Managing Director
Retail and Commercial Banking

9th Floor
Standard Bank Centre
5 Simmonds Street
Johannesburg
2001

PO Box 7725
Johannesburg 2000
Fax (011) 492-1270
Telephone (011) 636-6065
(011) 636-9111

Professor F.B. Schreiber, Ph.D.
Editor & Publisher
Crime & Security Newsletter
26720 Highway 169
Zimmerman, MN 55398

18 July 1995

Dear Professor Schreiber,

Thank you for your letter of 14 June 1995 as well as the enclosed back issues of ATM Crime and Security newsletter which have been passed on to the relevant people in our organisation for information. The newsletters certainly highlight that we are not alone in terms of our ATM security problems.

Details in respect of the issues you have expressed an interest in are outlined below:

1. **ATM Biometric Identification**

We are still in the process of investigating the possibility of using ATM fingerprint identification. User acceptance testing is in the final stages and a few pilot sites will be installed during August for evaluation. Briefly the system operates, as follows:

- Two fingerprints are stored for each customer on a memory chip card. The application controls the quality of prints enrolled and rejects those not up to certain standards.

- A video camera is integrated to allow enrolment of facial image which is also stored on the card.

- A biometric scanner is integrated into the ATM fascia panel as per photographs attached.

- The system allows for the customer to choose between PIN or biometric verification, in both cases the customer image is stored.

- A number of maintenance functions for re-enrolment, access control and housekeeping functions have also been developed.

2/ ...

- The enrolment function is completed after an account is opened for the customer and an ATM card has been instantly issued.

- Upon insertion of the ATM card, the system extracts the details from the memory chip and displays the customers name as well as a facial image.

- Dependent on the customer's choice, the customer is requested to either enter their PIN or commence biometric verification.

- A graphic image displayed on the screen directs the customer how to proceed.

- If verification is successful the customer proceeds with the transaction as normal.

- After three unsuccessful attempts with the first finger, the system requests the customer to try the second finger. In the event that both fingers are unsuccessful the customer will be referred to the branch who will verify the enrolment.

- The facility will at this stage not be available on ATM's in an unattended environment.

We have selected a fingerprint verification biometric scanner known as Startek for experimental purposes and a pamphlet describing its features is attached for your interest.

2. **ATM Crime**

The South African banking industry has experienced an upsurge in ATM Crime, on several fronts, over the past few years. As a point of reference and on a collective and national basis, our industry has in the region of 5 500 ATM's installed at 3 000 sites. Approximately 70% of the sites are located in major metropolitan areas. The main areas of concern include:

- **ATM Attacks**

  On an industry wide basis we have experienced a steady growth in physical attacks on ATM cash compartments since 1992. Criminals invariably use angle-grinders or oxy-acetylene torches to cut the machines open.

  70 incidents with cash losses amounting to USD 1.1 million were experienced countrywide in 1994. In the six month period ending 30 June 1995 there have been 62 incidents with losses of USD 770 000. 30% of the incidents are unsuccessful attempts.

  The losses referred to exclude loss of revenue as well as customer frustration due to downtime, and the cost of repairing damaged machines.

  Our protection efforts have been focused on the installation of upgraded intruder detection systems and purpose designed safe enclosures, which we developed in collaboration with a local safe manufacturer. I should mention that the measures implemented by ourselves have resulted in a 52% reduction in our incidents and a concomitant reduction in losses.

Several photographs of ATM's which have been attacks together with the safe enclosures used by ourselves are enclosed for interest.

- **ATM Card Swopping**

We are experiencing a growing trend involving "confidence tricksters" operating at ATM's. By sleight of hand and distraction tactics they manage to swop ATM users cards (just as the card is ejected from the machine and after observing customers key in their pin number). Within minutes amounts are drawn from customers accounts. It may be days before a customer is aware that his or her card has been swopped.

For a number of practical reasons quantitative information relating to the frequencies of these occurrences is unfortunately not available.

