SAND--90-0690C

DE90 012917

A PERFORMANCE EVALUATION OF BIOMETRIC IDENTIFICATION DEVICES

James P. Holmes; Russell L. Maxwell; Larry J. Wright
Sandia National Laboratories
Albuquerque, NM 87185

June 1990

ABSTRACT

A biometric identification device is an automatic device that can verify a person's identity from a measurement of a physical feature or repeatable action of the individual. A reference measurement of the biometric is obtained when the individual is enrolled on the device. Subsequent verifications are made by comparing the submitted biometric feature against the reference sample. Sandia Laboratories has been evaluating the relative performance of several identity verifiers, using volunteer test subjects. Sandia testing methods and results are discussed.

INTRODUCTION

The present generation of biometric identification devices offers cost and performance advantages over manual security procedures in many applications. Applications include physical access control at portals, computer access control at terminals and telephone access control at central switching locations. Installations can range from a single, stand alone verifier to control one access point; up to a large networked system of many verifiers, monitored and controlled by one or more central security sites.

Verifier performance should be an important consideration in any security application. Performance data, however, is not always easy to obtain or interpret. Test methods must be well documented if the results are to be meaningful. A verifier could be tested in an ideal environment with robotic simulation of biometric data to measure its theoretical performance limit. The results of such a test could be very different from its real world performance. The human element is an essential part of the performance of any identity verifier. Environmental factors such as noise, light, electromagnetic radiation, moisture, dust and temperature could also be important in the performance of a verifier.

Sandia started its latest verifier test series in November, 1989. These tests have incorporated the human element by making use of nearly 100 volunteer users, who attempted many verifications on each of the machines. Environmental considerations were minimal, as the tests were all performed in a laboratory room for the convenience of the test

---

volunteers. The biometric features used by the latest generation of verifiers in the Sandia tests include:

Fingerprint by Identix, Inc.
Hand geometry by Recognition Systems Inc.
Signature dynamics by Autosig Systems Inc.
Retinal vascular pattern by EyeDentify Inc.
Voice by Alpha Microsystems Inc.
Voice by Ecco Industries Inc.

GENERAL TEST DESCRIPTION

Verifier testing was performed to obtain statistics on false rejection error rates and false acceptance error rates for each verifier. A false rejection is the rejection of a validly enrolled user who makes an honest attempt to be verified. A false rejection error is also called a Type I Error. A false acceptance is the acceptance of an imposter as a validly enrolled user. A false acceptance error is also called a Type II Error.

Each verifier in the test is a commercially available unit. Software and/or firmware modifications were made by the manufacturer on some units to allow Sandia to collect the required test data. All such modifications were specified and purchased by Sandia. Each verifier was set up in accordance with the manufacturer's recommendations where possible. In most cases, a representative from each manufacturer visited the testing laboratory to verify that his device was properly set up. Where problems were pointed out, attempts were made to rectify them. Some attempts were more successful than others within the limits of our test facility resources.

The verifier tests at Sandia were conducted in an office like environment and made use of volunteers from the ranks of Sandia employees. A single laboratory room contained all of the verifiers. Each volunteer user was enrolled and trained on all verifiers.

There is a learning curve for the proper use of a biometric identification device. As a user becomes more familiar with a verifier, his/her false rejection rate decreases. This curve is different for individual users and verifiers. This learning effect was minimized for the Sandia testing by training the individuals before the test, monitoring their performance and by not using the first few weeks of test data in the results. A number of users were re-enrolled on verifiers where there was indication of below average performance. Other known errors were removed by instructing the users to annotate a hardcopy printout of any transaction when he/she made a mistake, or was "experimenting" and did not feel that the verification attempt was valid. A similar method was used to remove valid verifications on the false acceptance test when a user submitted his/her own PIN. There is no doubt that unrecognized errors remain in the data. These remaining

errors contribute to the overall test error rate, reflecting the human factors in the use of biometric identification devices.

