then make a mold to produce an artificial finger. The material for artificial fingers is gelatin which is obtained from bone, skin, etc., of animals. In this paper we are using the word "*gummy*" to refer not a sol but a gel of gelatinous materials. Accordingly, we use the terms "*gummy*" fingers to refer artificial fingers which are made of gelatin, since its toughness are nearly equal to gummies which are one kind of sweets, and also made of gelatin with some additives such as sugar and/or fruit juice. Here, the origin of the word "*gummy*" is "gummi" in the German language. **APPENDIX A** details the processes for making artificial fingers.

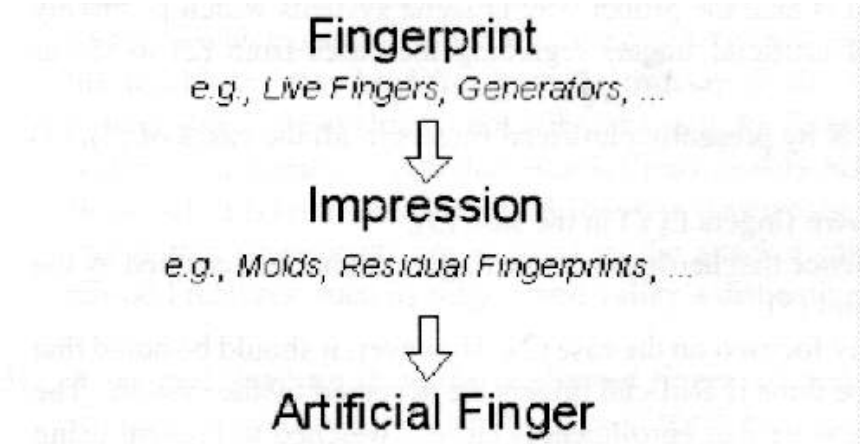


Figure 3.1 How to map a fingerprint onto artificial fingers.

Fingerprint Table 3.1 Types of Experiments.

Experiment	Enrollment	Verification
Type 1	Live Finger	Live Finger
Type 2	Live Finger	Gummy Finger
Type 3	Gummy Finger	Live Finger
Type 4	Gummy Finger	Gummy Finger

e.g., Live Fingers, Generators,

Experiment Enrollment Verification

Impression Type 1 Live Finger Live Finger

e c7., Moids, Pesiduaf F'Oluerprints, Type 2 Live Finger Gummy Finger

Type 3 Gummy Finger Live Finger

ID Type 4 iGummy Finger Gummy Finger

Artificial Finger

Figure 3.1 How to map a fingerprint onto artificial fingers.

3.2 Experimental Procedures

The goal of experiments which we conducted is to examine whether fingerprint systems, which are commercially available, accept the artificial fingers or not. Accordingly, we examined the acceptance rates of fingerprint systems by using the artificial fingers, i.e.. *gummy* fingers, and live fingers. The following describes procedures of the experiments.

(1) ***Types of artificial fingers:*** Two types of artificial fingers were examined. One is produced by cloning with a plastic mold. The other is produced by cloning from a residual fingerprint. These are detailed in APPENDIX A.

(2) ***Types of experiments:*** Four types of experiments (shown in Table 3.1) were conducted. Difference in the types are follows:

Type 1: A subject presents her/his live finger to verify with a template which was made by enrolling the live finger.

Type 2: A subject presents her/his live finger to verify with a template which was made by enrolling her/his live finger.

Type 3: A subject presents her/his live ringer to verify with a template which was made by enrolling her/his *gummy* finger.

Type 4: A subject presents her/his *gummy* finger to verify with a template which was rnade by enrolling the artificial finger.

(3) ***Rules in experiments:*** We conducted the experiments under the extra rules as follows:

[1] We allowed a tester as deputy for the subject to present or enroll the subject's artificial finger.

[2] In Type 4 experiment, we also allowed that an artificial finger which is presented is not always the same as one which was used in enrollment.

[3] The subject or tester must intentionally present the live/*gummy* finger to fit the center of it to that of a scanning area of the fingerprint devise.

[4] The *gummy* fingers can be modified their shape to fit the scanning area.

(4) ***The acceptance rates:*** Only one live/*gummy* finger must be enrolled as a template while we allowed to retry in enrollment. We attempted one-to-one verification 100 times in each type of experiment for each fingerprint system counting the number of times that it accepts a finger presented. As a result, we measured the acceptance rates in verification for the fingerprint systems.

(5) ***Subjects:*** The subjects are five persons whose ages are from 20's to 40's, in the experiment for the *gummy* fingers cloned with a plastic mold, whereas the subject is only one person in the experiment for the *gummy* fingers cloned from a residual fingerprint.

(6) ***Artificial Fingers:*** *Gummy* fingers of each subject were made in the two ways which we explained in APPENDIX A and used in the experiments.

(7) ***Fingerprint systems:*** We tested 11 types of fingerprint systems which are shown in **APPENDIX B.1**. Each of them consists of a finger device and a software for verification. We set a threshold value for the highest security level if the fingerprint system allows to adjust or select threshold values in verification. All of fingerprint devices can be connected with a personal computer (PC), and used for access control. The procedures for fingerprint systems are detailed in **APPENDIX B.2**.