Initiatives taken to combating this growing trend include:

* Customer vigilance and awareness campaigns via electronic and print media, screen message displays and posters at sites.

* Selective deployment of security guards at sites.

* Pilot installation of privacy screening.

* Use of surveillance camera's and teams (who have been successful in arresting perpetrators).

* Self selection of daily withdrawal limits.

* Introduction of an "autostop" card. Following commission of a crime (such as mugging) customers can prevent any further withdrawals by inserting a second card into any ATM which places a stop on their account.

* Re-design of a more concealed pin pad.

* Introduction of an ATM crime information reward scheme.

* Installation of telephones linked to the Police.

* Regular liaison with law enforcement authorities to focus attention on troublesome location.

* A number of ongoing systems developments, such as, biometric identification and restricted time window from last withdrawal.

Although customer muggings occur from time to time, incidents of this nature are relatively infrequent.

ATM Card Reader Vandalism

Card swoppers often take ATM's out of service by jamming card readers with paper, matches or glue.

Their intention is to channel customers to less secure ATM sites where swopping of cards is easier. The irony of this situation is the more vandalism one has, the greater comfort there is in knowing your sites are more secure and not targets for card swopping!!

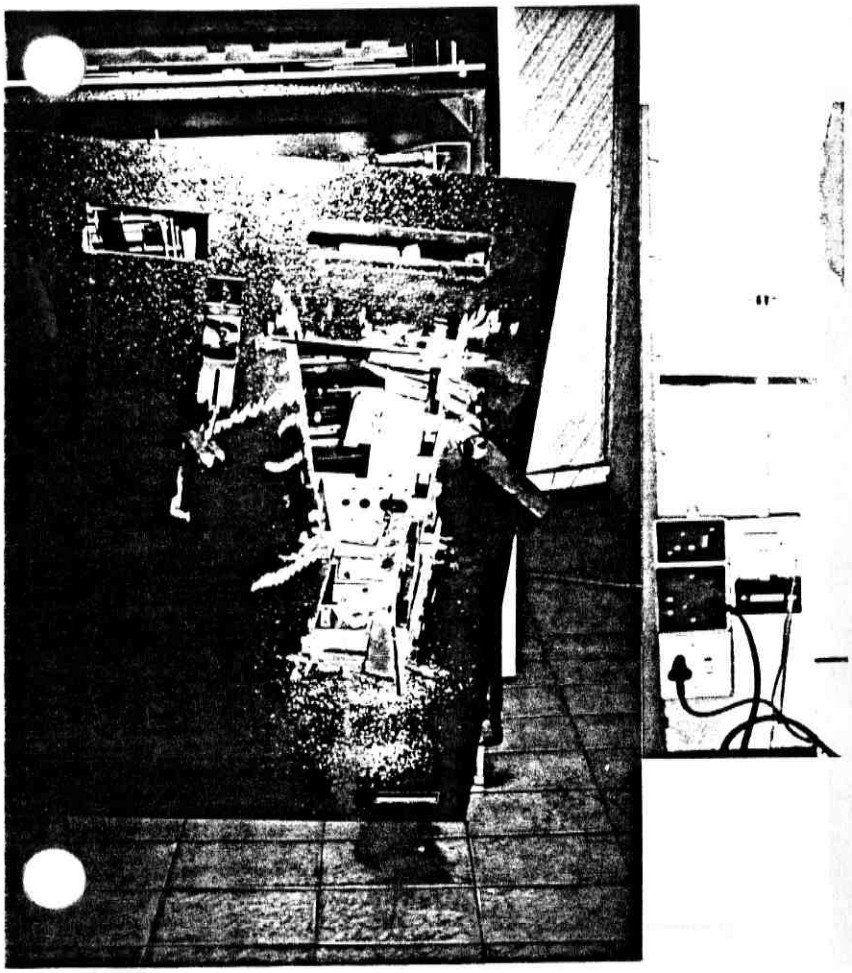
Once again, thank you for the interest shown in our local environment and I trust that the information provided will be of assistance to you.