The problem of selecting a representative test user group is the most vexing in the testing of biometric identification devices. The very differences in physiological and behavioral properties of humans that allow these devices to function, set one group of people apart from another in generating test results. The best solution to this problem seems to be the use of large numbers of users and large numbers of attempts. The larger the numbers, the more likely the results will be representative of true performance values. It is beyond the scope of this test report to analyze the probable error rate due to test population size. It will be an interesting subject for a future study.

No extraordinary incentives were offered the volunteer users who performed the tests. Treats were often available in the test room for users to tempt them to remain active in the tests. A free lunch drawing was made to reward regular users. About 80 of the almost 100 enrolled users remained fairly active in the tests. Work and travel schedules accounted for the loss of some users. Others just became disinterested after a while and did not continue in the tests.

The first test series was false rejection testing. This was done by the users attempting verification on each machine many times over a three month period. The second test series was passive false acceptance testing. In this series, each user submitted the personal identification number (PIN) of each other user and then submitted his/her own natural biometric in an attempt to be recognized or verified as that individual.

DATA PROCESSING

The first step in the data processing was to remove the invalid transactions that were noted on the print-outs. The data files were then processed to cull out incomplete records and to convert the data to a common format. The data was sorted into individual user groups. User groups of less than 6 transactions were deleted. User data obtained prior to their re-enrolling on a verifier were also deleted.

Transactions were divided into verification attempts, defined to be all tries at verification in a 5 minute period by one user on a verifier. A try is one cycle of the user presenting his/her biometric to the verifier and receiving a verification decision. Only the first three tries on an any attempt were used in the data analysis.

A validly enrolled user can have one of the following outcomes on a three-try attempt:

TRY 1	TRY 2	TRY 3	VALID USER OUTCOME DEFINITION
ACCEPT			one-try, two-try and three-try acceptance
REJECT	ACCEPT		one-try false reject and a two-try and three-try acceptance
REJECT	REJECT	ACCEPT	two-try false reject and a three-try acceptance
REJECT	REJECT	REJECT	three-try false reject

An imposter can have one of the following outcomes on a three-try attempt:

TRY 1	TRY 2	TRY 3	IMPOSTER OUTCOME DEFINITION
ACCEPT			one-try, two-try and three-try false acceptance
REJECT	ACCEPT		one-try reject and a two-try and three-try false acceptance
REJECT	REJECT	ACCEPT	two-try reject and a three-try false acceptance
REJECT	REJECT	REJECT	three-try reject

Not all attempts were three-try. One-try and two-try attempts were also recorded. Any attempt with one reject and no accepts is a one-try attempt. Any attempt with two rejects and no accepts is a two-try attempt.

The false reject error rate (FR) is the ratio of false rejects to total attempts at verification. The FR was calculated for each user for one-try, two-try and three-try verification attempts over a range of assigned thresholds. The transaction score data was used to find the number of errors that would have occurred, had the verifier test threshold been set at each of the assigned thresholds.

The false accept error rate (FA) is the ratio of false acceptances to total imposter attempts. As in the case of the FR, the FA was calculated for each user over the range of assigned thresholds.

The average percent FR and FA for each verifier was calculated by averaging its user percent error rates for each assigned threshold. This is the data that is presented in the error rate curves in the RESULTS section.

The Identix fingerprint verifier does not have a customer settable threshold, and we were not able to get user scores for our tests. All the other verifiers we tested did provide user test score data. The ability to set thresholds and to allow multiple try attempts broadens the operating range of verifiers. Prospective customers can make use of the error curves to select available threshold values that meet their requirements.

The transaction time information presented in these results was obtained by timing the users from the time they touched the verifier until the verification verdict was presented after the attempt. The users were not actively participating and were not told that they were being timed. We feel that the results reflect typical verification times that could be expected in an actual installation. We also know that these times are substantially greater than the minimum times that could be accomplished by a skilled user going as fast as possible.

