Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies
--- A Case Study for User Identification ---

14 May 2002

Tsutomu Matsumoto

Graduate School of Environment and Information Sciences

Yokohama National University

email: tsutomu@mlab.jks.ynu.ac.jp

Yokohama Nat. Univ.
Matsumoto Laboratory

Security Architecture

Operating Systems Security

Software Tamper Resistance

Mobile Code Security

Physical Tamper Resistance

Communications Security

Cryptographic Protocol

User Identification

……

***Security assessment** of biometric user identification systems should be conducted not only for the accuracy of authentication, but also for security against fraud.*
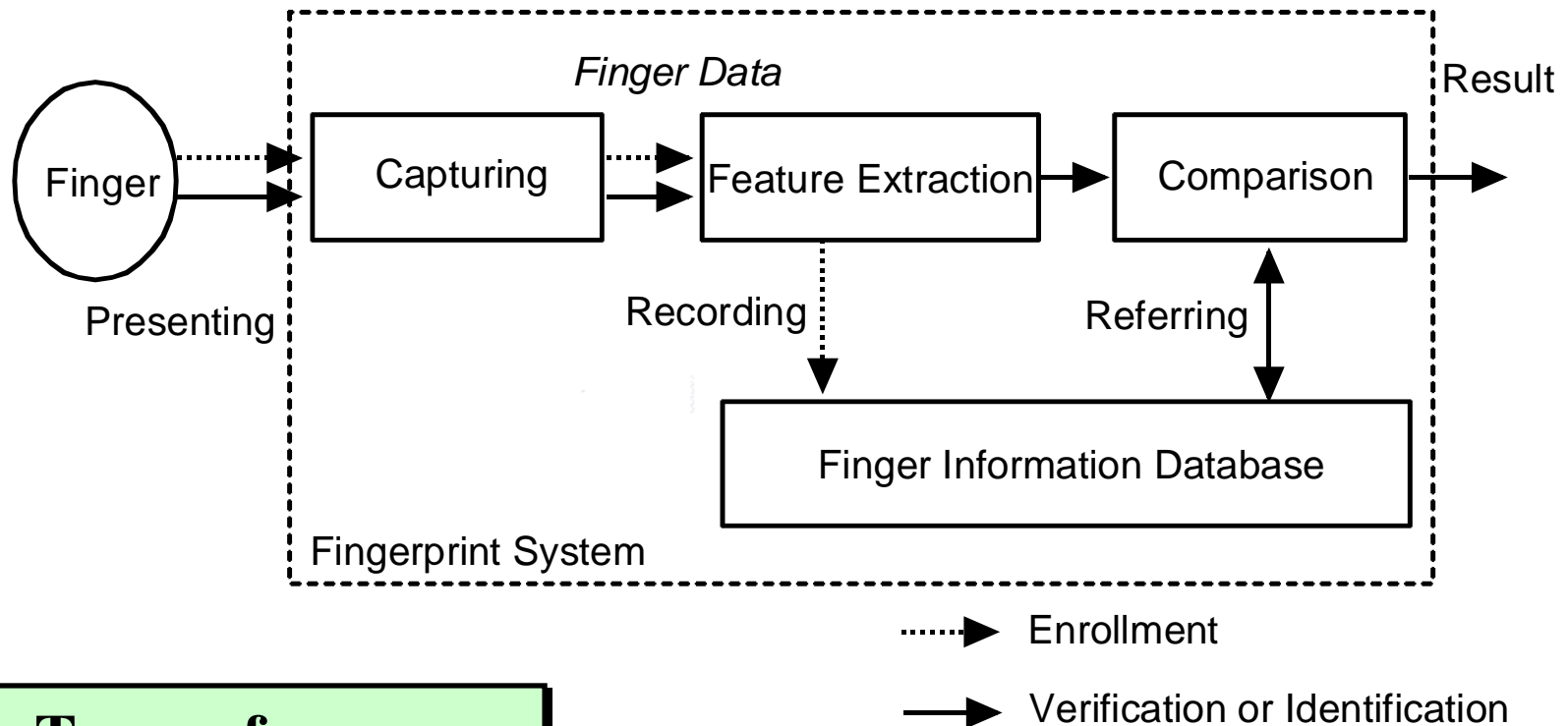
In this presentation we focus on Fingerprint Systems which may become widespread for Mobile Terminals.

Examine Adversarial Analysis as A Third Party

- *Can we make artificial fingers that fool fingerprint systems?*
- *What are acceptance rates?*

Typical structure of a fingerprint system

Finger Data

Result

Finger → Capturing → Feature Extraction → Comparison →

Presenting

Recording

Referring

Finger Information Database

Fingerprint System

········► Enrollment

───► Verification or Identification

Types of sensors

- **Optical sensors**
- **Capacitive sensors**
- **Thermal sensors, Ultrasound sensors, etc.**

"Live and Well" Detection

Attackers may present

1) *the registered finger,*
   by an armed criminal, under duress, or with a sleeping drug,

2) *an unregistered finger (an imposter's finger),*
   i.e., non-effort forgery,

3) *a severed fingertip from the registered finger,*

4) *a genetic clone of the registered finger,*

5) *an artificial clone of the registered finger, and*

6) *the others,*
   such as a well-known method as a "fault based attack."

Part of patterns of dishonest acts with artificial fingers against a fingerprint system.

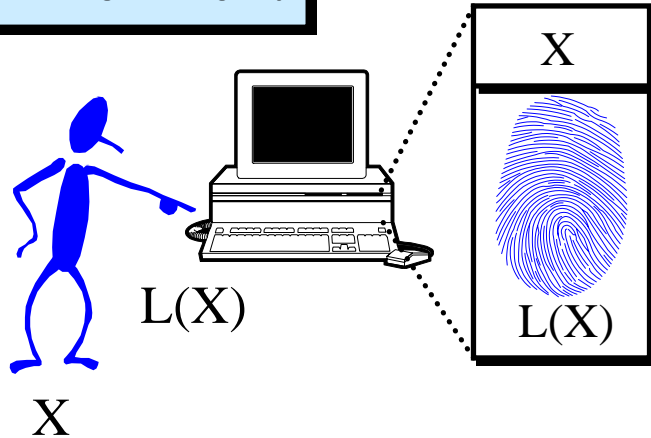| Enrollment	Verification / Identification				
	L(X)	A(X)	L(Y)	A(Y)	A(Z)
L(X)	(1)	(2)	– *	–	–
A(Y)	–	–	(3)	(4)	–
A(Z)	–	–	–	–	(5)

