. When matching between input fingerprint and the encrypted one, it executes file decryption automatically.

3. Administrative Function

Only the user who is not an administrator can't implement "Administrative
Tools".

3.1 Implement of Administrative Tools
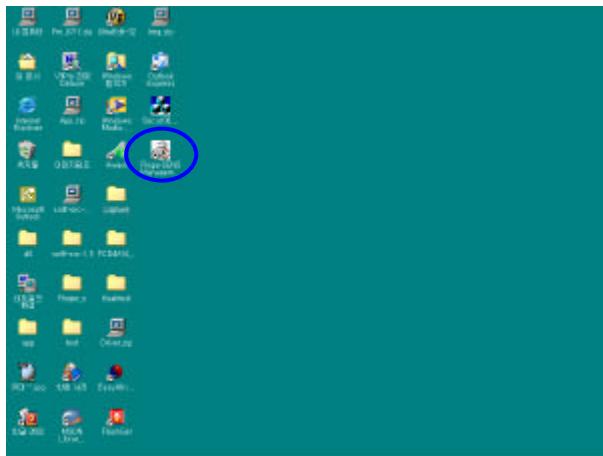
Figure 34) Administrative Tool Program

. Click [icon] icon on the desktop or click "Start->Program->SecuIT-
>Administrative tools".

. Only the user who is enrolled as administrator can implement
"Administrative Tools" program.

Figure 35) Verification of Administrator

. Once "Administrative Tools" program starts, administrator authentication
  screen is displayed.

. If administrator's input fingerprint and the registered fingerprint match, you
  are verified.

. When you click [ID/PW] button, it's proceeding is just same as like

clicking ID/PW button in windows logon administration.

Figure 36) Inputting ID/PW

． Upon verification, any menu in the "Administrative Tools" program is set

to be used (Figure 37).

Figure 37) Administrative Tools

## 3.2 Implementation of "User management"
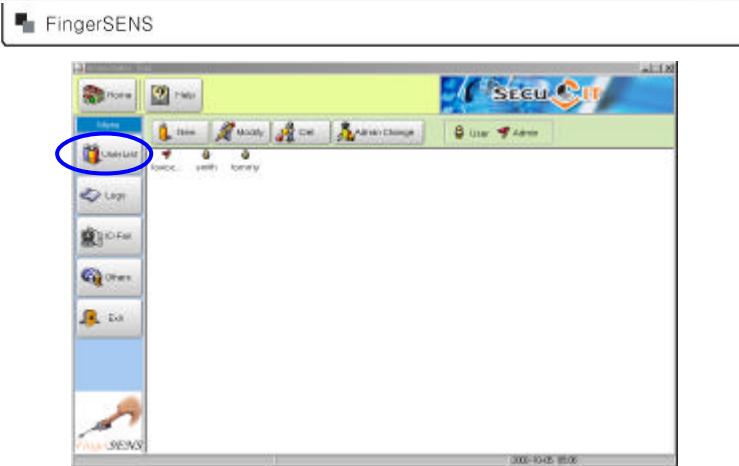
Figure 38) Administrative Tools "User management"

. If click [██████] button, it is able to check the enrollees (Figure 34).

. If click [██ New] button, it is able to enroll other users additionally.

. If click [██ Modify] button, it is able to modify the information of enrolled users.

. If click [██ Del] button, it is able to delete the enrolled users.

. If click [██ Admin Change] button, it is able to change the administrator.

3.2.1 Enrolling Users
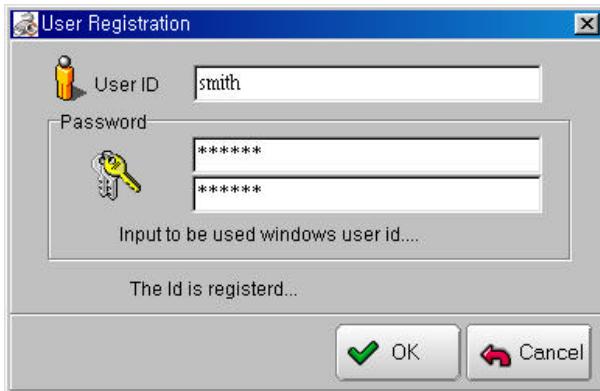
Figure 39) User Enrollment

ᕀ   Click 🔩 New button, and "User Enrollment" dialog is displayed.

ᕀ   After entering ID and Password for enrolling in the user enrollment

window and click ✔ OK button to save.
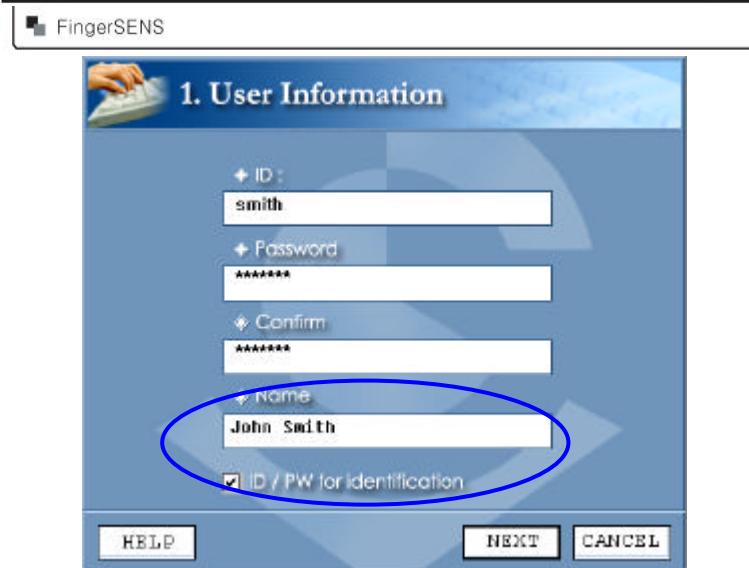
Figure 40) User Information

. The screen (Figure 40) is to choose running parallel ID/PW identification
with fingerprint verification and is to confirm user name.

. Type in user name and click [Next] button.

. ID/PW are providing against the fingerprint verification failure. Don't let
another person know about your ID/PW.