ALPHA MICROSYSTEMS VOICE VERIFIER

Alpha Microsystems of Santa Ana, California bought out Voxtron and is now selling an updated system called Ver-A-Tel. A personal computer (PC) contains the speech board hardware and the software programs to operate the system. User terminals are touch tone telephones that can be either direct connect or dial in. This system is intended to be networked with a number of users at different locations. Because of the low cost of adding user terminals (telephones), the cost per user drops as more users are added.

System management is performed at the PC by the use of a menu driven user interface. Access to the manager software is password protected. Prior to enrolling a new user, the system manager must enter the new user's PIN into the user data base.

Our user enrollment was accomplished over the same touch tone dial in telephone terminal that was used for the testing. Some differences can exist between telephones and we didn't want to introduce that unknown into the test results.

When enrolling, the system answers and then prompts the enrollee to enter his/her PIN by touch tone and then to say the phrase of choice. All users in our test used the same phrase; Yankee Doodle Dandy. The Enrollee is prompted to repeat the phrase until the system obtains enough consistent data to generate a template. After enrollment, the user verifies on the system by calling the verifier number and waiting for the prompts to enter his/her PIN and to say the phrase. The test system was set up for a maximum three-try attempt. An attempt is one utterance of the phrase. An adaptive algorithm updates the user's template each time a verification is successful.

Once the user is familiar with the system, it is not necessary to wait for the voice prompts to complete a verification attempt. Tone prompts preceding the voice prompts que the user to proceed in order to save time. The minimum time to lift the telephone, dial a 5 digit extension, wait for the tone prompts, enter a PIN, utter the phrase and be verified was about 13 seconds. The average user in our test took about 19.5 seconds for a complete verification. This average includes multiple try attempts.

AUTOSIG SYSTEMS SIGNATURE DYNAMICS VERIFIER

Autosig Systems of Irving, Texas manufactures a signature verification device that they call Sign On. This verifier consists of a user interface tablet and a controller which is designed to integrate into a host access control system. Applications range from stand-alone entry control through large network systems, facilitated by factory optional software interfaces to commercial computers.

The user interface is a low profile tablet approximately 8.5 by 11 inches in size. The tablet incorporates a digitizer tablet area, a pen attached by a cable, visual and audible prompts; a magnetic card reader and the interface electronics to communicate with the controller over a copper wire cable. The controller contains the system power supply, the interface logic and the processor logic. All signature templates are created, analyzed and validated in the controller.

The controller has an RS232 interface for a program monitor (typically a personal computer) to be attached temporarily for performing maintenance. This includes adding signature ID's and deleting signatures. Access to the maintenance menu is password protected.

Enrollment is accomplished at the user interface tablet. The visual prompt for ENTER ID should be illuminated before the enrollment sequence is started. A magnetic stripe card with a valid signature ID is swiped through the card reader to initiate the enrollment sequence. The visual prompt for SIGN ON illuminates, telling the user to sign his normal signature. The PLEASE WAIT prompt is then illuminated while the signature data is processed, followed by another prompt for SIGN ON. After the second signature is processed and the signature template is established, the DOOR OPEN prompt is illuminated to signify a successful transaction. When the ENTER ID prompt again reappears, it is necessary to repeat the process for one attempt to validate the template. If the validation is successful, the DOOR OPEN prompt will illuminate. Otherwise, the SIGN ON prompt will appear again until a successful validation has been made or until the maximum allowable tries have been unsuccessful. Unsuccessful attempts will result is all of the visual prompts blinking on and off simultaneously. Our test unit was set for a maximum of three tries per verification attempt.

The time to perform a verification depends in part on the amount of time a user takes to sign his/her name. Our users averaged about 15 seconds to verify on the Sign On, including multiple try attempts. The minimum time observed was around 12 seconds.

ECCO INDUSTRIES VOICE VERIFIER

Ecco Industries Inc. of Danvers, Mass. was represented by a voice verifier called the Voice Key. The Voice Key is self contained, wall mounted user interface that communicates with a control box over a copper wire cable. This device is well suited to stand alone applications as well as networked systems. The user interface contains a keypad, an alpha-numeric display, a microphone, an audible beeper and indicator lights to allow all necessary functions to be performed locally.