L(X): A Live Finger corresponding to Person X
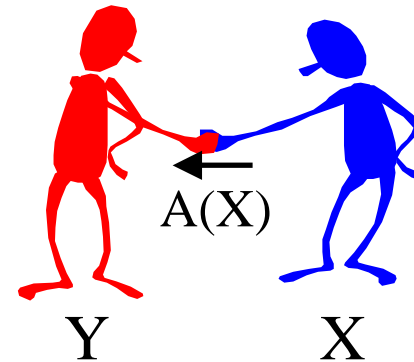**A(Y): An Artificial Finger corresponding to Person Y**
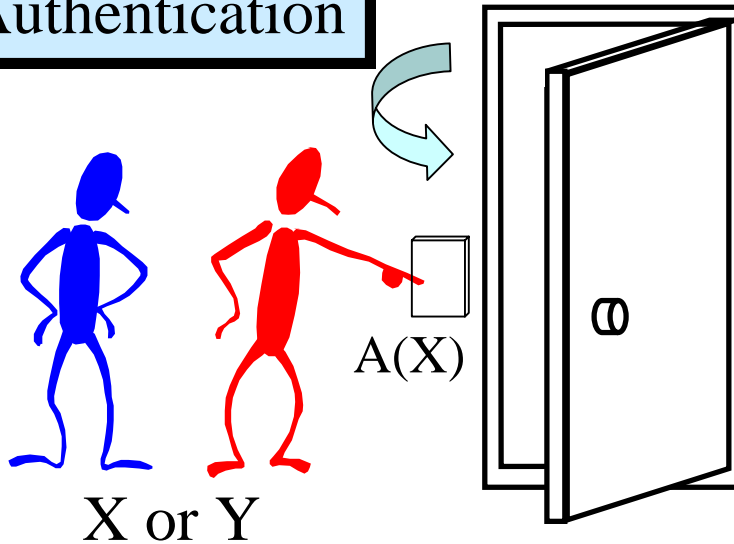**A(Z): An Artificial Finger corresponding to Nobody**

Enrollment

X

L(X)

X

L(X)

Authentication

A(X)

X or Y

Y obtains A(X).

A(X)

Y   X

Distribution of A(X)s

A(X)s

X obtains A(Y).

A(Y)

Y   X

X enrolls A(Y).

X

A(Y)

A(Y)

Authentication

A(Y)
or L(Y)

X or Y

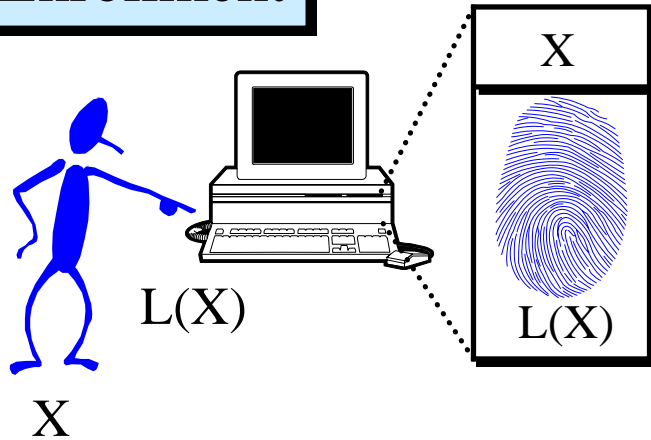Distribution of A(Y)s

A(Y)s
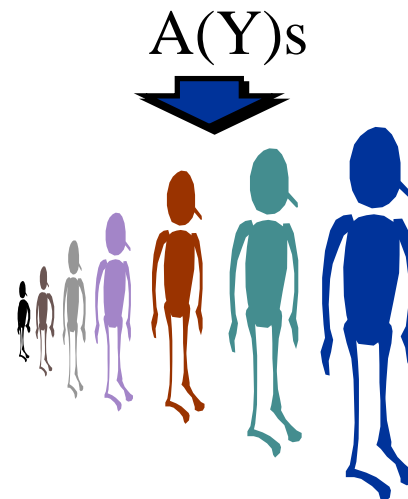
Fraud with Artificial Fingers III

Enrollment
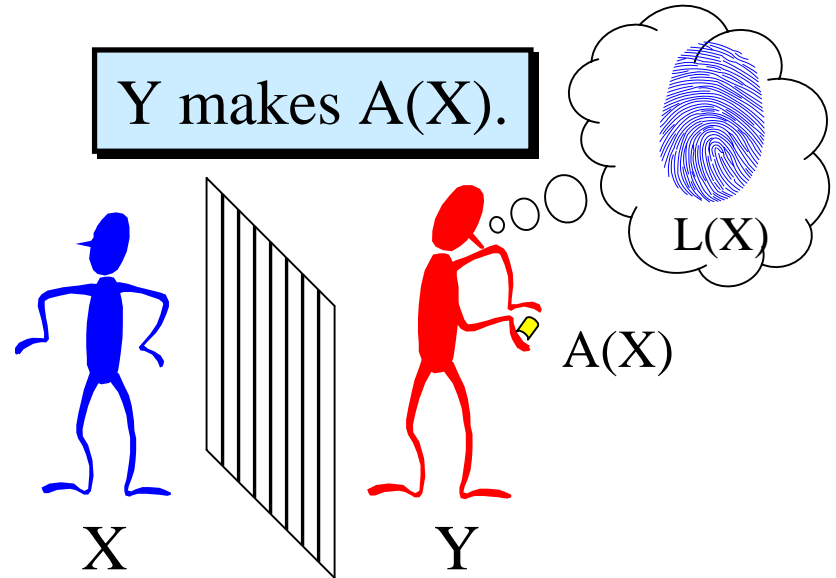
X

L(X)

L(X)

X

Y makes A(X).