> . ID and Password are automatically filled in as typed in (Figure
> 40).

. Password must be within the range of 1 . 31 characters. A warning is

shown if it is beyond the range.

˙ Retype a password in accordance with the form required in the program and click ⌷ Next ⌷ button.

˙ Click ⌷ Next ⌷ button, and the input screen for user registration appears. You must check beforehand whether the fingerprint sensor is connected to the PC.

Figure 41) Inputting User Fingerprint

.Input the corresponding fingerprint on the sensor 3 times and then select the

finger you want to register.

.You must input your fingerprint on the sensor first and then

select the finger from the graphic below. (Figure 41)

.The color of the selected finger changes into pink. You should

check it first and then input your fingerprint.
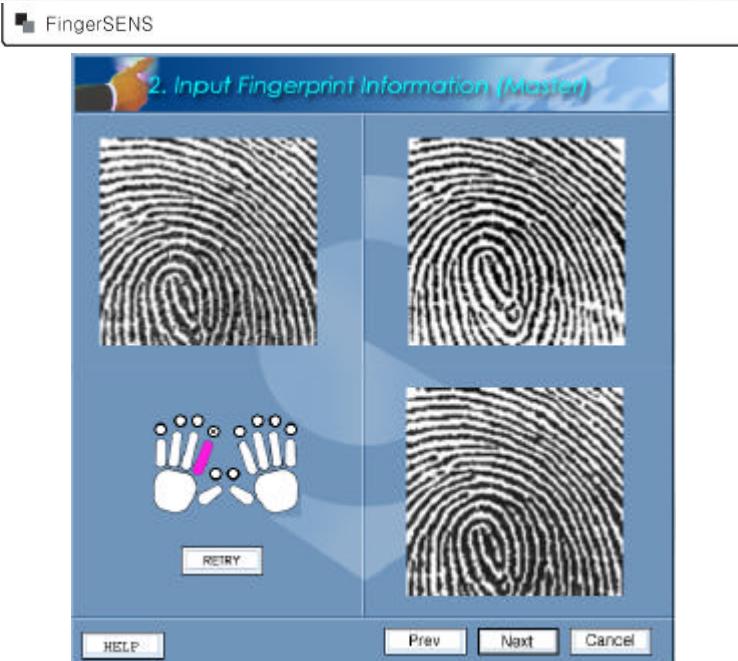
Figure 42) Completion of Inputting User Fingerprint

．The inputted 3 fingerprint images through fingerprint sensor appear
　(Figure 42).

．If you try to input fingerprints again, just click [RETRY] and repeat the
　process from ．in the same order.

．After checking the print images, click [Next] button to save them.
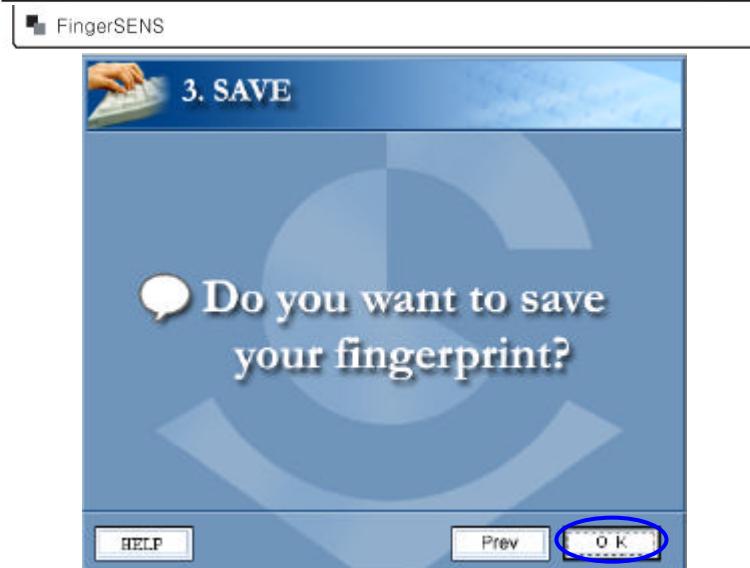
Figure 43) Completion of saving user's fingerprints

‚ Click [O K] button, saving of user's information and fingerprint is

done.
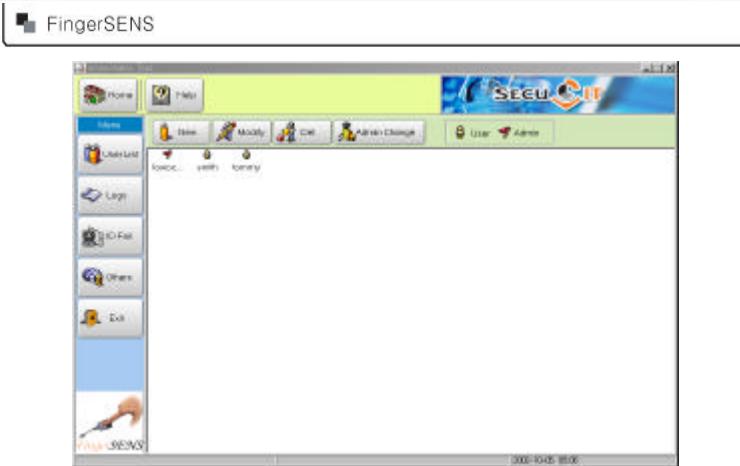
Figure 44) Confirmation of the enrollee

. After finishing user registration, you can confirm who registered by clicking

the "user administration" in the menu (Figure 44).

. Windows 2000 User Enrollment

In Windows 2000 case, when enroll user, it is in need of additional work.

Obviously have to enroll user first in Windows 2000 and then add the user registration in administrative tools by the enrolled user ID and password.

. In time of only user registration in administrative tools without user enrollment in Windows 2000, the users can not logon their PC. Please, be noticed.