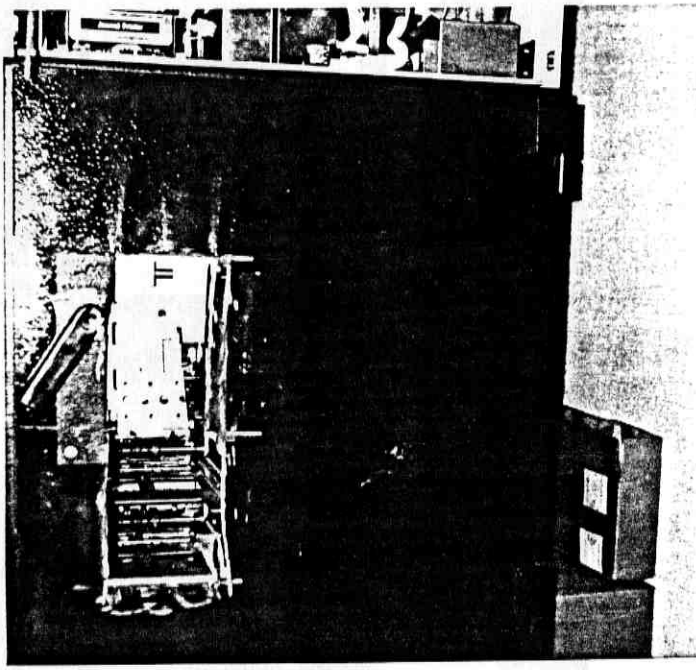
Kind regards,

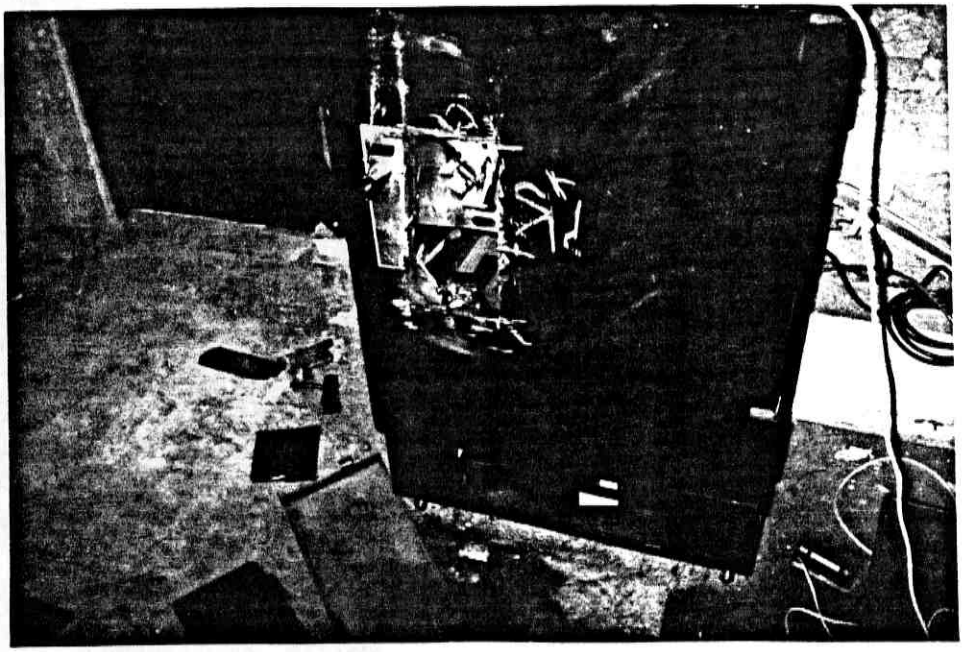
Yours sincerely,

D.R. Busse

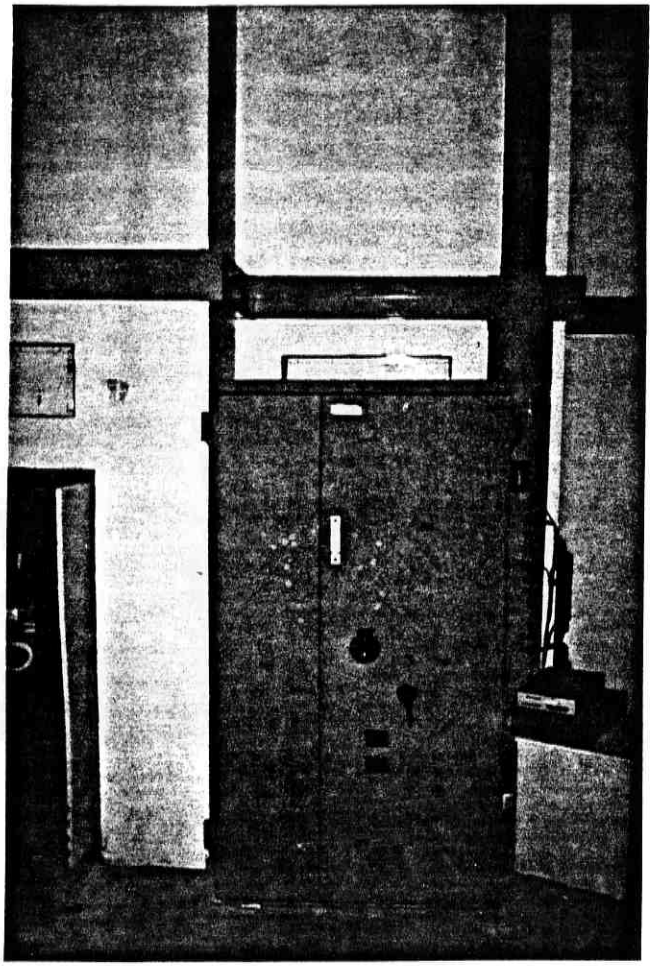
ATM PHYSICAL ATTACKS



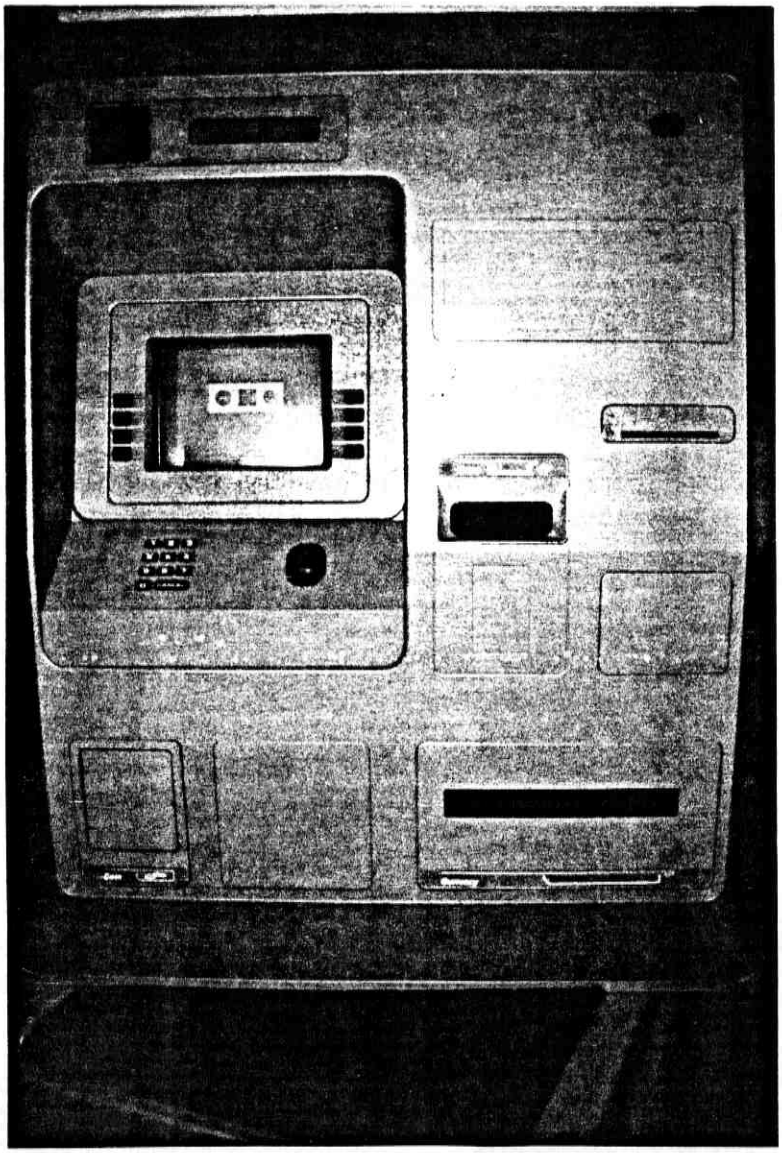


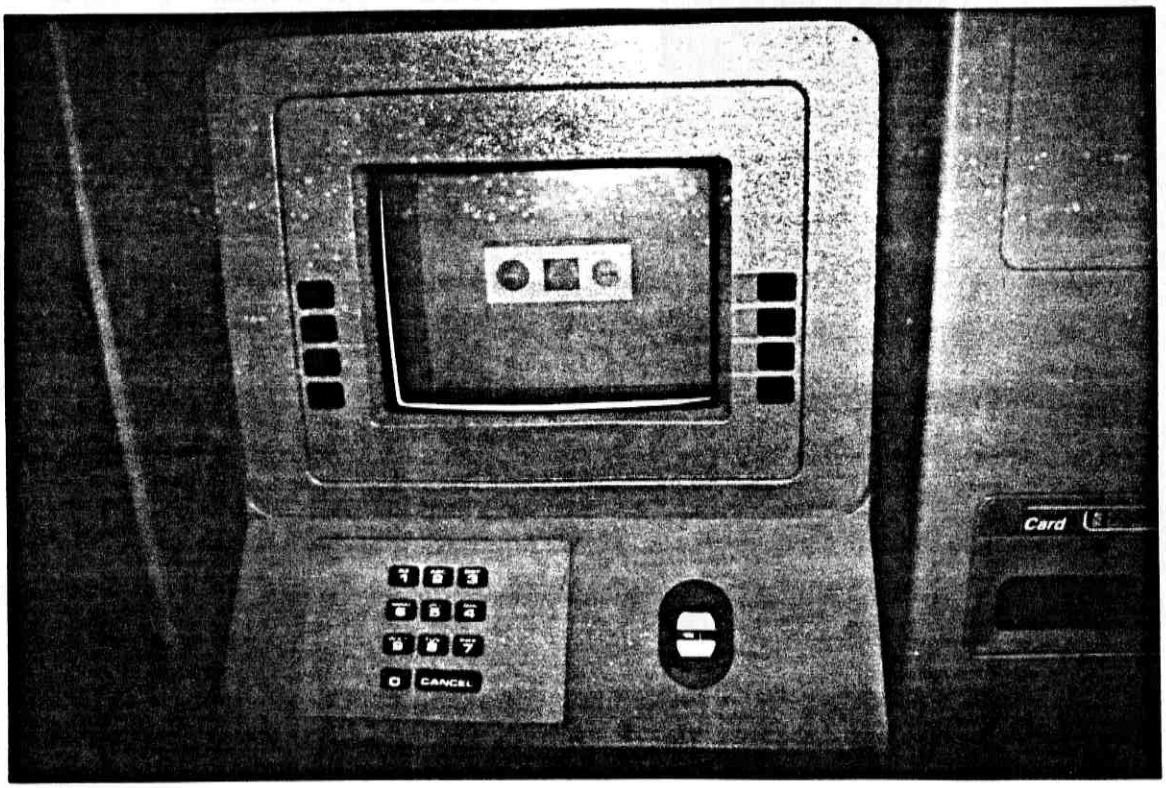


ATM ENCLOSURES