L(X)

A(X)

X   Y

Authentication

A(X)

Y

Distribution of A(X)s

A(X)s
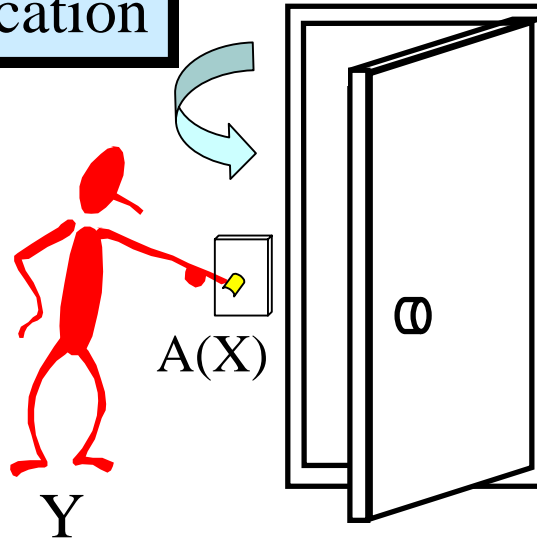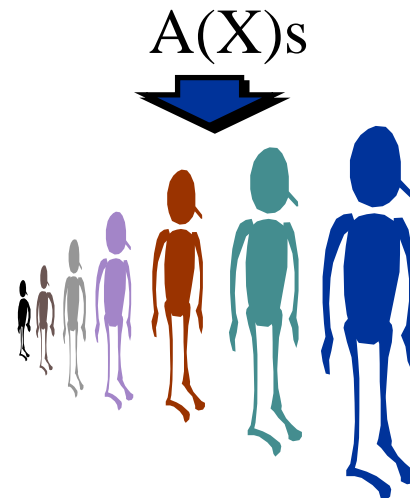
Finegerprint

e.g., Live Fingers, Generators, ...

⬇
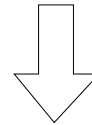
Impression

e.g., Molds, Residual Fingerprints, ...

⬇
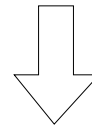
Artificial Finger

Process 0

(1) Finger
(2) Mold

(3) Silicone Rubber Finger

Optical Sensor

Finger

Detector

Light Source

⬇
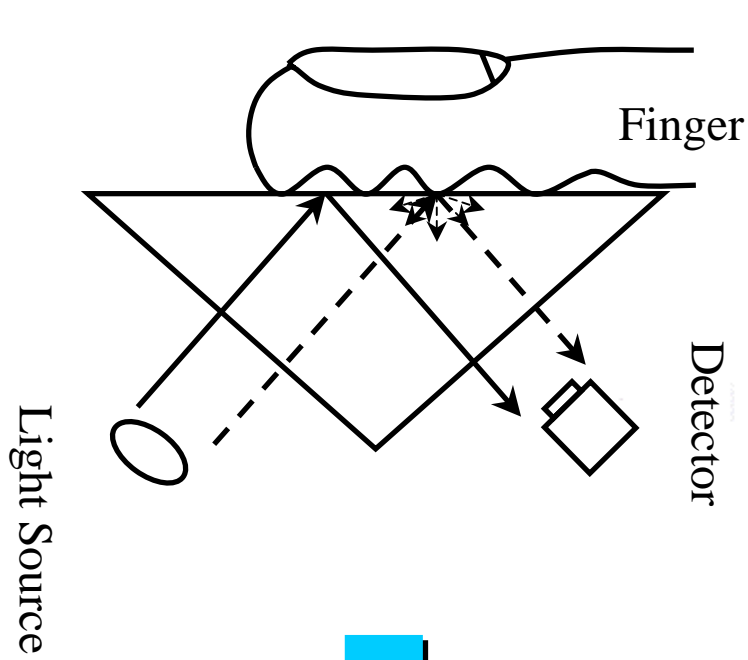
Often Accepts
Silicone Rubber Fingers

Capacitive Sensor

Finger

Array of Electrodes

⬇
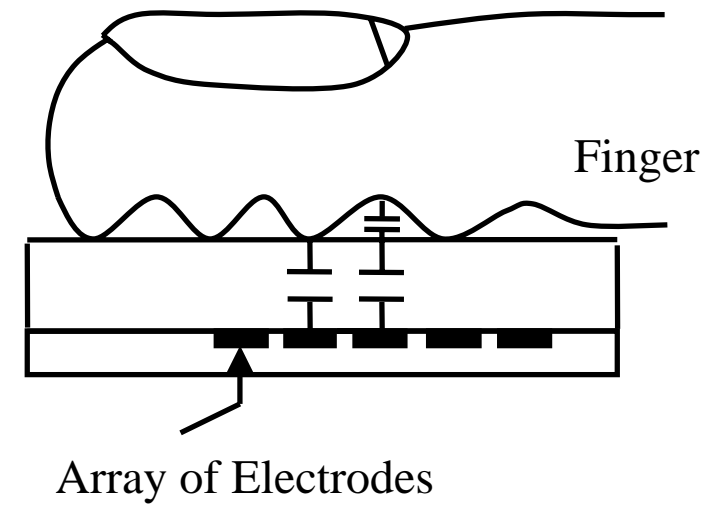
Usually Rejects
Silicone Rubber Fingers

Our Result

Process 1

(1) Finger

(2) Plastic Mold

(3) Gummy Finger

Making an Artificial Finger directly from a Live Finger

Materials

Free molding plastic
"FREEPLASTIC"
by Daicel FineChem Ltd.

Solid gelatin sheet
"GELATINE LEAF "
by MARUHA CORP

350JPY/35grams
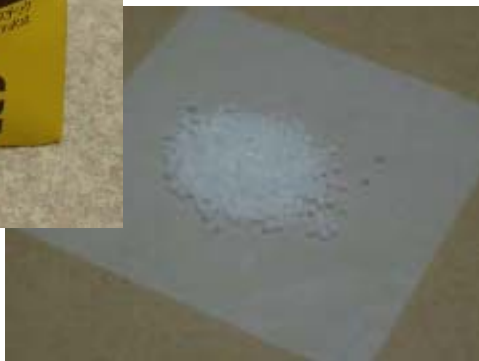
200JPY/30grams

Making an Artificial Finger directly from a Live Finger

How to make a mold

Put the plastic into hot water to soften it.

Press a live finger against it.

The mold

It takes around 10 minutes.

Making an Artificial Finger directly from a Live Finger

Preparation of material

● **A liquid in which immersed gelatin at 50 wt.% .**

Add boiling water (30cc) to solid gelatin (30g) in a bottle and mix up them.

It takes around 20 minutes.