A system manager enters the program mode by a combination of key strokes and a valid voice verification. The program mode allows the manager to perform all system functions from the keypad. Users are enrolled from the program mode by entering the proper sequence of key strokes, the enrollee PIN and the enrollee uttered password. Prompts and responses are signaled by light emitting diodes (LED). An amber LED is the prompt to utter the password. An amber and a red LED together is the prompt to wait. A red LED is the response to a verify failure and a green LED is the response to a verify accept. The red and green LED are built into the same lens, so some color blind users cannot determine whether or not they were verified by looking at the response.

A minimum of three utterances of the password is required to enroll. More may be required if the utterances are not consistent or there is significant background noise. Once enrolled, the user verifies by entering his/her PIN on the keypad and uttering the password at the amber LED prompt. The user template is modified by averaging in each successful verification input.

Verification can be accomplished in about 5 seconds, but our users averaged about 6.6 seconds per single try attempt.

EYEDENTIFY RETINAL PATTERN VERIFIER

The retinal pattern verifier in this test series was the model 8.5, manufactured by EyeDentify Inc. of Portland, Oregon. It offers a number of improvements over their model 7.5. All models of the EyeDentify verifiers use a very low intensity infrared light to scan a circular path around the retina. As this light crosses a blood vessel, the amount of light reflected back is decreased. The reflected signal data is recorded and processed to form the eye template.

A unique option of the model 8.5 verifier is the "hands-free" mode of operation. While the verifier is operating in this mode, the user merely peers into the viewing aperture and aligns an optical target by positioning his/her head. The verifier senses the user's presence, takes a scan and decides whether or not the scan data is an eye. If so, a template is generated and the verifier searches the template data base for a match. If a match is found, the verifier identifies the user as a validly enrolled member. Otherwise, the user is rejected.

The model 8.5 user interface is built into a molded plastic case designed for wall mounting. It incorporates the viewing aperture and a head rest that easily accommodates the use of either eye. A keypad, a magnetic stripe card reader and an alpha-numeric display are incorporated to allow conventional user interfacing. The user interface communicates with a remote electronics box over copper wire cables. This box contains the processor logic and interface logic required for system operation. Operational modes include stand alone, a network of units reporting to a host computer and as a component of an existing access control system.

Enrollment requires the use of a terminal or PC connected to the remote electronics box. A menu driven software program allows the system management options to be exercised over the terminal. Only a validly enrolled system manager, who must verify his/her identity by an eye scan, can gain access to the management program. To enroll a new user, the system manager sets up the user data record and initiates the enrollment sequence that requires the new user to take several eye scans. Each scan is initiated by the user pressing the ENTER button on the keypad, while peering into the viewing aperture at the center of the properly aligned optical target. A score is displayed on the terminal for each scan after the first. The manager has the option of accepting or rejecting any scan, and of continuing or terminating the enrollment process. The enrollment template is generated from an average of the accepted scans. This template does not get modified by subsequent valid verification, so it is important to accept only the best scores during enrollment. We tried to get at least three scores above 90 when possible. The system doesn't work well if the user is wearing glasses. Contact lenses present no problem, either in or out. Some users have vision problems without their glasses that make it difficult to align the optical target well enough to achieve consistent scores above 90.

Our test system was set up to allow three-try verification attempts. An attempt is initiated by the user inserting a magnetic stripe card into the card reader. The PIN number from the card is read and displayed, signaling the user to proceed. The user then peers into the aperture, aligns the optical target and presses the ENTER key on the keypad. If the verification is successful, the user's name appears on the display. Otherwise, the message REPEAT is displayed. The user continues to take scans until his/her name appears, or until three tries have been unsuccessful.

The average time for our users to perform the verification process was about 7 seconds, including multiple try attempts and some users that had to remove their glasses after inserting their card. The quickest times were around 4.5 seconds.

IDENTIX FINGERPRINT VERIFIER

The fingerprint verifier evaluated in this test was the TouchLock, manufactured by Identix Inc. in Sunnyvale, California. This system has a factory set threshold and does not generate score information. The test results, therefore, do not include the error rate curves. Only the percent false reject errors and percent false accept errors at the factory set threshold can be reported.