4. EXPERIMENTAL RESULTS AND DISCUSSIONS

4.1 Cloning with a Plastic Mold

4.1.1 Artificial Fingers

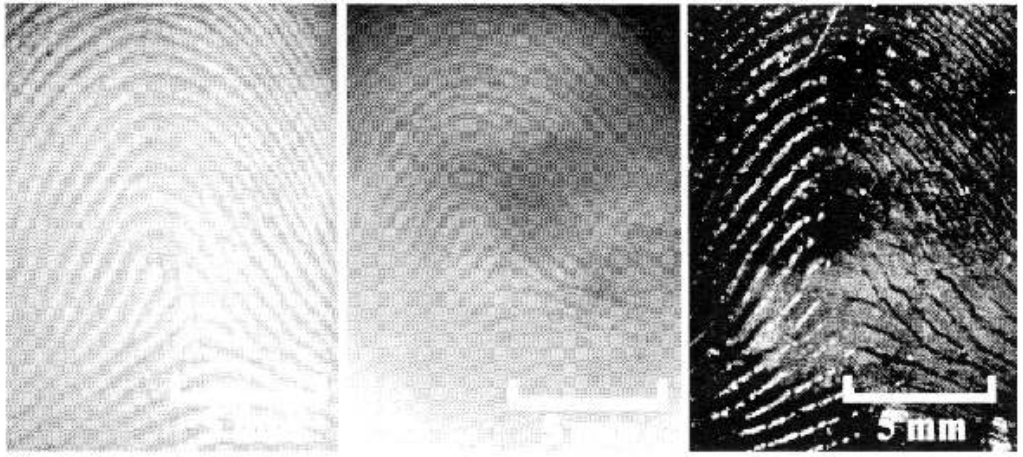


Figure 4.1 The photomicrographs of a live finger and its artificial fingers.

Figure 4.1 shows photomicrographs of a live finger and its artificial fingers. The *gummy* finger which is cloned by using a plastic mold with an impression of the live finger. The molded *gummy* fingers are rather transparent and amber while having ridges and valleys similar to those of the live finger, in terms of the outside appearance. Fingerprint images of a live finger, a silicone finger and a *gummy* finger, which were displayed by the system with Device C (equipped with an optical scanner), are shown in **Fig. 4.2**. Here, the silicone finger is the artificial finger made of silicone rubber, and presented so as to compare with the others. The captured image of the *gummy* finger in **Fig. 4.2** is very similar to that of the live fingerprint images of a live finger and a *gummy* finger, which were displayed by the system with Device H (equipped with a capacitive sensor), are shown in **Fig. 4.3**. While some defects are observed in the image (right side) of a gummy finger, both of the images are similar to each other. Here, the reason why we do not present the image of a silicone finger is that it cannot be accepted by the system with Device H.

(a) Live Finger (b) Silicone Finger (c) Gummy Finger

Figure 4.2 Fingerprint images of a live finger, a silicone finger and a *gummy* finger, which were displayed by the system with Device C (equipped with an optical scanner).

(a) Live Finger (b) Gummy Finger

Figure 4.3 The sample images of fingers which derive from the same finger and were displayed on the screen when being scanned by the capacitive sensor of Device H.

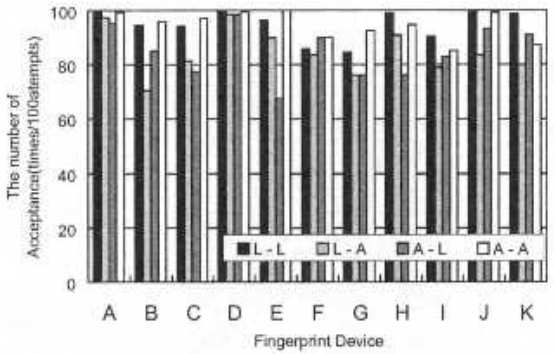


Figure 4.4 Average number of acceptance for each device, in terms of *gummy* fingers which were cloned with plastic molds. Here, the number of the subjects is five.

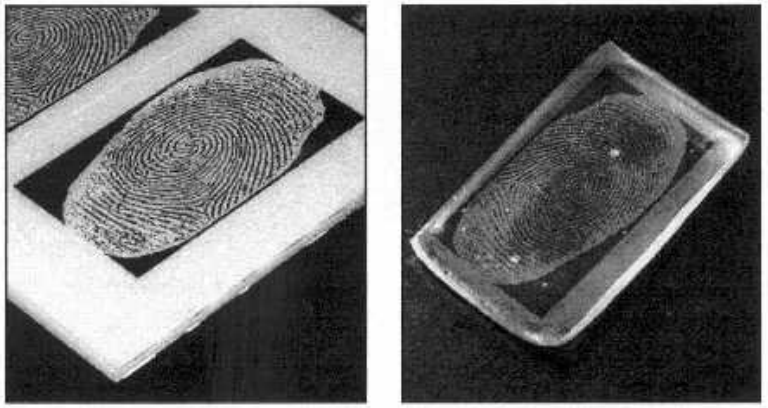
4.1.2 Acceptance Rates of the Artificial Fingers

The results of the experiments for the artificial fingers, which were cloned with molds, are shown in **Fig 4.4**. It was found through the experiments that we could enroll the *gummy* fingers in all of the 11 types of fingerprint systems. It was also found that all of the fingerprint systems accepted the *gummy* fingers in their verification procedures with the probability of 68-100%.