Making an Artificial Finger directly from a Live Finger

How to make a gummy finger

Pour the liquid into the mold.

Put it into a refrigerator to cool.

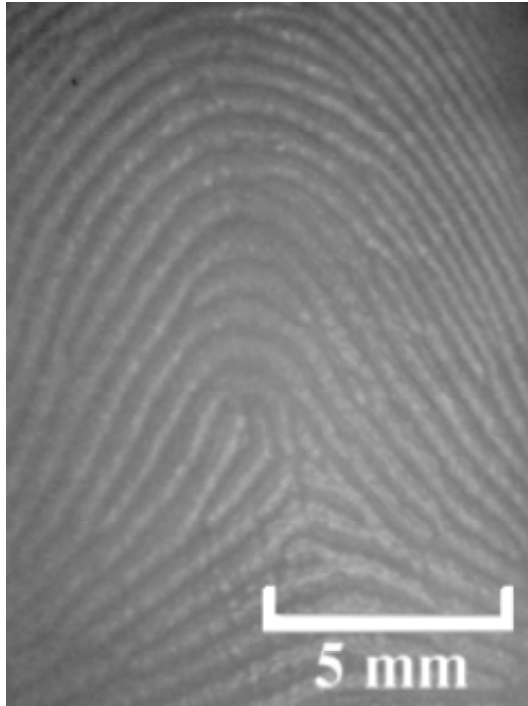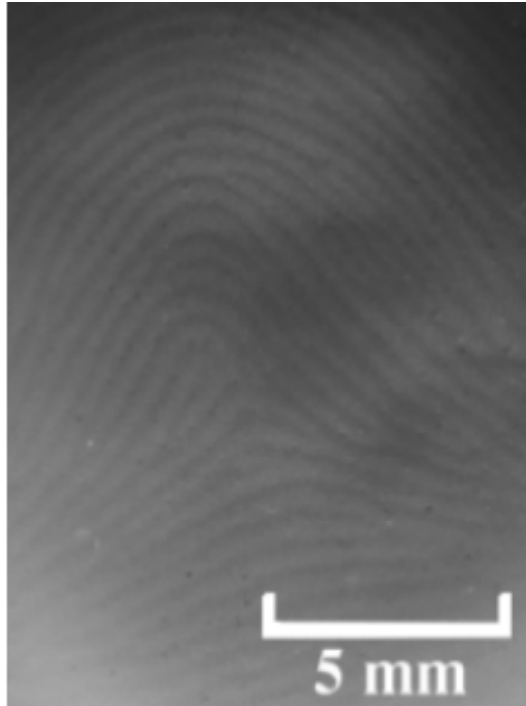**The gummy finger**

It takes around 10 minutes.

The photomicrographs of fingers

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

Captured images with the device C (an optical sensor).

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

Captured images with the device H (a capacitive sensor).

(a) Live Finger   (b) Gummy Finger

Subjects: five persons whose ages are from 20's to 40's

Fingerprint systems: 11 types

We attempted one-to-one verification 100 times counting the number of times that it accepts a finger presented.

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

The List of Fingerprint Devices

	Hardware Specifications					Software Specifications			Methods for Verification
	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
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
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)
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
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
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)
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)
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	Minutia matching
Device I	Sony Corporation	Sony Fingerprint Identification Unit	FIU-710	3000398	Capacitive Sensor	Live Finger detection	Systemneeds Inc.	Good-bye "*PASSWORD*"s	1 through 5	Pattern matching
Device J	Secugen	EyeD mouse II	SMB-800	9650172004	Optical Sensor	unknown	Secugen	SecuDesktop 1.55	1 through 9	Minutia matching
Device K	Ethentica	ethenticatior MS 3000 PC Card	MS 3000	M300F200991	Optical Sensor	unknown	Ethentica	Secure Suite Release1.0	Fixed	Minutia matching

Making an Artificial Finger directly from a Live Finger
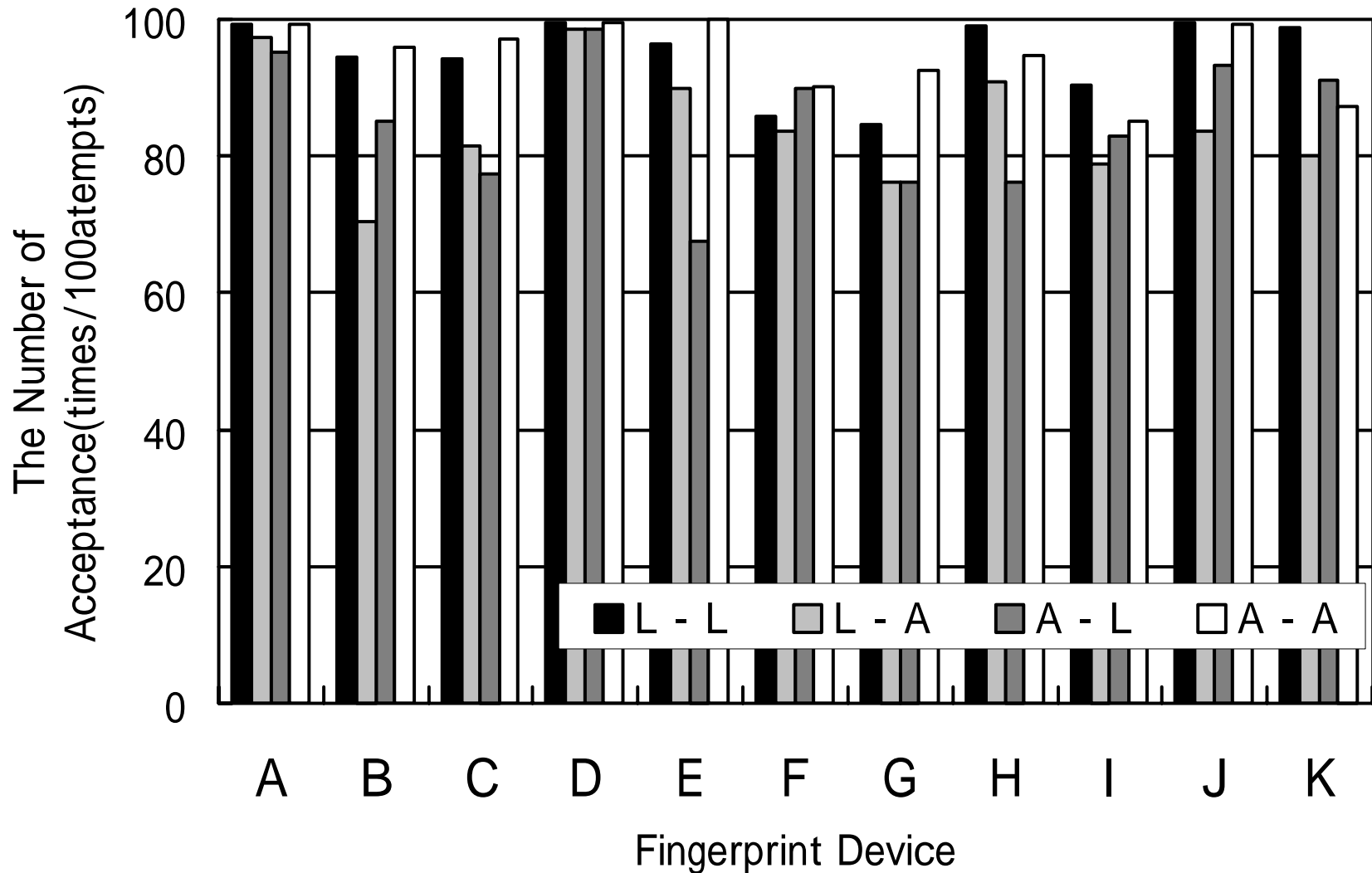
Our Result