BIOMETRIC SCANNER INTEGRATED INTO THE ATM FASCIA





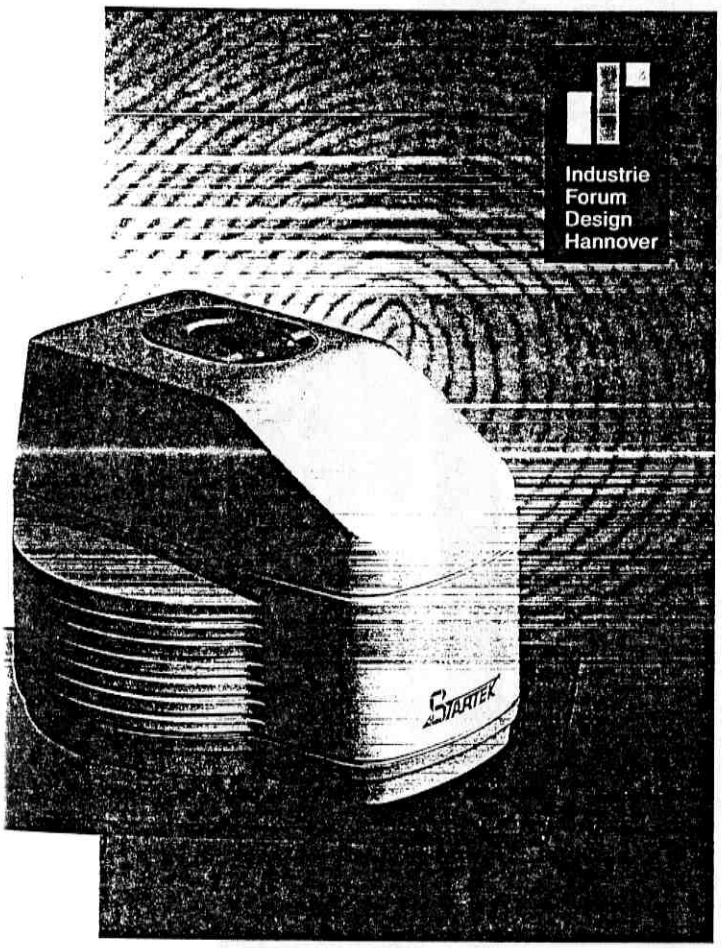
FingerCheck

Fingerprint Verifier FC100

IDEA

FingerCheck fingerprint verifier makes use of the unique and unchangeable characteristics of personal fingerprints to provide highly accurate identity verification by means of comparing the live-scan fingerprint captured by the fingerprint reader with the one previously enrolled into the computer system.

FingerCheck fingerprint verifier, FC100 provides a PC AT-BUS interface card to be integrated into IBM or compatible PCs or embedded control systems.
It provides a variety of applications based on the fingerprint recognition technology.



TECHNOLOGY

STARTEK ENG. INC. uses the technologies developed by professor Wen Hsing Hsu of National TSING HUA University, Taiwan, to commercialize the fingerprint recognition product series.

