



## Examining the reliability of a hand geometry identity verification device for use in access control

|               |   |
|---------------|---|
| Title         | Examining the reliability of a hand geometry identity verification device for use in access control |
| Item Type     | Thesis  |
| Authors       | Bright, Daryl C.  |
| URI           | <a href="https://hdl.handle.net/10945/22792">https://hdl.handle.net/10945/22792</a>                 |
| Date Issued   | 1987-03   |
| Download date | 2026-04-14 05:19:58   |
| Link to Item  | <a href="https://hdl.handle.net/10945/22792">https://hdl.handle.net/10945/22792</a>                 |

Downloaded from NPS Archive: Calhoun



DUDLEY KNOX LIBRARY  
NAVAL POSTGRADUATE SCHOOL  
MONTEREY, CALIFORNIA 93943-5002













# NAVAL POSTGRADUATE SCHOOL

## Monterey, California



# THESIS

EXAMINING THE RELIABILITY OF A HAND  
GEOMETRY IDENTITY VERIFICATION  
DEVICE FOR USE IN ACCESS CONTROL

by

Daryl C. Bright

March 1987

Thesis Advisor

Douglas E. Neil

Approved for public release; distribution is unlimited.

T23-265



## REPORT DOCUMENTATION PAGE

|  |       |   |   |  |                                |
|--|-------|---|---|--|--------------------------------|
| 1a REPORT SECURITY CLASSIFICATION<br>UNCLASSIFIED  |       |   | 1b RESTRICTIVE MARKINGS   |  |                                |
| 2a SECURITY CLASSIFICATION AUTHORITY   |       |   | 3 DISTRIBUTION/AVAILABILITY OF REPORT<br>Approved for public release;<br>distribution is unlimited. |  |                                |
| 2b DECLASSIFICATION/DOWNGRADING SCHEDULE   |       |   | 4 PERFORMING ORGANIZATION REPORT NUMBER(S)  |  |                                |
| 4 PERFORMING ORGANIZATION REPORT NUMBER(S)   |       |   | 5 MONITORING ORGANIZATION REPORT NUMBER(S)  |  |                                |
| 6a NAME OF PERFORMING ORGANIZATION<br>Naval Postgraduate School  |       | 6b OFFICE SYMBOL<br>(if applicable)<br>55 | 7a NAME OF MONITORING ORGANIZATION<br>Naval Postgraduate School                                     |  |                                |
| 6c ADDRESS (City, State, and ZIP Code)<br>Monterey, California 93943-5000  |       |   | 7b ADDRESS (City, State, and ZIP Code)<br>Monterey, California 93943-5000                           |  |                                |
| 8a NAME OF FUNDING/SPONSORING ORGANIZATION   |       | 8b OFFICE SYMBOL<br>(if applicable)       | 9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER  |  |                                |
| 8c ADDRESS (City, State, and ZIP Code)   |       |   | 10 SOURCE OF FUNDING NUMBERS  |  |                                |
|  |       |   | PROGRAM ELEMENT NO  | PROJECT NO                                       | TASK NO                        |
|  |       |   |   |  | WORK UNIT ACCESSION NO         |
| 11 TITLE (include Security Classification)<br>EXAMINING THE RELIABILITY OF A HAND GEOMETRY IDENTITY VERIFICATION DEVICE FOR USE IN ACCESS CONTROL  |       |   |   |  |                                |
| 12 PERSONAL AUTHOR(S)<br>Daryl C. Bright   |       |   |   |  |                                |
| 13a TYPE OF REPORT<br>Master's Thesis  |       | 13b TIME COVERED<br>FROM _____ TO _____   |   | 14 DATE OF REPORT (Year Month Day)<br>1987 March | 15 PAGE COUNT<br>40            |
| 16 SUPPLEMENTARY NOTATION  |       |   |   |  |                                |
| 17 COSATI CODES  |       |   | 18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)                    |  |                                |
| FIELD  | GROUP | SUB-GROUP                                 | Biometric, Access Control, Hand Geometry, Security  |  |                                |
|  |       |   |   |  |                                |
|  |       |   |   |  |                                |
| 19 ABSTRACT (Continue on reverse if necessary and identify by block number)<br>Controlling the access to secure government facilities has become increasingly important as these systems are entrusted with more sensitive applications. Unauthorized access could be very detrimental to our nation's security. The use of biometric measures, one of which is hand geometry, may represent a possible solution. This thesis looks at one hand geometry identification device, and determines its effectiveness as a function of the rejection threshold setting, a time lapse in use, and the construction of the reference templates. Rejection thresholds of 40, 60, 80, 100, 120, and 140; three weeks of inactivity by the test subjects; and construction of the reference templates from 1, 2, 4, 5, 6, 8, and 10 individual hand readings were examined. The application of hand geometry identification technology for protecting Command, Control, and Communications (C3) facilities was |       |   |   |  |                                |
| 20 DISTRIBUTION/AVAILABILITY OF ABSTRACT<br><input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT <input type="checkbox"/> DTIC USERS  |       |   | 21 ABSTRACT SECURITY CLASSIFICATION<br>Unclassified   |  |                                |
| 2a NAME OF RESPONSIBLE INDIVIDUAL<br>Prof. Douglas E. Neil   |       |   | 22b TELEPHONE (include Area Code)<br>2419   |  | 22c OFFICE SYMBOL<br>Code 55N1 |