Process 2

(1) Residual Fingerprint

(2) Digital Image Data

(3) Printed Circuit Board

(4) Gummy Finger

Making an Artificial Finger from a Residual Fingerprint

Materials

A photosensitive coated Printed Circuit Board (PCB)
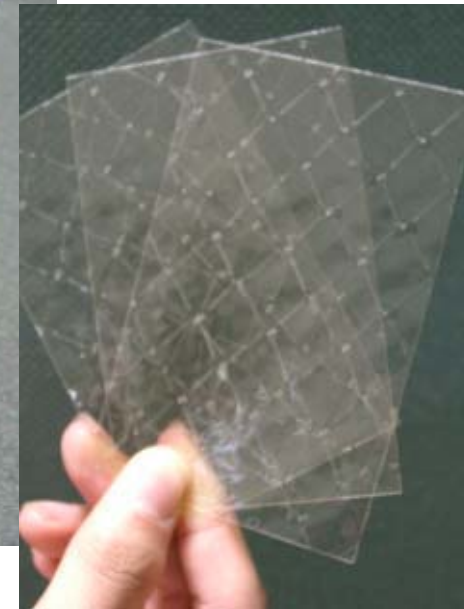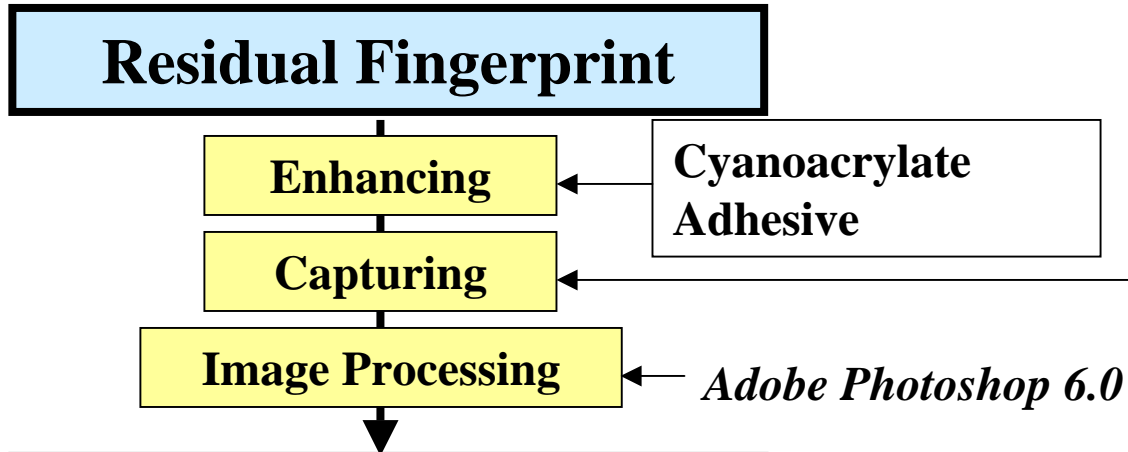
"10K" by Sanhayato Co., Ltd .

320JPY/sheet

Solid gelatin sheet
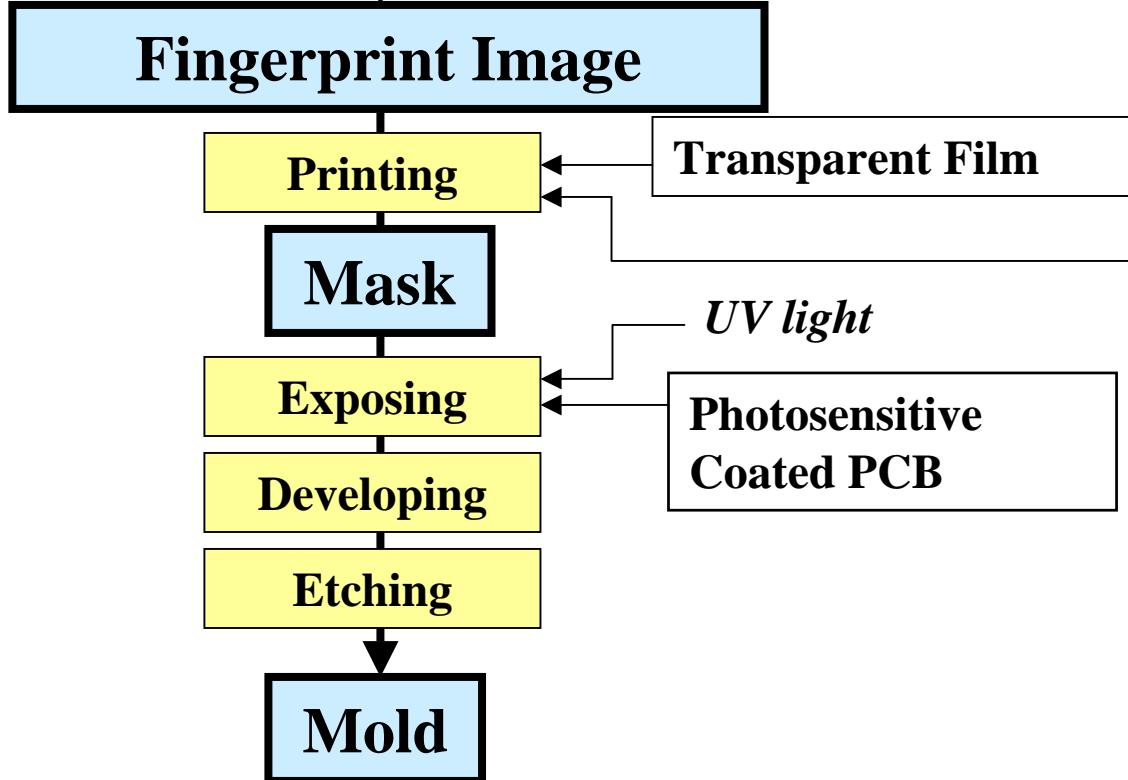"GELATINE LEAF "
by MARUHA CORP