4.2 Cloning from a Residual Fingerprint

4.2.1 Artificial Fingers

Figure 4.5 (a) shows the outside appearance of the mold which we used in our experiments. **Figure 4.5** (b) shows a photograph of the gummy finger which was produced from a residual fingerprint on a glass plate, enhancing it with a cyanoacrylate adhesive. We applied a technique for processing printed circuit boards to the production of the molds for cloning the gummy fingers. The fingerprint image of the *gummy* finger, which was displayed by the system with Device H (equipped with a capacitive sensor), is shown in **Fig. 4.6**.



(a) The mold for gummy fingers (b) Gummy finger

Figure 4.5 Photographs of the outside appearance of the mold and a *gummy* finger. The *gummy* finger was produced from a residual fingerprint on a glass plate, enhancing it with a cyanoacrylate adhesive

Figure 4.6 The Fingerprint image of the *gummy* finger, which was displayed by the system with Device H (equipped with a capacitive sensor).

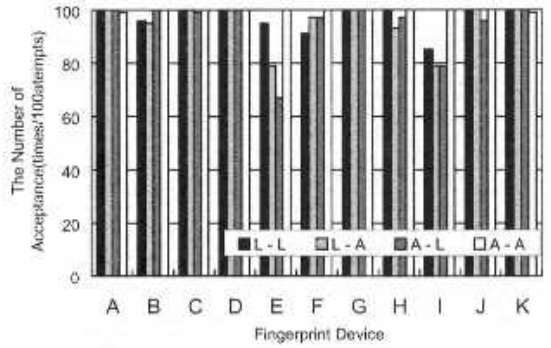


Figure 4.7 Average number of acceptance for each device, in terms of *gummy* fingers which were cloned from residual fingerprints. Here, the subject is one person.

4.2.2. Acceptance Rates of the Artificial Fingers

The results of the experiments for an artificial finger, which was cloned from a residual fingerprint, are shown in **Fig. 4.7**. As a result, we could enroll the *gummy* finger in all of the 11 types of fingerprint systems. It was found that all of the fingerprint systems accepted the **gummy** finger in their verification procedures with the probability of more than 67%.

4.3 Discussions

The number of samples in the experiments is so small that we cannot compare performance of the fingerprint systems. However, the number of samples is enough for us to see evidence that the *gummy* fingers could be accepted by commercial fingerprint systems. Based on our analysis, these variations may be caused by deformation of *gummy* fingers. We found that some of artificial fingers were damaged while being heated by the fingerprint sensors in the experiments. Some of the sensors frequently heated up when repeating verification in a short period. We think that the number of acceptance will increase if we pause for cooling every time after verification. We mentioned, in section 3.2, that the *gummy* fingers can be modified their shape to fit the scanning area. Accordingly, we cut the *gummy* fingers to fit the sensing area for some devices. This might cause decrease of errors in positioning the *gummy* fingers. Another reason why the number of acceptance varies is that we allowed retrying in enrollment. Finally, all of *gummy* fingers could be enrolled in the end in our experiments, even if the systems employ some protection. Also, the number of acceptance of live fingers is greater than that of *gummy* fingers for some systems that may employ so-called live and well detection.

We have investigated the difference in characteristics of live, *gummy* and silicone fingers. While silicone fingers were impossible to measure, the moisture and electric resistance of the gummy fingers could be measured as shown in **Table 4.1**. We used a moisture meter, and a digital multimeter (range: from 0 to 40 Mohms). According to this comparison, *gummy* fingers are more similar to live fingers in their characteristics than silicone fingers. The compliance was also examined for live and *gummy* fingers as shown in **Fig. 4.8**. Here, the compliance indicated by the change in resonance frequency (i.e., tactile sensor output) as the function of the pressure (i.e., pressure sensor output). In brief, Fig. 4.8 shows that the live finger is softer than the *gummy* finger. We found that these fingers are clearly different in compliance.[8]

Table 4.1 Characteristics of fingers

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

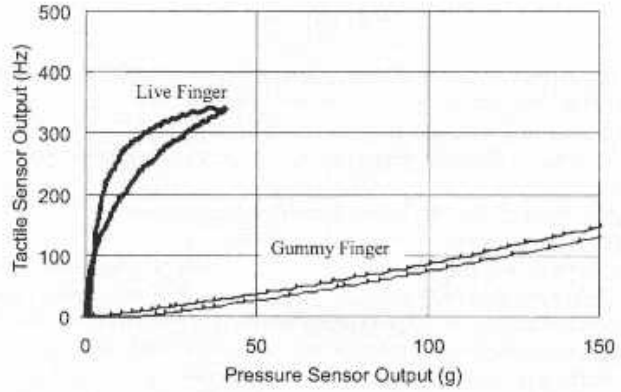


Figure 4.8 The compliance was also examined for live and *gummy* fingers.