then discussed. This study used the ID-3D Hand Geometry Identifier built by Recognition Systems, Inc. of San Jose, California. This device was very effective in producing low Type I and Type II error rates during 6300 trials covering all situations examined. This technology has great potential for protecting C3 facilities and systems.

Approved for public release; distribution is unlimited.

Examining The Reliability of a Hand Geometry Identity Verification  
Device For Use in Access Control

by

Daryl C. Bright  
Captain, United States Air Force  
B.A., University of Minnesota, Morris, 1970

Submitted in partial fulfillment of the  
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY  
(Command, Control and Communications)

from the

NAVAL POSTGRADUATE SCHOOL  
March 1987

## ABSTRACT

Controlling the access to secure government facilities has become increasingly important as these systems are entrusted with more sensitive applications. Unauthorized access could be very detrimental to our nation's security. The use of biometric measures, one of which is hand geometry, may represent a possible solution. This thesis looks at one hand geometry identification device, and determines its effectiveness as a function of the rejection threshold setting, a time lapse in use, and the construction of the reference templates. Rejection thresholds of 40, 60, 80, 100, 120, and 140; three weeks of inactivity by the test subjects; and construction of the reference templates from 1, 2, 4, 5, 6, 8, and 10 individual hand readings were examined. The application of hand geometry identification technology for protecting Command, Control, and Communications (C3) facilities was then discussed. This study used the ID-3D Hand Geometry Identifier built by Recognition Systems, Inc. of San Jose, California. This device was very effective in producing low Type I and Type II error rates during 6300 trials covering all situations examined. This technology has great potential for protecting C3 facilities and systems.

## TABLE OF CONTENTS

|      |  |    |
|------|--|----|
| I.   | INTRODUCTION .....                       | 8  |
| II.  | THE EXPERIMENT .....                     | 10 |
|      | A. THE EQUIPMENT .....                   | 10 |
|      | B. OBJECTIVES OF THE EXPERIMENT .....    | 12 |
|      | C. EXPERIMENTAL PROCEDURE .....          | 14 |
|      | 1. Participants .....                    | 14 |
|      | 2. Enrollment Process .....              | 14 |
|      | 3. Experiment Sessions .....             | 16 |
| III. | RESULTS AND DISCUSSION .....             | 18 |
|      | A. TYPE I AND TYPE II ERRORS .....       | 18 |
|      | 1. Different Threshold Settings .....    | 20 |
|      | 2. Time Lapse .....                      | 23 |
|      | 3. Template Construction .....           | 26 |
|      | 4. Updating Algorithm .....              | 26 |
|      | 5. The Three Try Strategy .....          | 28 |
|      | 6. Biometric Device Comparison .....     | 30 |
|      | B. OTHER MEASURES OF EFFECTIVENESS ..... | 30 |
|      | 1. Time to Achieve Recognition .....     | 30 |
|      | 2. Administration .....                  | 31 |
|      | 3. Convenience to User .....             | 31 |
|      | 4. Costs .....                           | 31 |
|      | 5. Equipment Reliability .....           | 32 |
|      | C. C3 APPLICATIONS .....                 | 32 |
| IV.  | CONCLUSIONS AND RECOMMENDATIONS .....    | 36 |
|      | LIST OF REFERENCES .....                 | 38 |
|      | INITIAL DISTRIBUTION LIST .....          | 39 |