. Select user and password in windows control pad.
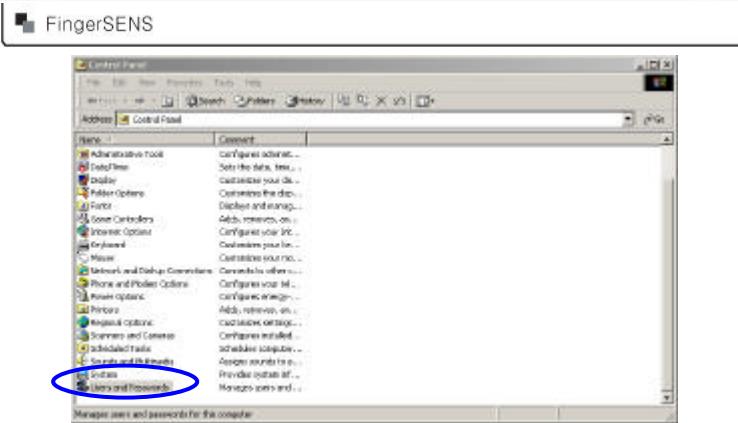
■ FingerSENS

˙ Click [ADD…]("Addition") button.
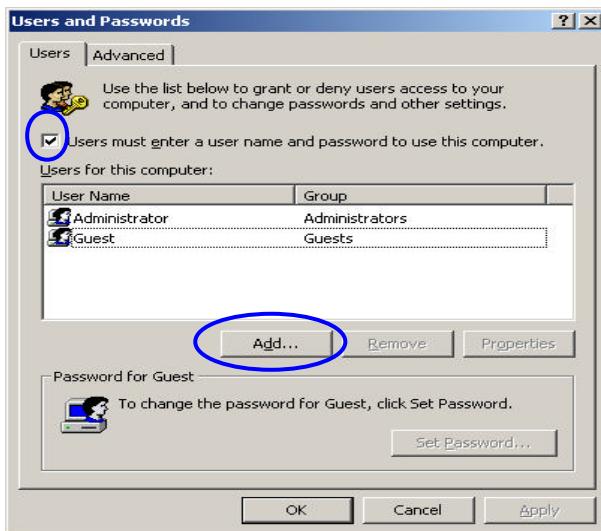
˙ Enter the basic information and ID for the new user.

FingerSENS

. Type a password for the new user.
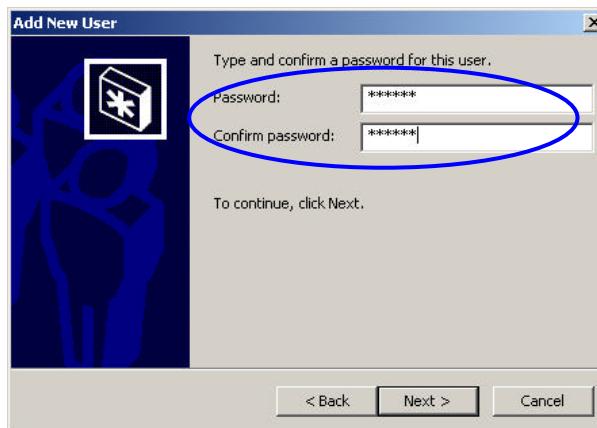
. Assign user's the level of access to grant.
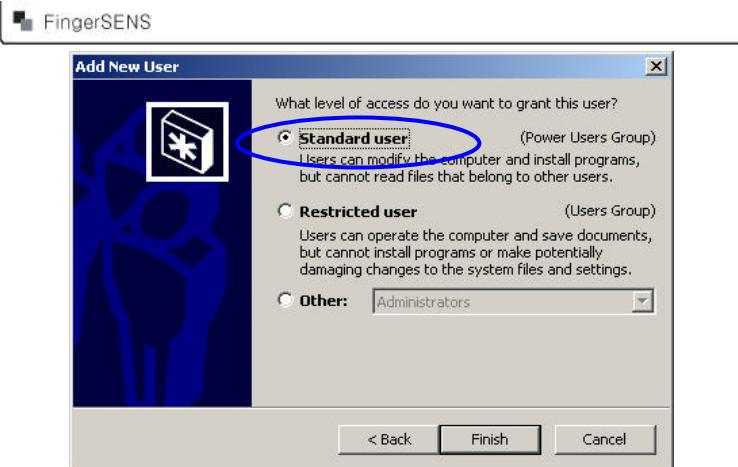
. Confirm whether input the information for user is good or not.
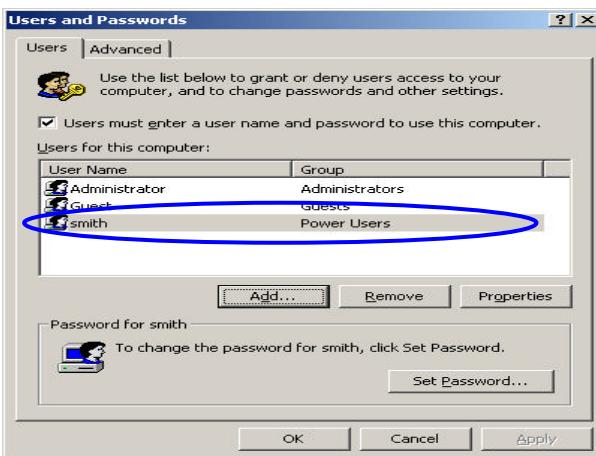
. Click [New] button in the administrative tools menu, the window for user's enrollment appears.
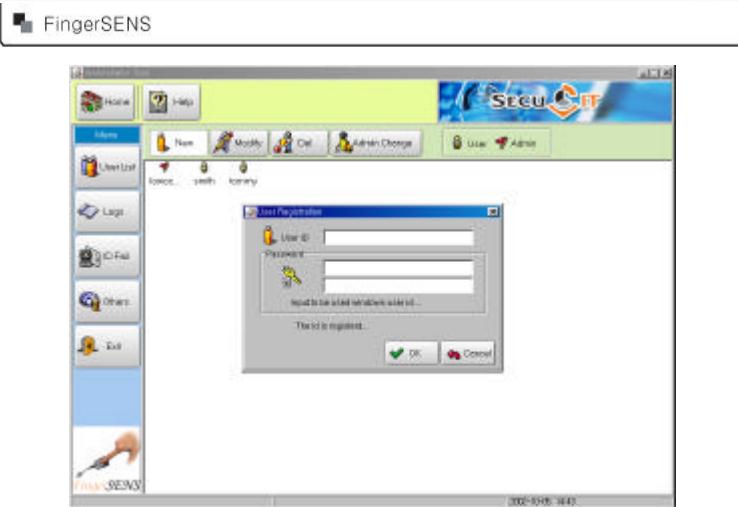
. After entering ID and Password for the new user, click ![OK] button. But, in Windows 2000 case, user ID and Password are just same with the added user ID and Password in windows 2000. Otherwise, you can not use program functions as Windows logon and so on. Please, be noticed.