If "live and well" detectors can clearly distinguish their moisture, electric resistance, transparency or bubble content (i.e., bubble rich material or not) between live fingers and *gummy* fingers, fingerprint systems can reject *gummy* fingers. Also, detection of compliance would be helpful for preventing *gummy* fingers. Furthermore, some of measures which have been proposed in patent literature may be useful in preventing *gummy* fingers.

5. CONCLUSIONS

In this paper, we illustrated a risk analysis for fingerprint systems. The risk analysis revealed that there are many attack ways to deceive the systems, even if their templates and communication are protected by a secure measure. Conventional arguments tend to focus on a question how to detect use of artificial fingers, which derive from live fingers of legitimate users. However, as we pointed out, there can be various dishonest acts using artificial fingers against the systems. We also pointed out that artificial fingers can be made not only of silicone but also of gelatin, and examined 11 types of fingerprint systems whether or not they accept the *gummy* fingers. Consequently, all of these systems accepted the *gummy* fingers all in their enrollment procedures and also with the rather higher probability in theirverification procedures. The results are enough for us to see evidence that artificial fingers can be accepted by commercial fingerprint systems. The objection will no doubt be raised that it is very difficult to take an impression of the live finger from a legitimate user without the cooperation of her/him. Therefore, we demonstrated that the *gummy* fingers made from residual fingerprints can be accepted by all of the 11 systems.

After we started this study, we come to know by the published book, that Dutch researchers reported that an artificial finger, which was made of silicone rubber, putting saliva on its surface can be accepted by fingerprint systems with capacitive devices. Their study and ours share certain similarities in that both intend to encourage the suppliers and users of fingerprint systems to reconsider security of their systems. While their study is seen to be of use in designing fingerprint systems, unfortunately, details of the experimental conditions have not been described.

As we mentioned, a user of biometric systems cannot frequently replace or change her/his biometric data because of limits of biometric data intrinsic to her/himself. For example, gelatin, i.e., an ingredient of gummies, and soft plastic materials are easy to obtain at grocery stores and hobby shops, respectively. The fact that *gummy* fingers, which are easy to make with cheap, easily obtainable tools and materials, can be accepted suggests review not only of fingerprint systems but also of biometric systems. Manufacturers and vendors of biometric systems should carefully examine the security of their systems against artificial clones. Also, they should make public results of their examination, which lead users of their system to a deeper understanding of the security. The experimental study on the *gummy* fingers will have considerable impact on security assessment of fingerprint systems.

Declaration: We would like to stress that this study intends to encourage the suppliers and users of fingerprint systems to reconsider security of their systems, not to criticize libelously fingerprint systems for their security, and not to compare their performance.[17] For this purpose, we have collected, for our experiments, as many fingerprint systems commercially vailable as we could, and have detailed their specification and the experimental conditions.

ACKNOWLEDGMENT

The authors thank Yuldko Endo for her assistance in the experiments. This research was partially supported by MEXT Grant-in-Aid for Scientific Research 13224040 (Tsutomu Matsu

REFERENCES

1. AfB and ICSA: 1998 Glossary of Biometric Terms, Association for Biometrics and International Computer Security Association, to be referred at URL: http://www.afb.org.uk/ (1998).

2. ANSI A9.84-2001, Biometrics Information Management and Security (2001).

3. Bahuguna, R.D. and Corboline, T.: Prism fingerprint sensor that uses a holographic optical element, APPLIED OPTICS, Vol. 35, No. 26 (1996).

4. Bicz, W. et al.: Fingerprint structure imaging based on an ultrasound camera, http://www.optel.com.pl/article/english/article.htm, July 1 (2000).

5. Bovelander, E. and van Renesse, R. L.: An Introduction to Biometrics, in *Chip Card: Trump Card? Consequences for investigation and prosecution* 2nd Edition, Knopjs, F. and Lakeman, P. J. eds., Politie, Amsterdam (1999).

6. Collins, C. G.: Problems and Practices in Fingerprinting the Dead, FINGERPRINT SCIENCE: How to Roll, Classify, File and Use Fingerprints, Copperhouse Bublishing Company, ISBN 0-942728-18-1, Chapter 11, pp. 131-165:(1998).

7. ECOM: Report by the Working Group on PersonalAuthentication (WG6) Ver. 1.0, Electronic Commerce Promotion of Japan (ECOM), April 27 (1998).

8. Endo, Y., Matsumoto H. and Matsumoto, T.: Comparison Between Dry Live Fingers and Artificial Fingers in Fingerprint Authentication, *Technical Report of IEICE*, ISEC2001-14, pp. 17-24, May (2000).

9. Hoshino, S., Matsumoto H. and Matsumoto, T.: Mapping a Fingerprint linage to an Artificial Finger, *Technical Report of IEICE*, ISEC2001-60, pp. 5,3-59, September (2001).

10. Igaki, S., Eguchi, S, Yamagishi, F., Ikeda, H. and Inagaki, T.: Real-time fingerprint sensor using a hologram, APPLIED OPTICS, Vol. 31, No. 11 (1992).T

11. Jain, K.: INTRODUCTION TO BIOMETRICS, in *Biometrics: Personal Identification in a Networked Society*. The Kluwer Academic Publishers, International Series in Engineering and Computer Science, Jain, A. K., Bolle, R. and Pankanti, S. eds., Vol. 479, Chapter 1, pp. 1-41 (1999).