## LIST OF TABLES

|  |    |
|--|----|
| 1. TYPE I AND TYPE II ERROR RATES .....              | 22 |
| 2. TYPE I AND TYPE II ERRORS FOR PARTS 1 AND 2 ..... | 25 |
| 3. CHANGES IN TEMPLATE CONSTRUCTION .....            | 26 |
| 4. THREE TRY STRATEGY RESULTS .....                  | 29 |

## LIST OF FIGURES

|     |   |    |
|-----|---|----|
| 2.1 | ID-3D Hand Geometry Identity Verifier . . . . .               | 10 |
| 2.2 | ID-3D Picture Acquisition . . . . .                           | 12 |
| 2.3 | ID-3D Functional Block Diagram . . . . .                      | 13 |
| 2.4 | Part 2 Operating Instructions . . . . .                       | 17 |
| 3.1 | Preferred Performance of Biometric Access Device . . . . .    | 19 |
| 3.2 | Realistic Error Curves For Biometric Access Devices . . . . . | 20 |
| 3.3 | ID-3D Identifier Test Results . . . . .                       | 22 |
| 3.4 | Type I and Type II Errors During Part 1 . . . . .             | 24 |
| 3.5 | Type I and Type II Errors During Part 2 . . . . .             | 25 |
| 3.6 | Test Results With Updating Algorithm . . . . .                | 27 |

## I. INTRODUCTION

Controlling the access to government owned and operated facilities has become increasingly important as these systems are entrusted with more sensitive applications and information. In fact, the subject of personal access to Command, Control, and Communications (C3) systems is of the greatest national interest (FIBS Pub 48, 1977), and it is essential that the Department of Defense protect its information processing systems against unauthorized access as required by national security considerations (DOD 5200.1, 1984). Greater effectiveness in access control is a necessity in today's C3 world of sensitive information and protected systems.

There are three methods of verifying a persons identity in order to establish access control procedures (FIBS Pub 83, 1980). These methods are:

- 1) Something a person knows
- 2) Something a person possesses
- 3) Something about a person.

The first method includes such things as passwords and lock combinations. The second includes badges, passes, keys, and cards with machine-readable information. The third category includes physiological attributes such as a persons weight, voice, blood vessel pattern, hand geometry, etc.

Verification of identity through information known only to a person is a common method of controlling access to time-shared systems. Of course, anything known by one person may become known by another. This often happens because items like passwords and lock combinations are selected which are related to a person's interests or surroundings, or are written down to prevent them from being forgotten. It is then easy for an imposter to obtain this known information and to successfully gain unauthorized access. Locks, keys, badges, and card-keys are familiar mechanisms used to control access to secure facilities. However, the degree of security afforded by these items is also limited because they too can be stolen or lost, and then easily used to gain unauthorized access. What may be worse is that these items may fall into the hands of an unauthorized user, duplicated, and returned. Unauthorized access could then be gained without anyone even realizing it was taking place. Because of these vulnerabilities in the first two methods of providing access control, much emphasis has

recently been focused on the technology of personal identification through physiological attributes (Riganati, 1985). This area of study is called Biometrics, and is defined as the use of unique personal characteristics to identify an individual. Through the use of biometric devices, a person can be identified by virtue of what he is, rather than through items he possesses or knows (Bakke, 1986). This third method of identity verification can significantly increase the effectiveness of access control.

A number of personal attributes have been considered in developing biometric access control devices. These include fingerprints, retinal blood vessel patterns, voice prints, and signature dynamics (Government Computer News, 1985). Other characteristics also considered are lip grooves, bite patterns, ear structures, and electrocardiograms (Forsen, Nelson, Staron, 1977). Hand geometry is another type of biometric identification. It uses a three dimensional image of the hand to uniquely verify a persons identity. Hand geometry has been selected as a usable attribute for biometric access control because the hand "is sufficiently rich in detail to meet even the most stringent error specifications" (Forsen, Nelson, Staron, 1977, p. 2-13).

The ID-3D Hand Geometry Identifier by Recognition Systems, Inc of San Jose, California is one such hand geometry identification verification device. It is the basis of this thesis. The ID-3D Identifier verifies identification by comparing identity discriminating characteristics of an individual hand picture to a reference template made from a number of previously taken hand pictures of the same person. How close the individual hand picture must be to the template in order to verify identification is controlled by a threshold setting. For this study, an experiment was conducted to determine the reliability of the ID-3D Hand Geometry Identifier as a function of the threshold setting, the number of hand pictures used to make the reference template, and a three week time lapse during which the test subjects did not use the device. This thesis will describe the experiment, present the results, and discuss the applicability of using the ID-3D Identifier to control access to C3 systems.