FingerSENS
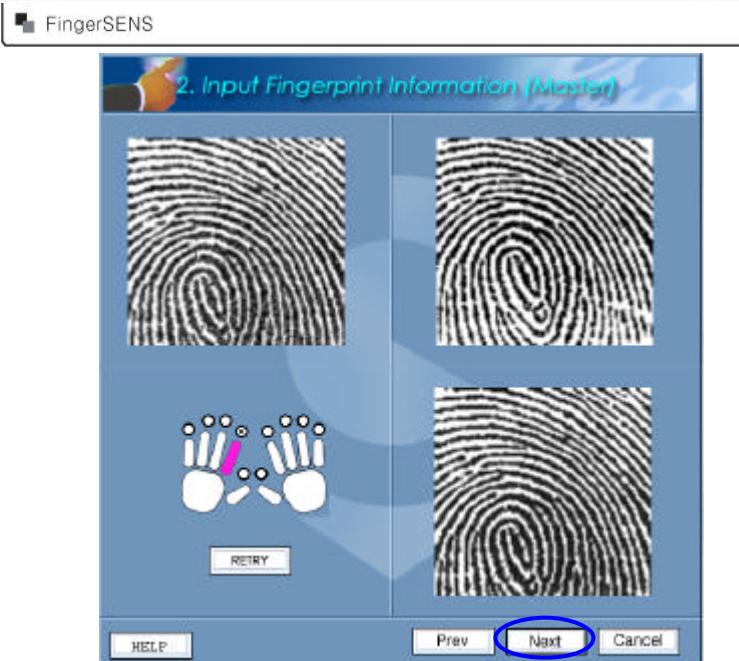
Figure 45) Inputting User's Fingerprints

ㆍSave inputted ID and Password, and the screen for user's fingerprint input

appears.

Figure 46) Completion of registration

ㆍIf click [O K] button, the inputted user's information and fingerprint are saved.

3.2.2 Modification of User Information

. Select a user you want to modify in the administrative tools program and click ![Modify].
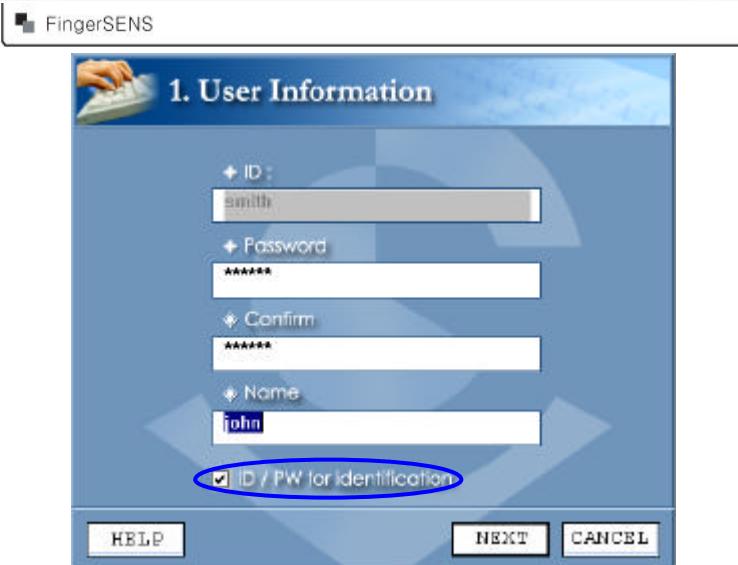
Figure 47) Modifying User Information

﹒   After modifying a user ID and Password, click Next button.

﹒ID & PW are providing against the fingerprint verification failure. Instead

of the fingerprint verification, you can use ID & PW.

Figure 48) Modifying User's Fingerprint

·   Proceed the same procedure just as you did in registration.

·Among the process of input 3 times, when you input your fingerprint each

    time, take on and off your finger repeatedly.
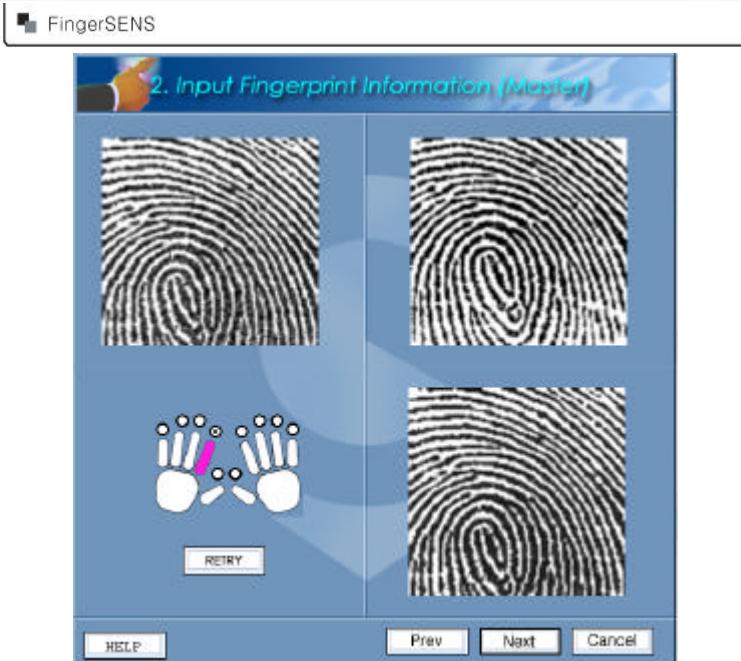
Figure 49) Completion of Inputting the modified user prints