12. Japanese patent numbers; 11-250255 and 10-105710.

13. Japanese patent numbers; 2000-76450, 2000-20684, 11-45338, 10-307904, 10-302047, 10-290796, 10-261086, 10-240942, 10-154231, 9-259272, 6-187430, 6-162 175, 4-241680, 3-188574, 1-233556. 63-123 168, and 61-221883.

14. Jung, S., Thewes, R, Scheiter, T. and Gorser K. F.: A Low-Power and High-Performance CMOS Fingerprint Sensing and Encoding Architecture, *IEEE Journal of Solid-State Circuit*, Vol. 34, No. 7 (1999).

15. Mainguet, J. F., Pegulu, P. and Harris, J. B.: Fingerprint recognition based on silicon chips, *Future Generation Computer Systems*, Vol. 16, No.4 pp.403-15, (1999).

16. Matsumoto, T.: Availability of Artificial Fingers That Fool Fingerprint Systems, *Proc. JCP2000*, Yokoh ma, Japan, October (2000).

17. Matsumoto, T.: What will you do if you find a particular weakness of a security technology?, *Journal of IEICE*, Vol. 84, No.3 (2001).

18. Miyauchi, H., et al.: Fluorigenic Detection for Latent Fingerprints on the Colored paper with NBD-C1 and NBD-F, *Reports of National Research Institute of Police Science*. Vol. 42, No.4, pp. 16-18 (1989).

19. Network Computing: Six biometric devices point the finger at security, reviews, pp. 84-96 (1998). also to be referred at URL: http://www.networkcomputing.com, August 2000.

20. O'Gorman, L.: Fingerprint Verification, in *Biometrics: Personal Identification in Networked Society*, The Kluwer Academic Publishers, International Series in Engineering and Computer Science, Jain, A. K., Belle R. and ankanti, S. eds., Vol. 479, Chapter 2, pp. 43-64 (1999).

21. Ratha. N. K. and Bolle, R.: SMARTCARD BASED AUTHENTICATION, in *Biometrics: Personal Identification in Networked Society*, The Kluwer Academic Publishers, International Series in Engineering and Computer Science, Jain, A. K., Bolle R. and Pankanti. S. eds., Vol. 479, Chapter 18, pp. 369-384 (1999).

22. Shigematsu, S., Morimura, H., Tanabe, Y., Adachi, T. and Machida, K.: A Single-Chip Fingerprint Sensor and Identifier, *IEEE Journal of Solid-State Circuit*, Vol. 34, No. 12 (1999).

23. SJB Service: Fingerprint Verification, in *The Biometric Report 1999*, Second Edition, Newham, E., Bunney, C. and Mearns, C. eds., Chapter 4, pp. 61-91 (1998).

24. Sonident : US patent numbers 5258922 and 5515298.

25. van der Putte, T. and Keuning, J.: Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned, *SMART CARD RESEARCH AND ADVANCED APPLICATIONS*, IFIP TCS/WG8.8 Four\th Working Conference on Smart Card Research and Advanced Applications, pp. 289-303 (2001) *[See http://cryptome.org/fake-prints.htm]*

26. van Renesse. R. L.: An Introduction to Biometrics, in *Optical Document Security*, Second Edition, Artech House, Rudolph L. van Renesse ed., Chapter 15, (1998).

27. Yamada, K., Matsumoto H. and Matsumoto, T.: Can We Make Artificial Fingers That Fool Fingerprint Systems? *Technical Report of IEICE and IPSJ*, ISEC2000-45, pp. 159-166, and Vol. 2000 No.68, pp 159-166 respectively, July (2000).

28. Yamada, K., Matsumoto H. and Matsumoto, T.: Can We Make Artificial Fingers That Fool Fingerprint Systems? (Part II), *Proc. of IPSJ for Computer Security Symposium 2000*, Vol. 2000, No. 12, pp. 109-114, Tokyo, Japan, October (2000).

29. Yamada, K., Matsumoto H. and Matsumoto, T.: Can We Make Artificial Fingers That Fool Fingerprint Systems? (Part III), *Proc. of IEICE for The 2001 Symposium on Cryptography and Information Security*. Vol. II, pp. 719-724, Oiso, V Kanagawa, Japan, January (2001).

APPENDIX A

A. Recipes for Artificial Fingers

A.1 Making an Artificial Finger Directly from a Live Finger[27-29]

+ Ingredients

- ***Material for molds:*** "FREEPLASTIC"

Free molding plastic is used for plastic models and can be bought at hobby shops. The cost of the material is around 300 yen per 35 grams. Here, "FREEPLASTIC" is a registered trademark of Daicel

FineChem Ltd. (formerly Dalcel Craft Ltd.). Also, silicone rubber can be alternatively used for the impression material.

- ***Material for artificial fingers:*** "GELATINE LEAF"

  Solid gelatin sheet is used for ingredients for confectionery such gel foods as jellied meats. soups, and candies and molded desserts, and also can be bought at grocery stores. The cost of the material is around 200 yen per 30 grams. Here, "GELATINE LEAF" is a product of MARUHA CORP. Gelatin powder can be used altematively for solid gelatin sheet, and however is a little hard to treat.