## II. THE EXPERIMENT

The ID-3D Hand Geometry Identifier is a biometric recognition access device which uses a three dimensional image of the hand to uniquely verify a persons identity. The device operates by storing reference information of the hand's geometry in a microprocessor, and, upon entry demand, compares the stored information with the hand pattern of the individual seeking access. If the stored information and that presented by the individual agrees within a threshold limit, access is allowed. If the data does not compare within the limit, access is denied. (Users Manual, 1986)

### A. THE EQUIPMENT

The ID-3D Identifier can operate in a stand-alone mode, in a hybrid mode, or in an integrated system mode (Sidlauskas, Oct 1986). It can also be configured in a Test System, and was set up as such for this experiment. The Test System consists of a hand reader, a 12 digit keypad, and an IBM XT personal computer. The hand reader and keypad were mounted in one housing as shown in Figure 2.1.



Figure 2.1 ID-3D Hand Geometry Identity Verifier.

The hand reader contains 256 Kbytes of random-access memory for hand geometry data storage, 32 Kbytes of program memory, and two full duplex serial communication ports for communication with host systems and local peripherals such as a printer or terminals for user enrollment. The 12 button keypad is connected to the hand reader, and is used to enter the users personal identification number (PIN).

The IBM XT computer portion of the Test System was used for system control, monitoring, and data storage. It was connected to the hand reader, a keyboard, and a video display unit, and contained a 20 Mbyte capacity hard disk for storage of over 10,000 hand images. In the experiment, the computer was used to enroll new users, set system operating thresholds, and record all hand reader activity and operators comments.

To operate the hand reader, the user enters his PIN via the keypad, and places his hand on the measuring platen (Figure 2.1). Eight Kbyte digital pictures are then acquired by the hand reader camera as in Figure 2.2. The camera consists of a light source which illuminates the hand, and a lens which focuses a three dimensional image of the hand on a silicone image detection chip. The chip is a square array of 256 by 256 individual picture element photo detectors. This chip changes the focused image into a 8 Kbyte digit stream.

The analysis of the hand picture by the hand reader is functionally depicted in Figure 2.3. The 8 Kbyte digital pictures are continually acquired until the hand position detector determines the hand is properly positioned. Once positioned, a single 8 Kbyte picture is captured for dimensional analysis. This analysis consists of measuring the physical dimensions of the hand. It considers the location of finger tips, the location of the webs between the fingers, the widths and lengths of the fingers, the total hand area, the thickness of the palm, etc. This dimensional analysis, a physical measuring of the hand, produces a 96 Byte dimension vector. This vector is the collection or aggregate of the 48 physical characteristics measured in the dimensional analysis. Each measurement requires 2 Bytes, so 96 Bytes are needed for this vector. The dimension vector then undergoes feature extraction. This consists of transforming the dimension vector by using the data stored in the calibration matrices. These matrices are tables of numbers which depict the relationships between characteristics of universal hands. The matrices are used to eliminate those features in the dimension vector which are common to all hands, and to retain those features which are unique to the hand being read. What results is an 18 Byte feature vector. This vector no