. After inputting fingerprints 3 times, click Next button .
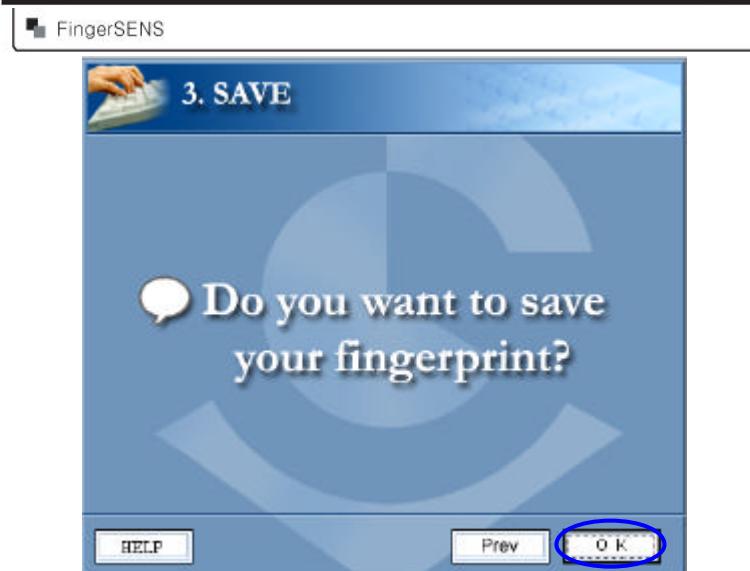
Figure 50) Completion of modifying user information

. If the process of input is correct, click [OK] button to save modified

information.

3.2.3 Deleting a User

Figure 51) Deleting a User

˙ Select a corresponding user in the "Administrative management" and click

 button.
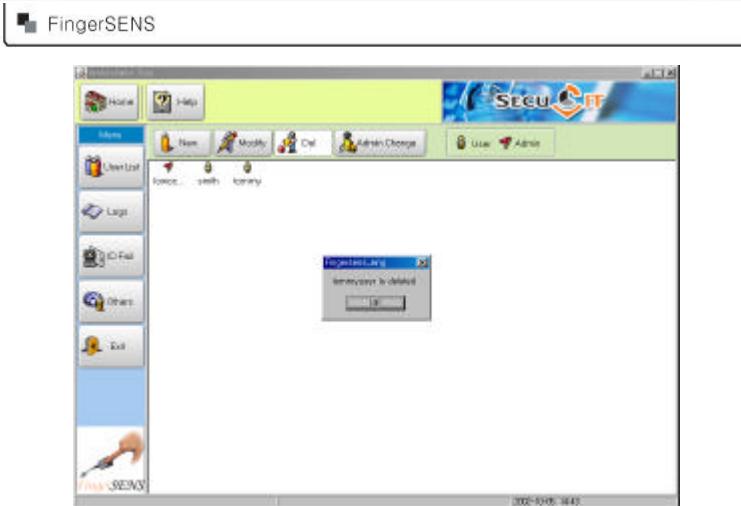
Figure 52) Completion of Deleting a User
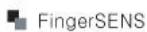
3.2.4　Switching administrator
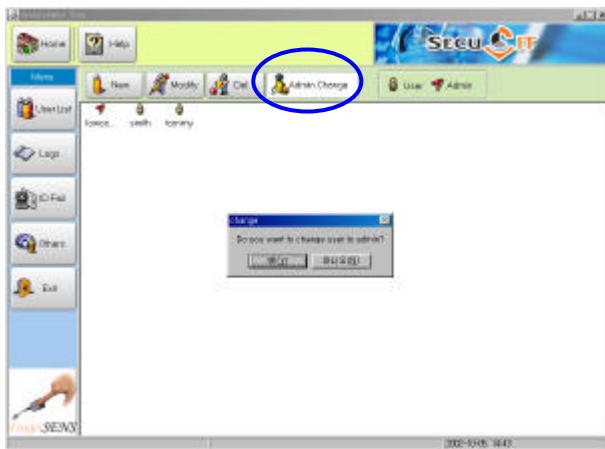
Figure 53) Switching administrator

、　It transfers the administrator rights to one of the users from the current administrator. To do so, select user1 and click [Admin Change] button. (The current administrator is shown as red flag icon)
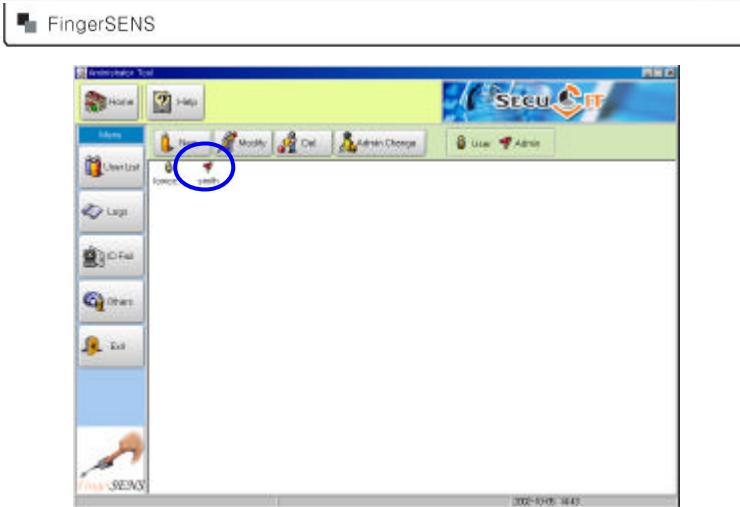
Figure 54) Completion of switching administrator

˚ After switching the administrator, you can verify it as like (Figure 54).

3.3 Log Management

You can see the result of user verification, date, time, work list, log type,

user list and so on in the log management.