+ How to make a mold

We make molds, which are made of free molding plastic, of live fingers, and then make artificial fingers, which are made of gelatin, with the molds.

We make molds by the following procedures.

(1) Put the material "FREEPLASTIC" into hot water, which temperature is more than around 60 degrees Centigrade, to soften it, and then take it out.

(2) Wait until the plastic will get a little cool, and then make it round as a small ball.

(3) Press against the plastic ball so as to make the fingertip be in the same condition as it was scanned by fingerprint devices.

(4) Wait till the plastic hardens. And then, remove the fingertip from the mold. It takes around ten minutes.

+ How to make artificial fingers

We make artificial fingers by the following procedures.

(1) Add boiling water (30cc) to solid gelatin (30 grams) in a bottle and mix up them. Cap the bottle and wait till the mixture forms a gel as it cools, and then melt to form a sol by heating with a microwave oven. After that, cool down to form a gel and heat up to form a sol several times to reduce bubbles, if necessary. As a result of this procedure, a liquid in which immersed gelatin at 50 wt.% (a sol) will be obtained.

(2) Prepare a mold, and pour the liquid into the mold. Remove carefully bubbles which are formed around the base of the mold, if necessary.

(3) Put this mold into a refrigerator to cool, and wait for about ten minutes till the liquid changes back to a gel. Pull the gel (i.e., artificial finger) out of the mold.

Repeat (2) and (3) to make the *gummy* fingers.

A.2 Making an Artificial Finger from a Residual Fingerprint[9]

+ Ingredients

- ***Material for molds:*** photosensitive coated PCBs "10K"

  You can find a photo sensitive coated printed circuit board (PCB) ready to use in most electronics shops, or hobby shops. The cost of the PCB is around 320 yen per sheet. Here, "10K" is a product of Sanhavato Co., Ltd. The other materials necessary for processing will be given in the followings.

  Material for artificial fingers: "GELATINE LEAF"

  Solid gelatin sheet is used for ingredients for confectionery such gel foods as jellied meats, soups, and candies and molded desserts, and also can be bought at grocery stores. The cost of the material is around 200 yen per 30 grams. Here, "GELATINE LEAF" is a product of MARUHA CORP. Gelatin powder can be used alternatively for solid gelatin sheet, and however is a little hard to treat.

+ How to make a mold

We make molds, which are made by photolithographic processes, of live fingers, and then make artificial fingers, which are made of gelatin, with the molds.

We make molds by the following procedures.

- ***Making a mask***

  (1) Press the live finger against a glass plate so as to make its residual fingerprint.

  (2) Enhance this latent fingerprint with a cyanoacrylate adhesive. If you put the adhesive with the glass plate intolairtight container, it will keep for quite a long time. Wait for a minute. The fingerprint will stand clearly outlined against the glass plate.

  (3) Capture an image of the fingerprint with a digital microscopic camera (e.g., KEYENCE; VH-6300, 900k pixels). Set the fingerprint image right side left, and make its contrast better with an image processing software (e.g., Adobe; Photoshop 6.0).

  (4) Print the fingerprint image in a transparency sheet with an inkjet printer (e.g., Canon; BJ-F800, 1200x600dpi). It can be used for a mask.

- ***Making a mold***

  (1) Prepare a photo sensitive coated PCB, and fix the mask so that its printed surface is attached on the PCB. Exose an UV light source for 6 minutes to copy the mask to the photo resist layer of the PCB. Caution: The UV light are harmful for your eyes and you shouldn't look it many time, or any at all.

  (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 mold for artificial fingers can be obtained.

- ***Making an artiflicial finger***

  We make artificial fingers by the following procedures.

  (1) Add boiling water (30cc) to solid gelatin (24 grams) in a bottle and mix up them. Cap the bottle and wait till mixture forms a gel as it cools, and then melt to form a sol by heating with a microwave oven. After that, cool down to form a gel and heat up to form a sol several times to reduce bubbles, if necessary. As a result of this procedure, a liquid in which immersed gelatin at around 40 wt.% (a sol) will be obtained.

  (2) Prepare a mold, and drip the liquid onto the mold. Remove carefully bubbles which are formed around the base of the mold, if necessary.

  (3) Put this mold into a refrigerator to cool, and wait for about ten minutes till the liquid changes back to a gel. Peel carefully the gel (i.e., artificial finger) from the mold.

  Repeat (2) and (3) to make the *gummy* fingers.

APPENDIX B

B. Fingerprint Systems

The list of fingerprint devices and the procedures for the fingerprint systems are shown in APPENDIX B.1, and B.2, respectively.