The user interface is the TouchLock sensor module containing the fingerprint reading optics, a numeric keypad, an alpha-numeric display and an audible tone generator. It is housed in a plastic enclosure approximately 8.2 by 3.9 by 4.4 inches high. It can be either wall-mounted or used on a table top. The sensor module communicates with a remote processor box over a copper conductor cable. A host PC was connected to the processor box for system management, which was performed by the use of a menu driven management program. Access to the management program is password controlled.

User enrollment is performed at the sensor module by a system manager, who must be verified by a fingerprint scan to gain access to the enrollment mode. The alpha-numeric display prompts the enrollee to enter his PIN number into the keypad and then to place his finger on the fingerprint reader. A pressure-actuated switch signals the reader to scan the fingerprint. A series of audible beeps and display prompts direct the enrollee to place and remove his/her finger from the reader until enough data is obtained to generate a template. An enrollment score is displayed, allowing the manager the option of either accepting the enrollment or trying again. The fingerprint template is generated from an average of several enrollment scans. The template is not updated with successful verifications. A low enrollment score and/or difficulty in verifying is cause to re-enroll a user.

User authentication is also performed at the sensor module. We used a magnetic stripe card for PIN entry on verification attempts on the false reject portion of the test and the keypad PIN entry for the false accept testing. The user swipes his card through the reader, follows the prompts to place his finger on the reader and then remove it and then waits for the result. If the identity is not verified, the user is prompted to try again. Access is denied after three unsuccessful tries.

Our users averaged about 6.6 seconds for a card PIN entry verification, including multiple try attempts. The fastest users verified in under 5 seconds. We did not time anyone using the keypad PIN entry method.

RECOGNITION SYSTEMS HAND PROFILE VERIFIER

The model ID3D-U hand profile verifier manufactured by Recognition Systems Inc. (RSI) of San Jose, California was evaluated in this test. This self contained unit is packaged in a metal case approximately 12.5 inches wide by 13.5 inches high and 8 inches deep. It incorporates the hand measurement plate, a numeric keypad, an alpha-numeric display, an insertion magnetic stripe badge reader, a hand geometry sensor, a power supply, the processor logic and the interface logic. The verifier can operate as a stand-alone unit, or as a host to a network of verifiers, or as a component in a host computer network. Our test set up had two verifiers connected to a host PC for test data acquisition and data base management. Our management software was custom for our test and is not required for system operation.

System management functions are performed at the verifier. A designated manager can access the management functions by entering a password within a time limit after he/she has been successfully verified. The manager selects the enrollment option and enters the PIN of the enrollee. The verifier then prompts the enrollee to place his/her hand on the measurement plate. Alignment pegs and optical checks insure that the user's hand is in proper position before the hand geometry is read. After the read, the enrollee is prompted to alternately remove and replace his/her hand on the measurement plate until three reads have been taken. The user template is generated from an average of the three reads. It is worth mentioning that the nine-byte RSI template is the smallest of any of the veifiers we have tested.

An enrolled user can verify by entering his/her PIN at the verifier and following the prompt to place his/her hand on the measurement plate. Our test verifiers would allow PIN entry by either keypad entry or by the use of a magnetic stripe card in an insertion reader. We used the card entry option for false reject testing and for our timing data. The keypad PIN entry was only used for false acceptance testing.

The average verification time for our users was about 5 seconds, using card PIN entry. Times as low as about 2.9 seconds were observed.

RESULTS

The test data is still being processed. It will go here in the final version of the report.

CONCLUSION

The present generation of biometric identification devices can provide reliable and cost effective protection of assets. Available computer interfaces and software provides for effective security management with real time control, transaction logging and audit tracking capabilities. The need in the biometric identification field now is to have the market make greater use of this existing capability. Although there are still biometric devices emerging into the market, it is not likely that any one of them will soon offer such a price/performance breakthrough that it will turn the market around on its own.