Figure 55) Log Management

. If you click [Logs] button, the screen which is what each users do comes up like (Figure 55).
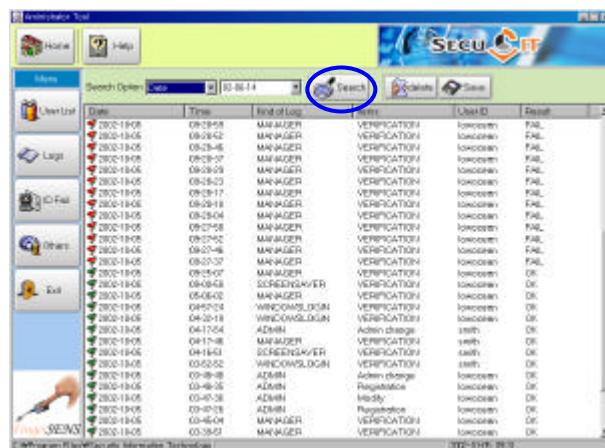
Figure 56) Log Management Search

• As (Figure 56), the search condition is "date", "user" and "work type". You may input search word in search condition, and then click [Search] button.

3.3.1 Log Management - Deletion
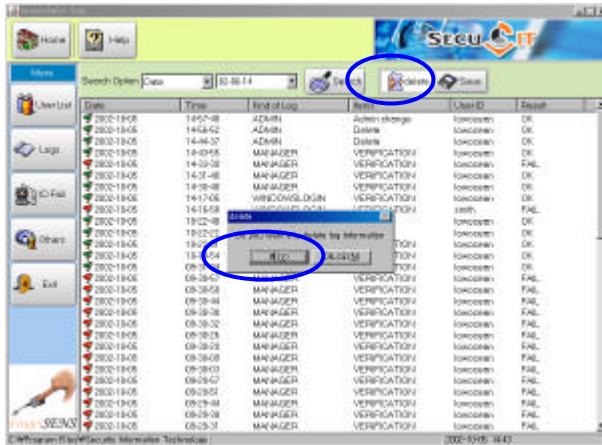
Figure 57-1) Log Management-Deletion

. Click a log file you want to delete in the list.

. Click ![delete] button in the menu above and ![button] button in the dialog
box. Then the log information is deleted

> . You just deleted information that is shown on the screen.
> If you want to replace the new log file with the current
> list, you have to choose "Save" in the menu above.

3.3.2 Log management-Save
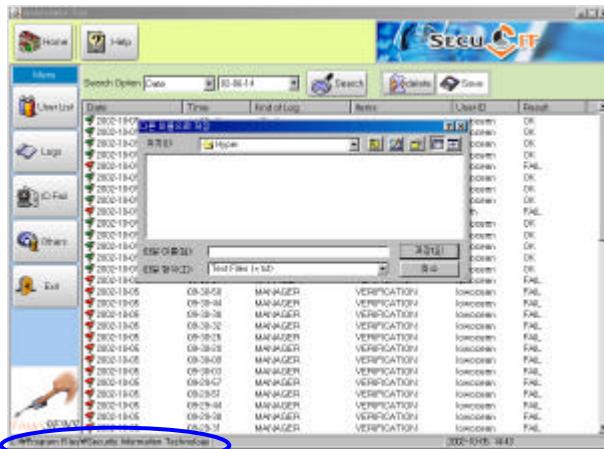
Figure 57-2) Log Management-Save

. The log information on the screen is being saved as text file.

. If you want to change log information which is in current list, you save the

   file into path routine which is in the left bottom of the screen and then log

   information will be changed current list.

3.4 Verification Failure Management

Each user's verification failure fingerprint will be managed separately. Each user information and fingerprint will be saved automatically, so you can check who tries to access the PC.
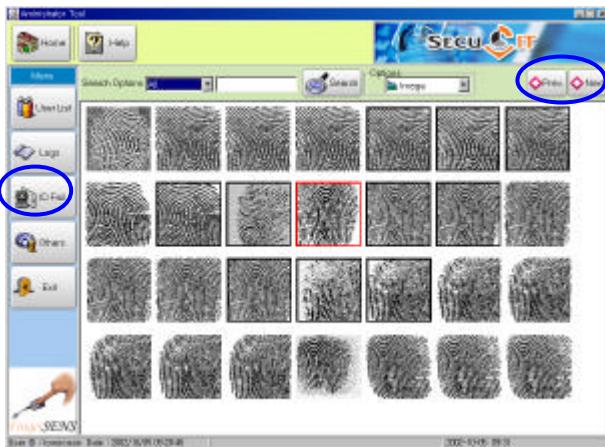
Figure 58) Verification Failure Management

- When you click ![button] button in the "Administrative Tools", you can see failed fingerprint images (Figure 58).

- When you drag mouse onto the fingerprint image, there appear a failed user's ID and the time user tried.

- Next/Prev. : Searched fingerprints are over 28, this button is activated.

- If you have double click the fingerprint image, you can see detailed information.

FingerSENS

3.4.1 Verification Failure Management – Viewing Images

? Popup Menu

Figure 59-1) Verification Failure-Viewing Images-Popup Menu

If you click the right button of the mouse on the fingerprint which you want
to see, popup menu appear.

. Zoom in (detail view) : Shows enlarged image and information of the
image.(Double-clicking an image has the same effect)

. Save as : Selected image is saved in bmp file.
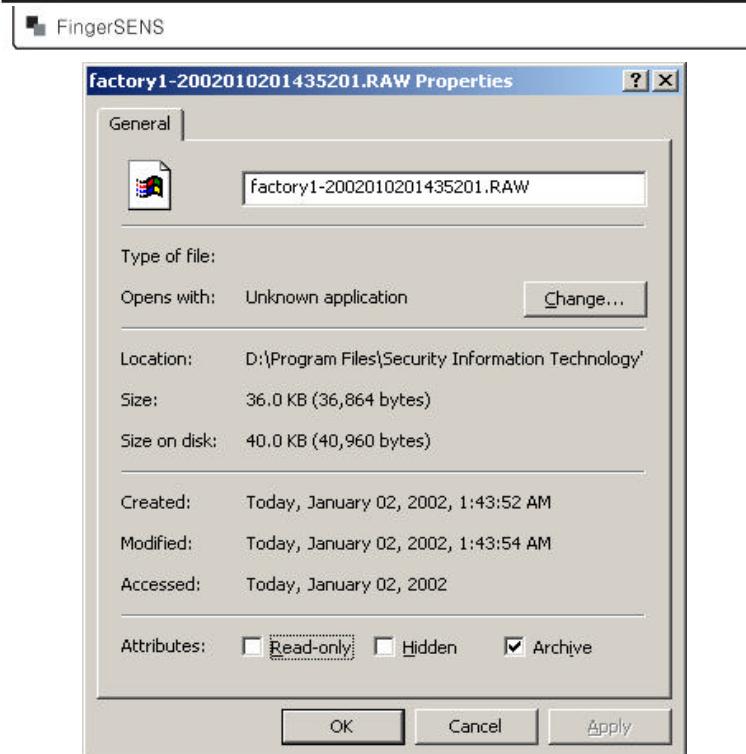
Figure 59-2) Properties

˳ Properties : Show the information of the chosen image via Windows

Properties screen.