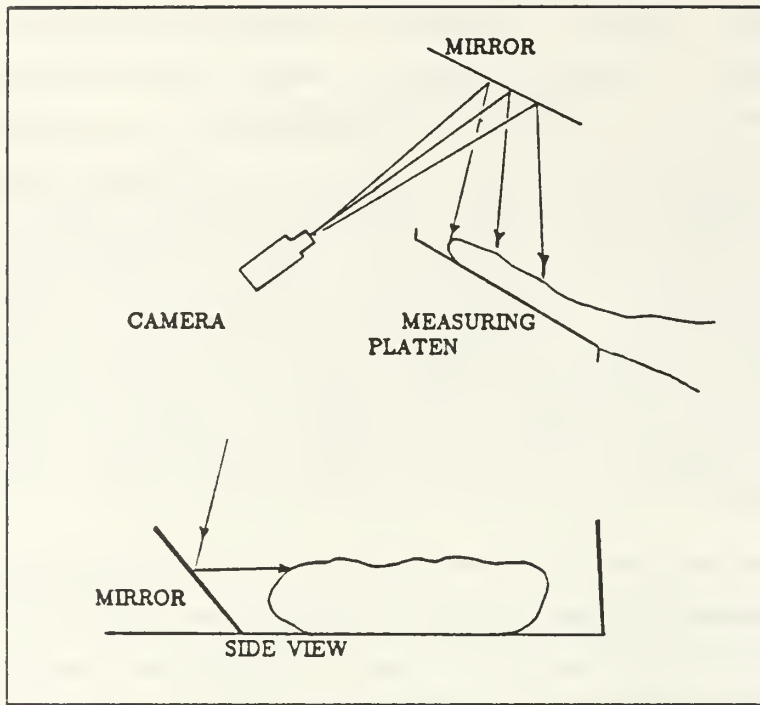


Figure 2.2 ID-3D Picture Acquisition.

longer represents the actual 48 physical characteristics measured, but is a representation of the features which make the individual hand unique. These operations of dimension analysis and feature extraction are accomplished to reduce the amount of data, and at the same time retain all of the identification features of the hand. During user enrollment, five of these feature vectors are mathematically averaged, and the average is stored as the reference template vector of the enrollee. During verification attempts, the feature vector produced is compared to the previously saved reference template vector. A verification decision is then made based on the magnitude of the difference between the feature vector and the template vector. The difference between these two vectors is reduced to a single number which can range from 0 to 400. It is this difference score which is compared to a preset threshold difference setting to determine successful identity verification.

## B. OBJECTIVES OF THE EXPERIMENT

There are two types of errors that can be made during access control efforts (FIBS Pub 83, 1980). They are:

- 1) Type I Errors - Falsely rejecting an authorized user.
- 2) Type II Errors - Falsely accepting an unauthorized user.

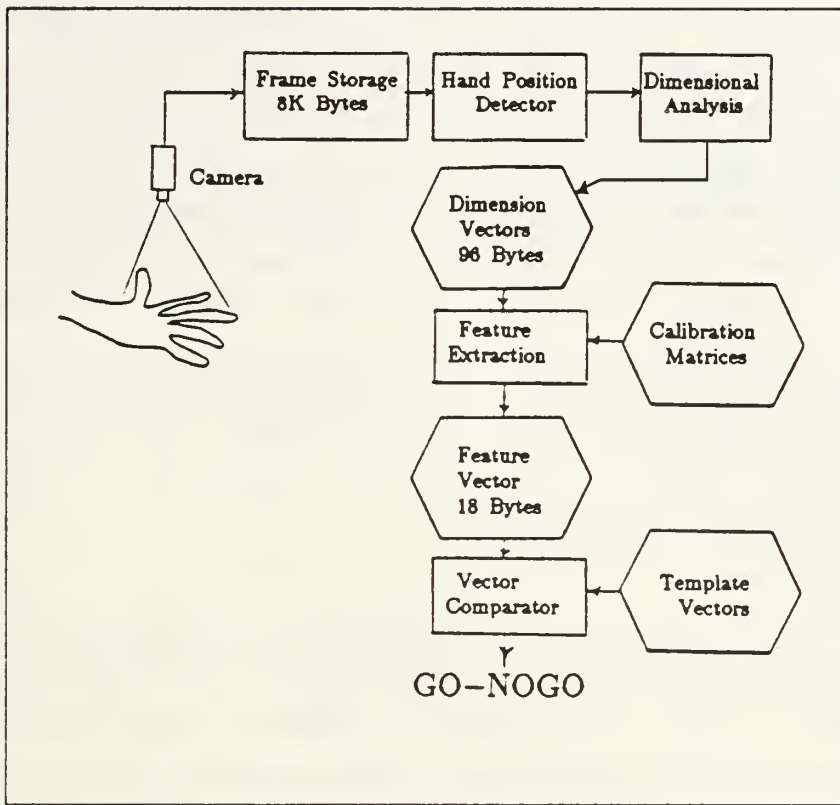


Figure 2.3 ID-3D Functional Block Diagram.

Both of these types of errors must be considered in evaluating hand geometry biometric access devices. These errors occur because of the difficulty in performing precise and repeatable measurements of the human hand. An optimal biometric device can correctly distinguish between the interpersonal variations in large groups of people, and eliminate the effects of intrapersonal variations of a single individual (FIBS Pub 48, 1977). However, any access control device which is not perfect must deal with the problems of both Type I and Type II errors.