B.1 The List of Fingerprint Devices

	Hardware Specifications						Software Specifications			Methods for Verification	References (Note: '*' stands for a web site in Japanese
	Manufacturer/ Selling Agency	**Product Name**	**Type**	**Product Number**	**Sensor**	**Live and Well Detection**	**Manufacturer/ Selling Agency**	**Product Name (Application)**	**Comparison Levels**		
Device A	Compaq Computer Corporation	Compaq Stand-Alone Fingerprint Identification Unit	DFR™ -200	E03811US001	Optical Sensor	unknown	Compaq Computer Corporation	Fingerprint Identification Technology Software version 1.1	1 through 3	Minutiae Matching	http://www.compaq.com/products/quickspecs/10690_na/10690_na.HTML
Device B	MITSUBISHI ELECTRIC CORPORATION	Fingerprint Recognizer	FPR-DTmkII	003136	Optical Sensor	unknown	Sumikin Izumi Computer Service Co., Ltd.	SecFP V1.11	Fixed	Minutiae Matching	http://www.melco.co.jp/rd_home/map/iesl/fields/b03e.html * http://www.mitsubishi-fpr.com/jp/index.html
Device C	NEC Corporation	Fingerprint Identification Unit (Prism)	N7950-41	9Y00003	Optical Sensor	unknown	NEC Corporation	Basic Utilities for Fingerprint Identification	Fixed	Minutiae Matching (Minutia and Relation)	http://www.sw.nec.co.jp/english/pid_e/index.html * http://www.sw.nec.co.jp/pid
Device D	OMRON Corporation	Fingerprint Recognition Sensor	FPS-1000	90500854	Optical Sensor	unknown	OMRON Corporation	"*YUBI PASS*" U.are.U™ Fingerprint Verification Software	Fixed	Minutiae Matching	http://www.digitalpersona.com/ * http://www.omron.co.jp/ped-j/home.html
Device E	Sony Corporation	Sony Fingerprint Identification Unit	FIU-002-F11	00709	Optical Sensor	Live Finger Detection	TSUBASA SYSTEM CO., LTD.	Fingerprint Identification Unit Windows ™ 95 Interactive Demo Version 1.0 Build 13	1 through 5	Pattern Matching	* http://www.sony.co.jp/SonyInfo/News/Press/199705/97Co-035/ http://www.biometrix.at/page19.htm
Device F	FUJITSU LIMITED	Fingsensor	FS-200U	00AA000257	Capacitive Sensor	unknown	FUJITSU LIMITED	Logon for Fingsensor V1.0 for Windows ™ 95/98	Fixed	Minutiae Matching (Correlation)	* http://www.fmworld.net/product/hard/keyboard/finsensor/index.html
Device G	NEC Corporation	Fingerprint Identification Unit (Serial)	PK-FP002	0300529S	Capacitive Sensor	unknown	NEC Corporation	Basic Utilities for Fingerprint Identification	Fixed	Minutiae Matching (Minutia and Relation)	http://www.sw.nec.co.jp/english/pid_e/index.html * http://www.sw.nec.co.jp/pid

Device H	Siemens AG (Infineon Technologies AG)	FingerTIP™ EVALUATION KIT	EVALUATION-KIT	C98451-D6100-A900-4	Capacitive Sensor	unknown	Siemens AG (Infineon Technologies AG)	FingerTIP™ Software Development Kit (SDK) Version: V0.90, Beta 3 "Demo Program"	Fixed	Minutiae Matching	http://www.Fingertip.de/ http://www.infineon.com/products/chipcds/portfol/biometr/introduction.htm
Device I	Sony Corporation	Sony Fingerprint Identification Unit	FIU-710	3000398	Capacitive Sensor	Live Finger Detection	Systemneeds Inc.	SecuDesktop™ 1.55 Japanese version	1 through 5	Pattern Matching	http://www.sony.co.jp/en/Products/puppy/contents03.html * http://systemneeds.co.jp/products/index.htm
Device J	SecuGen™ Corporation	EyeD Mouse II (SecuGen™ Mouse)	SMB-800	9650172004	Optical Sensor	unknown	Secugen	Secure Suite Release 1.0	1 through 9	Minutiae Matching	* http://secugen.co.jp/products.html http://secugen.com/products.html
Device K	Ethentica Inc.	Ethenticator™ MS 3000 PC Card	MS 3000	M300F200991	Optical Sensor	unknown	Ethentica		Fixed	Minutiae Matching	http://www.ethentica.com/product.html

Note 1: DFR™ is a registered trademark of Compaq Computer Corporation. Windows ™ is a registered trademark of Microsoft Corporation. FingerTIP ™ is a registered trademark of Siemens AG (Infineon Technlogies AG). U.ar.U™ is a registered trademark of DigitalPersona, Inc. SecuGen™ and SecuDesktop™ are a registered trademarks of SecuGen Corporation. Ethenticator™ is a registered trademark of Ethentica Inc.

Note 2: All contents of this table are based on our investigation on attached catalogs, web sites in the references, etc.

[Chart image (355KB)]

B.2 The Procedures for the Fingerprint Systems

The followings give the procedures for each fingerprint device.

Device A: We enroll a finger as a template in the system. And then, enrollment will be finished if the template can be verified in a subsequent verification. We used a logon sequence, which is a function of the system, to know whether the system accepts the finger or not. Fingerprint images are displayed on the screen of the PC both in enrollment an in verification.

Device B: We enroll a finger four times in the system to make a template. We can check whether the template in good condition by activating a verification function. We used this function to know whether the system accepts the finger or not Fingerprint images are not displayed on the screen ofthe PC.