˳ Fingerprint and information which are failed in verification can

be used to trace data some who try to access illegal.
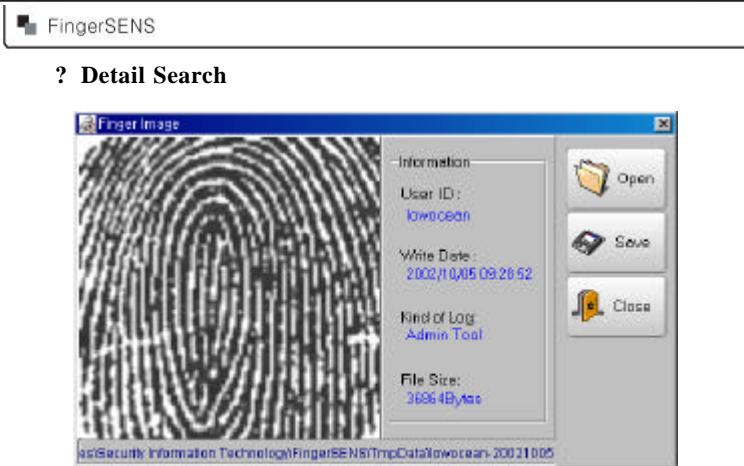
? Detail Search

Figure 59-3) Detail Search

. [Open] : Display the selected raw image file.

. [Save] : Saves the current image as bmp file.

? Search

Figure 59-4) Search

˙All : Shows all failed fingerprint images.

˙User : Shows the failed fingerprint image when you enter a user name who
failed verification.

˙Date : Shows the failed fingerprint image that were input on the particular
date.

? Verification Failure Management-Viewing List

Figure 59-5) Viewing List

- The list above shows the detailed information of the failed fingerprints.

- When you double-click an item in the list, the detail view screen (Figure 59-3) appears.

? Popup Menu
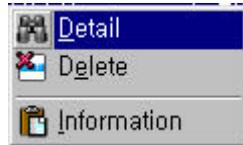
Figure 59-6) Popup Menu

- Detail : Select the file and detailed information appears as like (Figure 59-3).

- Delete : Selected fingerprint information file is deleted.

- Information : The selected file information appears (Figure 52-2).

? Delete
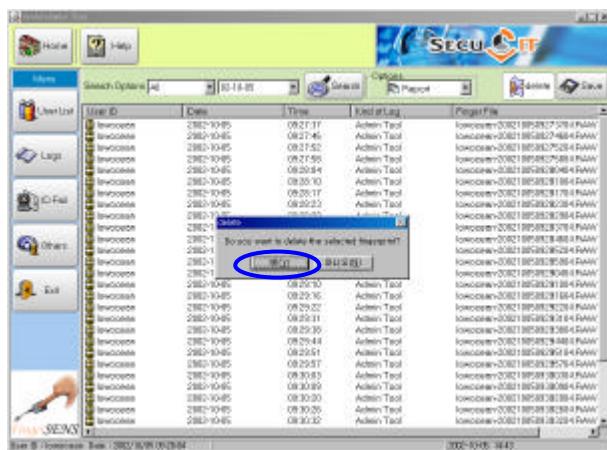
Figure 59-7) Delete

The selected file in the list is deleted.
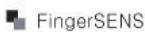
3.5 Other Setting

Figure 60) Other Setting

、   This menu informs user information and failed image path.

、   By clicking , you can check where "User Information and
     Failed Images" are going to be stored (Figure 53).

> 、Notice : If you change the save directory, system will be in
>   trouble. Please be noticed

?. Appendix

1. Glossary Definition

Glossary	Description
TruePrint	It reads through the outer layer of skin to the live layer, below the surface.
Dynamic Optimization	It uses the flexibility of the TruePrint technology to adapt the person's current skin condition.
LED	luminescent diode
User	User can do logon, screen saver and encryption.
Administrator	Someone who takes care about user information and registration.
Management Tool	Only administrator can run this program. This program can check each user's registration, modification and management.
Verification	Literally it means a public confirmation of an action or a document that was made in a proper manner. Here it means an user is authenticated to get an access to the computer using user's fingerprint.
Enrollment	Literally it means recording something in a document officially to expect legal protection. Here it means registering a user's fingerprint, ID and password on the computer.

Logon	A performance for a user to register user's ID and password and to be verified to get access to the host computer or the network
USB	Stands for Universal Serial Bus, it designs to communication with PC and other devices. As compared with SCSI, its cable is in detail, and light. Because connector can be more small, the cost will be reduced. The other advantage is plug and play type. This function makes USB connect with other devices easily. So, it reduces much work to extend PC.

2. Notice

2.1 Connect Fingerprint before installing the program

Make sure you connect FingerSENS to the computer before you install programs. Otherwise, there pops up a warning "There is no device".

2.2 Enrolling Administrator

After installing, you should register administrator first. If you don't register, it occurs a fatal error when you logon again.

2.3 Installing FingerSENS Drive

Before you install FingerSENS, you should install FingerSENS drive first. Physically, FingerSENS should be connected.

2.4 Storage of FingerSENS

Avoid the humid place to store FingerSENS.

2.5 Uninstalling FingerSENS

When you want to uninstall FingerSENS, sometimes it doesn't work properly. You must use Control Panel – "Program add/remove" as instructed in the manual.

2.6 Inputting User Fingerprint

When you input your fingerprint, do it 3 times for faster, more reliable verification. In that way, the sensor takes the best image in the first place and compares the input image of a user who is trying to get access to the registered ones.