200JPY/30grams

Residual Fingerprint

Enhancing ← Cyanoacrylate Adhesive

Capturing

Image Processing ← *Adobe Photoshop 6.0*

Fingerprint Image

Printing ← Transparent Film

Mask

Exposing ← *UV light*

← Photosensitive Coated PCB

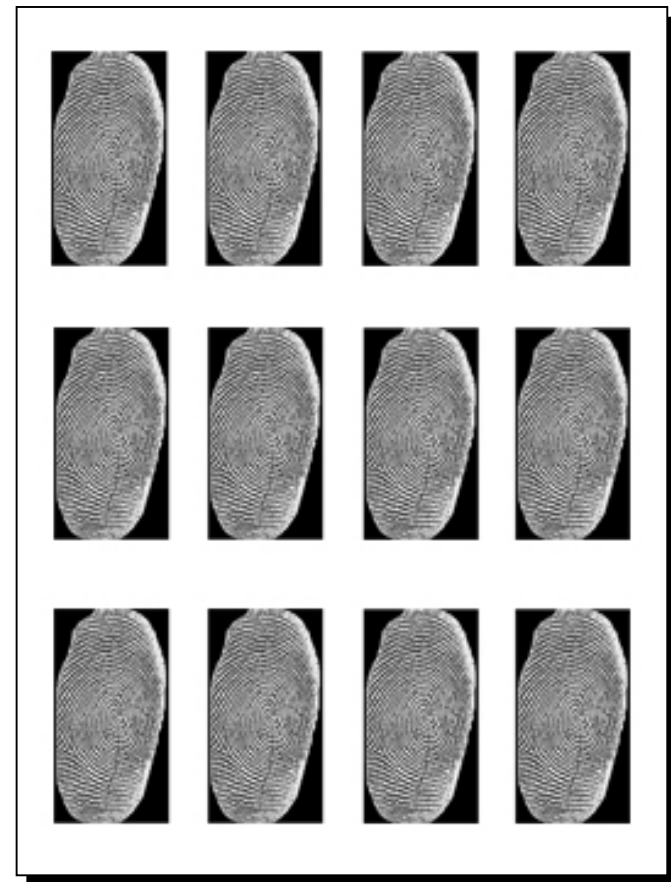**Developing**

Etching

Mold

Digital Microscope

KEYENCE VH6300: 900k pixels
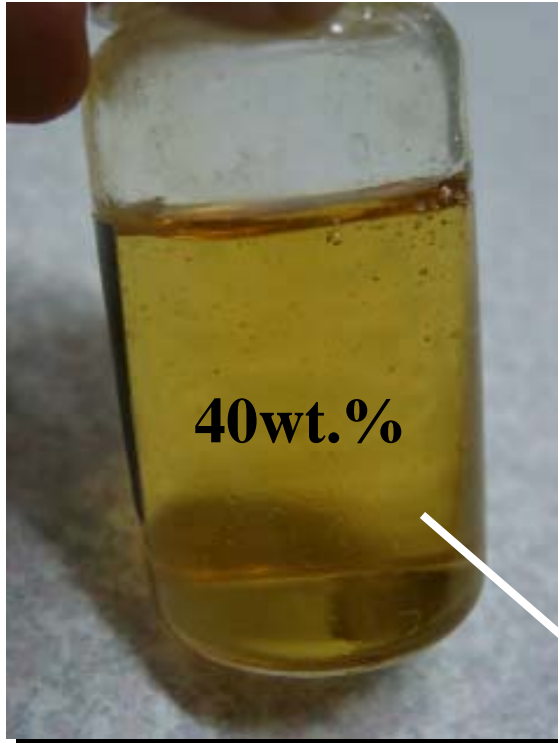
Inkjet Printer