Device C: We enroll a finger three times in the system to make a template. And then, we exit the application of the fingerprint system. We can encounter a verification procedure when we start the application again. We used this procedure to know whether the system accepts the finger or not. Fingerprint images are displayed on the screen of the PC only in enrollment.

Device D: We enroll a finger four times in the system to make a template. We used a logon sequence, which is a function of the system, to know whether the system accepts the finger or not. Fingerprint images are displayed on the screen of the PC only in enrollment.

Device E: We enroll a finger as a template in the system. We can check whether the template is in good condition by activating a verification function. We used this function to know whether the system

accepts the finger or not. Fingerprint images are displayed on the screen of the PC both in enrollment and in verification.

Device F: We enroll a finger four times in the system to make a template. We used a logon sequence, which is a function of the system, to know whether the system accepts the finger or not. Fingerprint images are displayed on the screen of the PC only in enrollment.

Device G: The system is the same as that of Device C.

Device H: We enroll a finger three times in the system to make a template. We can check whether the template is in good condition by activating a verification function. We used this function to know whether the system accepts the finger or not. Fingerprint images are displayed on the screen of the PC both in enrollment and in verification.

Device I: We enroll a finger four times in the system to make a template. We can check whether the template is in good condition by activating a verification function. We used this function to know whether the system accepts the finger or not. Fingerprint images are displayed on the screen of the PC only in enrollment.

Device J: We enroll a finger two times in the system to make a template. We used a logon sequence, which is a function of the system, to know whether the system accepts the finger or not. Fingerprint images are displayed on the screen f the PC only in enrollment.

Device K: We enroll a finger three times in the system to make a template. We used a logon sequence entering the user's ID, activating a verification function, to know whether the system accepts the finger or not. Fingerprint images are displayed on the screen of the PC only in enrollment, but not in verification.

Transcription and HTML by Cryptome.

From Bruce Schneier's Crypto-Gram, 15 May 2002

Fun with Fingerprint Readers

Tsutomu Matsumoto, a Japanese cryptographer, recently decided to look at biometric fingerprint devices. These are security systems that attempt to identify people based on their fingerprint. For years the companies selling these devices have claimed that they are very secure, and that it is almost impossible to fool them into accepting a fake finger as genuine. Matsumoto, along with his students at the Yokohama National University, showed that they can be reliably fooled with a little ingenuity and $10 worth of household supplies.

Matsumoto uses gelatin, the stuff that Gummi Bears are made out of. First he takes a live finger and makes a plastic mold. (He uses a free-molding plastic used to make plastic molds, and is sold at hobby shops.) Then he pours liquid gelatin into the mold and lets it harden. (The gelatin comes in solid sheets, and is used to make jellied meats, soups, and candies, and is sold in grocery stores.) This gelatin fake finger fools fingerprint detectors about 80% of the time.

His more interesting experiment involves latent fingerprints. He takes a fingerprint left on a piece of glass, enhances it with a cyanoacrylate adhesive, and then photographs it with a digital camera. Using PhotoShop, he improves the contrast and prints the fingerprint onto a transparency sheet. Then, he takes a photo-sensitive printed-circuit board (PCB) and uses the fingerprint transparency to etch the fingerprint into the copper, making it three-dimensional. (You can find photo-sensitive PCBs, along with instructions for use, in most electronics hobby shops.) Finally, he makes a gelatin finger using the print on the PCB. This also fools fingerprint detectors about 80% of the time.

Gummy fingers can even fool sensors being watched by guards. Simply form the clear gelatin finger over your own. This lets you hide it as you press your own finger onto the sensor. After it lets you in, eat the evidence.

Matsumoto tried these attacks against eleven commercially available fingerprint biometric systems, and was able to reliably fool all of them. The results are enough to scrap the systems completely, and to send the various fingerprint biometric companies packing. Impressive is an understatement.

There's both a specific and a general moral to take away from this result. Matsumoto is not a professional fake-finger scientist; he's a mathematician. He didn't use expensive equipment or a specialized laboratory. He used $10 of ingredients you could buy, and whipped up his gummy fingers in the equivalent of a home kitchen. And he defeated eleven different commercial fingerprint readers, with both

optical and capacitive sensors, and some with "live finger detection" features. (Moistening the gummy finger helps defeat sensors that measure moisture or electrical resistance; it takes some practice to get it right.) If he could do this, then any semi-professional can almost certainly do much much more.

More generally, be very careful before believing claims from security companies. All the fingerprint companies have claimed for years that this kind of thing is impossible. When they read Matsumoto's results, they're going to claim that they don't really work, or that they don't apply to them, or that they've fixed the problem. Think twice before believing them.

Matsumoto's paper is not on the Web. You can get a copy by asking:

Tsutomu Matsumoto <tsutomu@mlab.jks.ynu.ac.jp>

Here's the reference:

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.

Some slides from the presentation are here:

http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf

My previous essay on the uses and abuses of biometrics:

http://www.counterpane.com/crypto-gram-9808.html#biometrics>

Biometrics at the shopping center: pay for your groceries with your thumbprint.

http://seattlepi.nwsource.com/local/68217_thumb27.shtml