2.7 Encryption & Decryption of Folder and File

After user encrypts file and folder, user changes user's fingerprint information. In this case, decryption will not be worked properly. You should be careful with encrypted file and folder.

3. Trouble Shooting

3.1 Failed to open a fingerprint sensor
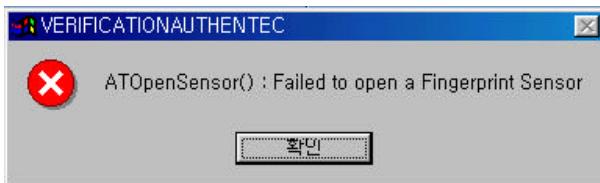
The above error message means there is no FingerSENS attached. Therefore, check if FingerSENS and cable are properly connected to PC.

3.2 When registered person isn't verified

When the registered fingerprint images do not have good quality for verification, fingerprint doesn't match well. In this case, you should input your fingerprint 3 times again for better verification.

3.3 When the device doesn't get the fingerprint image

When FingerSENS is in humid or is damaged from physical shock, it doesn't work properly. It should be repaired.

3.4 Program Removal

When you have double click to remove the setup file, sometimes setup file doesn't work properly. In this case, you should follow next steps.

、   Start -> Setting -> Control panel
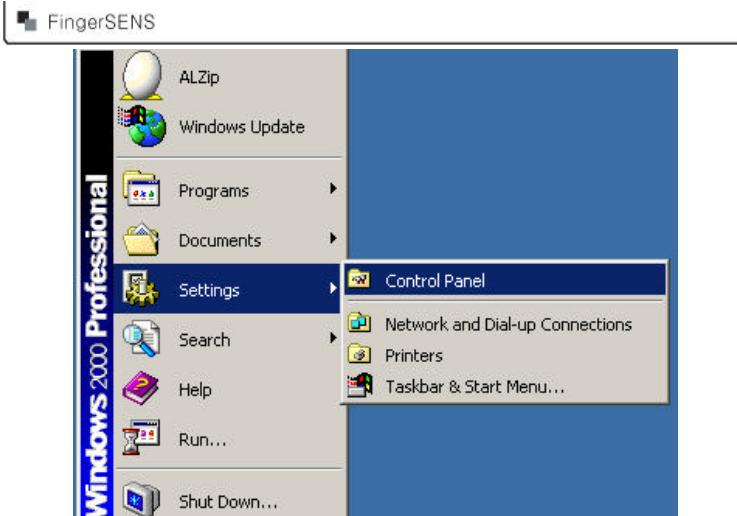
FingerSENS

. Control panel -> Program Add/Remove
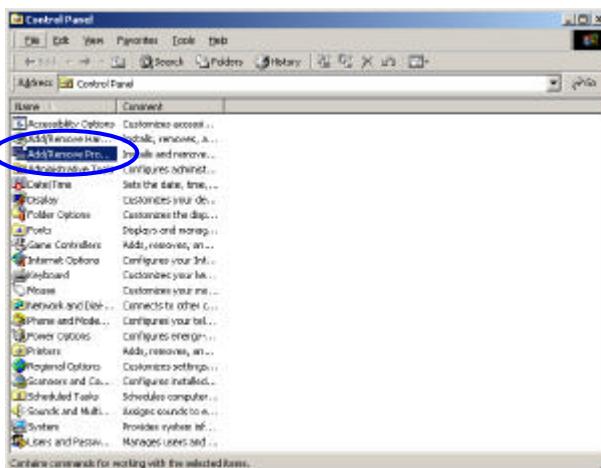
· In the program list, select FingerSENS and then press "Add/Remove"..
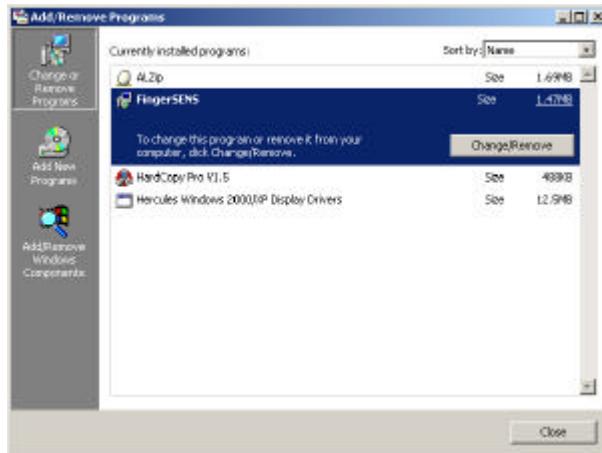
· When you choose "Add/Remove", the screen of fingerprint confirmation

appears.

- The program can be removed through administrator's fingerprint
  verification.

- As you have following screen, you success to remove the program.
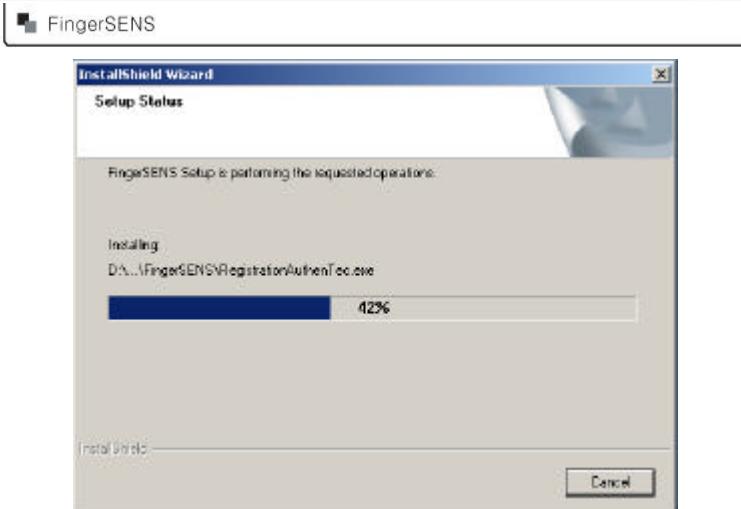
4. FCC Notice

FCC NOTICE

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC

Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment of and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

NOTE: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.