Canon BJ-F800: 1200x600dpi

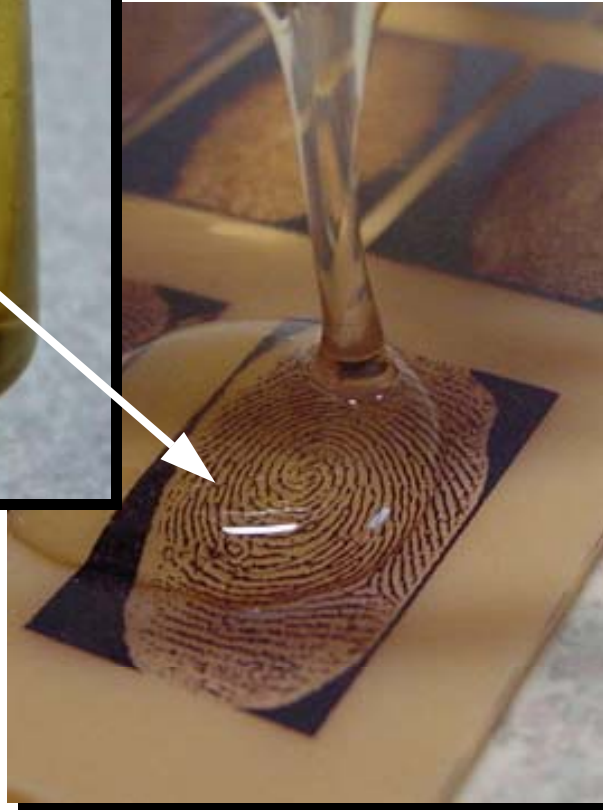**A Mask with Fingerprint Images**
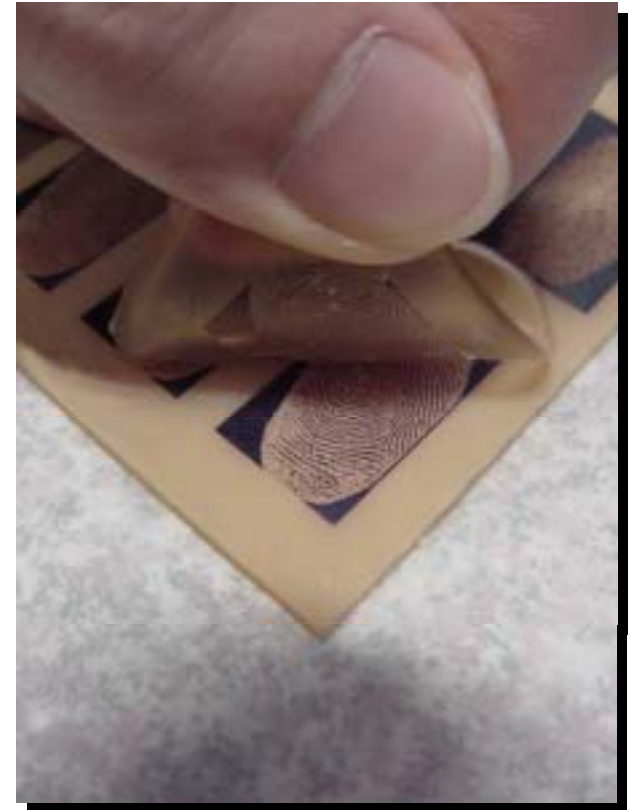
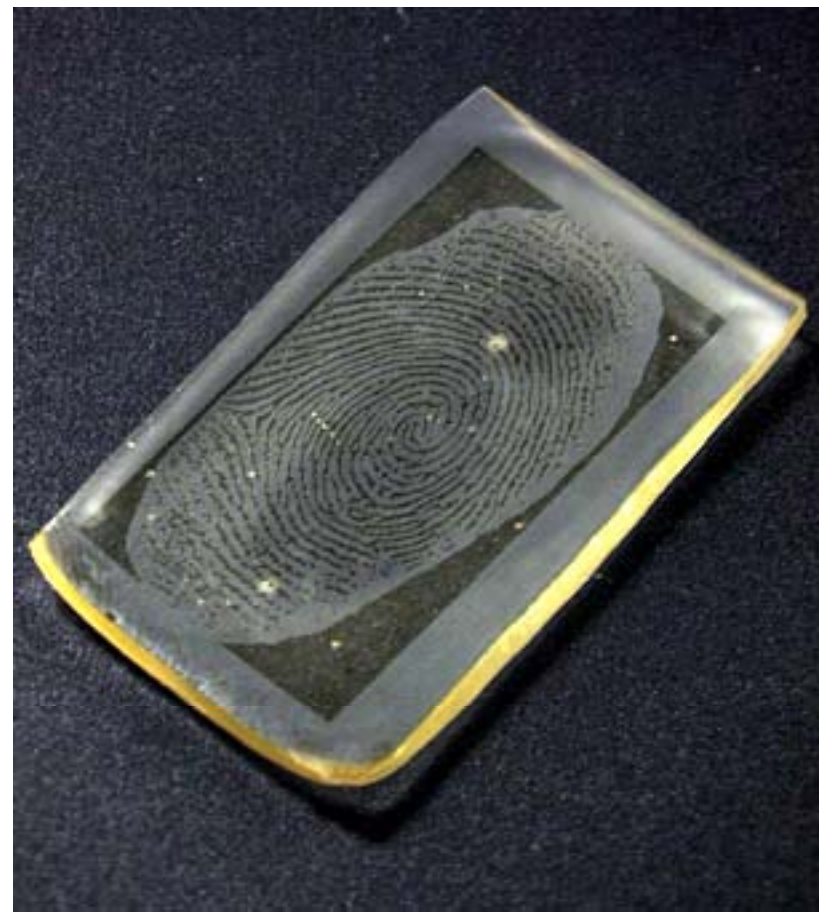**An Enhanced Fingerprint**   **A Fingerprint Image**

Gelatin Liquid

40wt.%

Drip the liquid onto the mold.

Put this mold into a refrigerator to cool, and then peel carefully.

Mold: 70JPY/piece
(Ten molds can be obtained
in the PCB.)

Gummy Finger: 50JPY/piece

Pores can be observed.