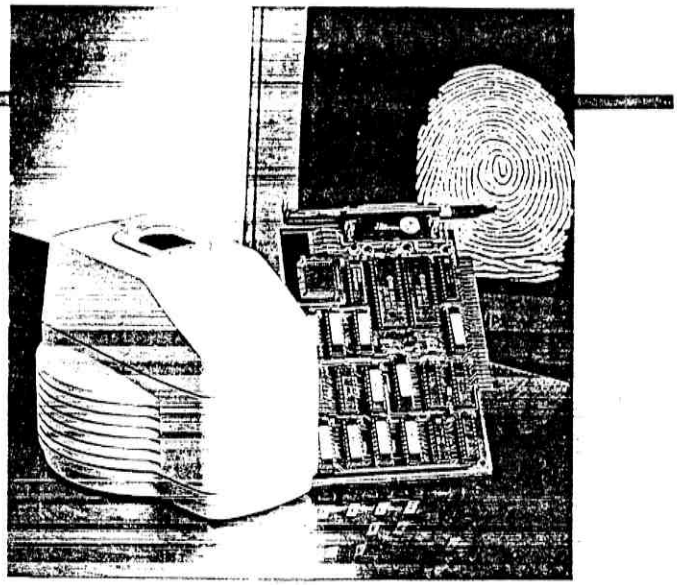
- Device and Technique for Binary Image Thinning and Feature Extracting.
- Method and Device for Allocating Core Points of Fingerprints.
- Automatic Planar Point Pattern Matching Method and Device.
- Method for Determining Background for Object Pixel of Digitized Image Data.

FEATURES

- The optical system of FingerCheck fingerprint reader rejects counterfeited fingerprints duplicated in any way when used to access the system.
- FingerCheck fingerprint reader provides true replica pictures of live-scan fingerprints when connected to a computer and printer.
- The features of each live-scan fingerprint are extracted into a minutia file for matching, and the size of each minutia file is only 256 bytes. This reduces the requirements for database management.
- Due to the small size of the minutia file for matching, the fingerprint data can be stored on card systems (like smart cards, optical cards). This allows one-on-one matching between a live-scan fingerprint from fingerprint reader and the fingerprint data on the card.
- FingerCheck fingerprint verifier takes only 2-3 seconds for one-on-one matching (with computing power of IBM PC-386SX-33). This provides high speed for identity verification.
- The False Rejection Rate (FRR) of the matching mode is less than 1%. This provides easy-to-use features.
- The False Acceptance Rate (FAR) of the matching mode is less than 1/100,000. This avoids the possibility of a ghost writer tremendously. (fingerprint plus password provides double security)

Fingerprint Verifier FC100

FingerCheck



APPLICATIONS

FingerCheck fingerprint verifier can be integrated with computers or embedded control systems for the following market segments with fingerprint recognition technology.

- Medical & Insurance Industry
- Banking Industry
- Government Projects
- Education

Typical applications are:

- Database management systems with fingerprints.
- Computer access or transaction control.
- Computer database security control.
- Physical access control by connecting FingerCheck fingerprint verifier with control circuitry to activate door locks (stand-alone system). The stand-alone system can be connected to a computer network to perform other functions such as event recording and communications for management (network type system).
- For law enforcement applications, the FingerCheck fingerprint verifier can work with card systems, such as smart cards and optical cards, to perform identity verification. It provides social welfare security by using cards such as an ID card, drivers license, passport, credit card and so on.

CUSTOM DESIGN FOR OEM CONFIGURATION IS AVAILABLE

Custom design configurations for integrating the FingerCheck fingerprint verifier into any hardware or software system are welcome.
Please contact the sales & marketing department of STARTEK ENG. INC.

Specifications:

Field Size	22mm(H) x 24mm(V)
Image Resolution	512 x 480 pixels
Gray Level	256 levels (8 bits/pixel)
Minutia File Size	256 bytes
Scanning Speed	1/30 second
Matching Speed	2-3 seconds (computing power of IBM PC/386SX-33)
False Rejection	less than 1% (matching mode)
False Acceptance	less than 1/100,000 (matching mode)
Hardware Interface	IBM PC Interface Card
Height	122mm
Width	130mm
Depth	155mm
Weight	950g (Reader only)
Power Consumption	+5V 1.5A, +12V 600mA, -12V 1mA
Functions of S/W API (application interface)	• Image Capture • Enrollment • Matching

* Specifications are subject to change without notice.

STARTEK

STARTEK ENG. INC.

3F, No. 54, Park Ave II, Science-Based Industrial Park,
Hsinchu 300, Taiwan, R.O.C.
TEL : 886-35-785388 FAX : 886-35-787089