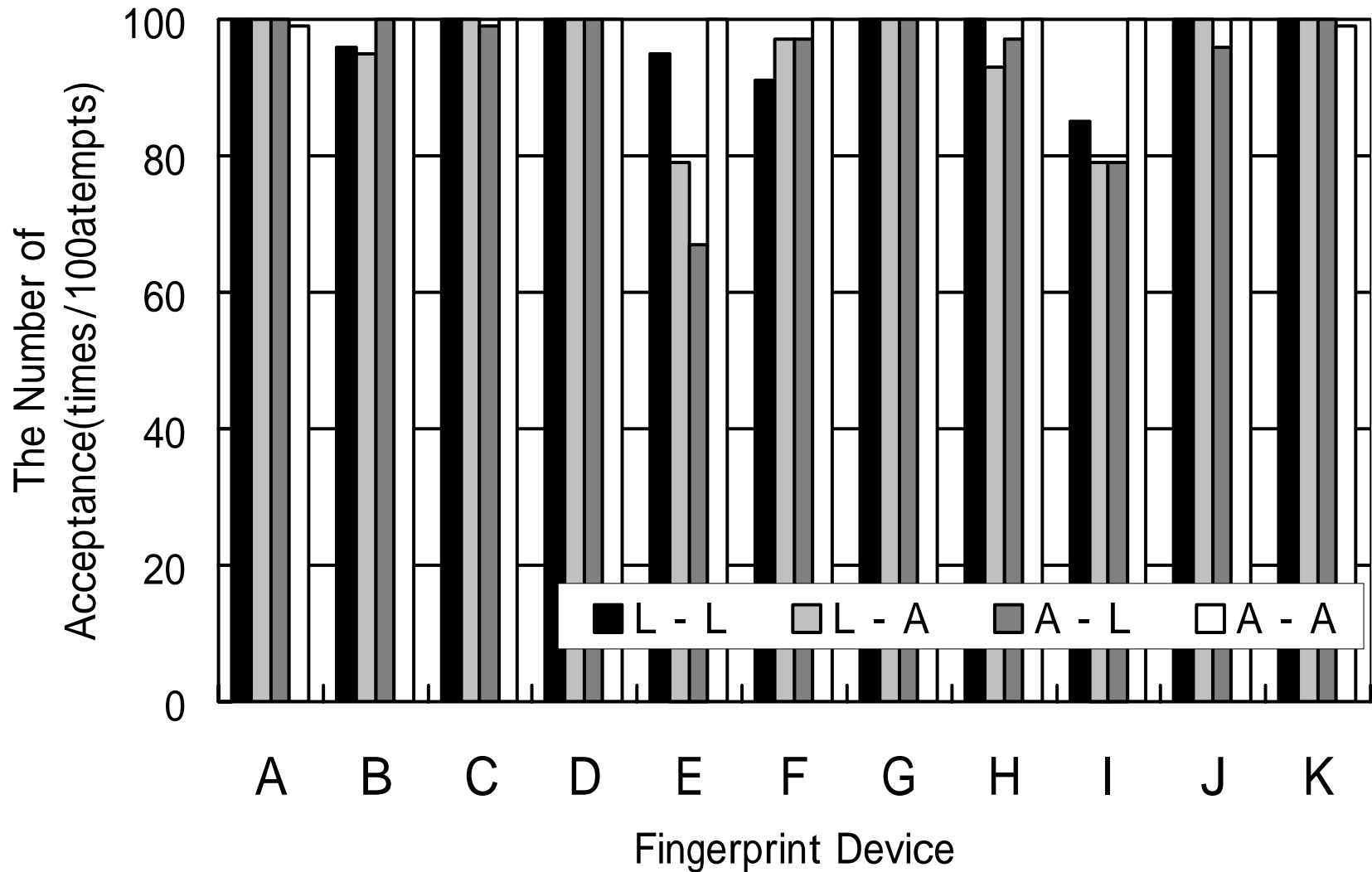**Enhanced Fingerprint**

**Captured Fingerprint Image of
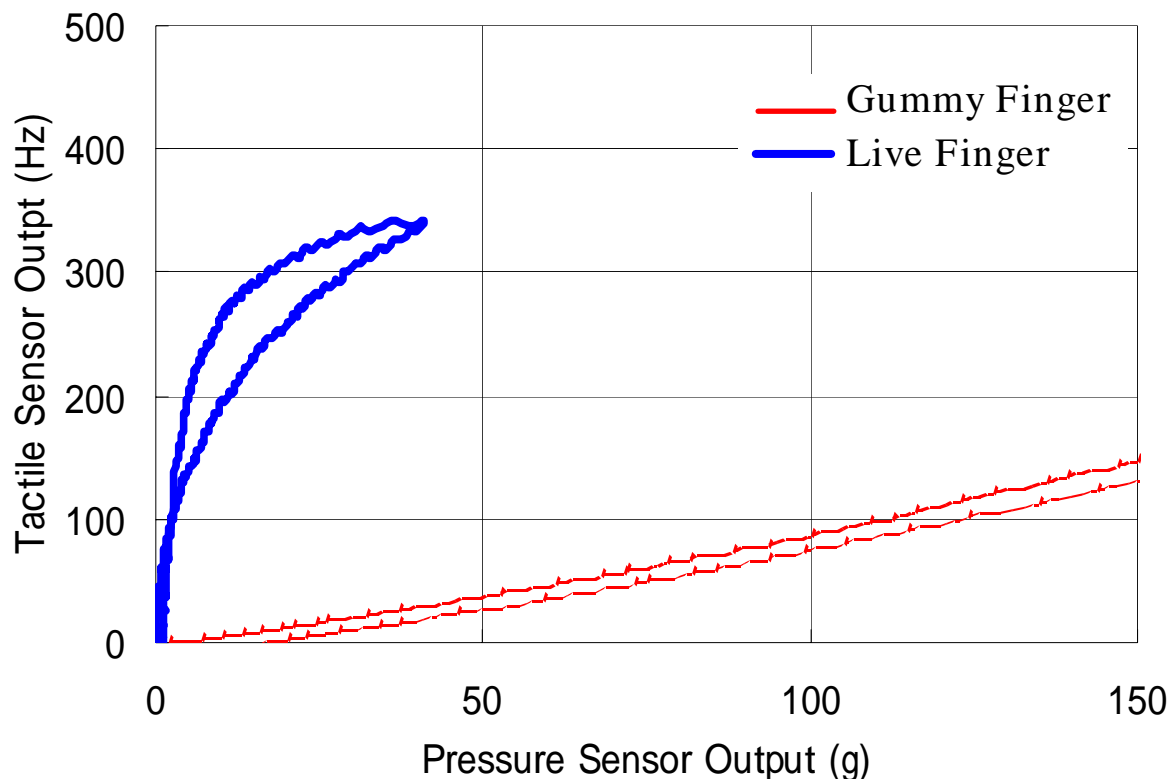the Gummy Finger
with the device H (a capacitive sensor)**

from Residual Fingerprints (for 1 subject)

The Number of Acceptance(times/100atempts) vs Fingerprint Device (A–K)

Legend: ■ L - L ▫ L - A ▨ A - L ☐ A - A

Characteristics of Gummy Fingers

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

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

- *There can be various dishonest acts using artificial fingers against the fingerprint systems.*

- *Gummy fingers, which are easy to make with cheep, easily obtainable tools and materials, can be accepted by 11 types of fingerprint systems.*

- *The experimental study on the gummy fingers will have considerable impact on security assessment of fingerprint systems.*

- *Manufacturers,vendors, and users of biometric systems should carefully examine security of their system against artificial clones.*

- *How to treat such information should be an important issue.*

- *Paper:*

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.

- *Send any comments to*

  tsutomu@mlab.jks.ynu.ac.jp

Yokohama Nat. Univ.
Matsumoto Laboratory