The objective of this experiment was to determine the Type I and Type II error rates of the ID-3D Hand Geometry identity verifier in various configurations and situations. The first variable considered was that of different threshold settings. These settings control how close an individual hand picture must be to the reference template in order to grant access. Threshold differences of 40, 60, 80, 100, 120, and 140 were used. The second variable was the number of hand pictures that were averaged to make the reference template. Templates made from 1, 2, 4, 5, 6, 8, and 10 individual pictures were used. These templates, once constructed from a specific number of hand

readings, were not updated or changed during the experiment. The third variable considered was that of a time lapse between periods of use by the test subjects. After being enrolled and using the ID-3D for three weeks, a three week break was built into the experiment. Test subjects then resumed use for two additional weeks. These variables of threshold setting, reference template construction, and a time lapse in use were used to determine the Type I and Type II error rates of the ID-3D Identifier. These error rates determine the reliability of the ID-3D Identifier. If this device is reliable in terms of denying access to imposters, and granting access to authorized users, recommendations can be made as to the suitability of using this device in controlling access to C3 systems.

## **C. EXPERIMENTAL PROCEDURE**

### **1. Participants**

One hundred and eight subjects participated in the experiment. All subjects were between the ages of 25 and 38, and were students at the Naval Postgraduate School taking either the Man-Machine Interaction or Human Factors System Design course. There was one civilian participant, and all other 107 were military officers. There were 10 international officers, and 97 US military officers. Ten of the participants were women. A majority of the participants were technically oriented, and all were cooperative, and curious about the ID-3D Identifier. There were no incentives to succeed at the verification attempts, such as the granting of access to a place of employment, as would be typical in an operational access control situation. The device was set up in a laboratory, and available to the subjects during the school day. The subjects were totally unsupervised while accomplishing their verification attempts. None of the subjects were familiar with the ID-3D Identifier as none of them had used it or any other hand geometry verification device prior to the experiment.

### **2. Enrollment Process**

The first step in the experiment was the enrollment process. This process is the procedure by which each subject's hand geometry is converted into a reference template and stored in the hand reader's memory. This is the reference template against which all other hand pictures are compared when access is attempted.

To insure a consistent enrollment procedure, each subject selected an arbitrary four digit identification number, and then read these operating procedures:

Using the hand reader is a simple matter of entering your ID number via the keypad, placing your hand on the hand reader, and observing the results. Whenever the READY lamp on the hand reader front panel is flashing, it is ready to accept an ID number. Once the ID number has been entered, it is registered in the hand reader by pressing the # key. Once a valid ID number has been registered, the PLACE HAND lamp on the hand reader front panel will light. Once this light comes on, the camera illumination lamp will come on, as well as the four finger position indication lamps, and the hand should be placed on the measuring platen. The hand is to remain held on the platen for a brief moment until the PLACE HAND and camera lights go out. The results of the verification attempt will then be indicated by the panel lights. (Users Manual, 1986, pp. 25-26)

To increase the probability of building an accurate reference template, each subject was also given a copy of these correct hand placement rules (Users Manual, 1986. p. 26):

- 1) Bump the web between the middle and index finger up against the tall web pin.
- 2) Close all fingers together so that they touch their respective placement guide pins.
- 3) The balls of the finger tips should be against the platen surface, and the hand should be as flat as is comfortable.
- 4) If large rings are worn, care should be taken to see that the ring is rotated so that the stone is up in the normal position.

The actual enrollment of each subject was done individually under complete supervision. The supervisor set up the hand reader for the enrollment process using the appropriate menu selections from the control program in the IBM computer. Each subject was then given a practice ID number and allowed to operate the hand reader five times to become familiar with the equipment and to practice hand placement. The enrollee then accomplished five hand readings using his valid PIN. After these five valid hand readings were completed, the display screen showed the results by printing the five difference scores such as 16, 38, 12, 21, 9. These numbers represented the differences between the template that had been formed by averaging all five pictures, and each of the five individual hand readings. The supervisor then had the choice of accepting, rejecting, or quitting the individual enrollment. If accepted, the user was enrolled, and the reference template stored. If the session was quit, the user was not enrolled. If rejection was chosen, the individual hand reading with the largest difference was discarded and a new hand reading prompted for. All hand readings with a score of 60 or less were accepted for this experiment. Also, the enrollees removed their hands from the hand reader between each of the five enrollment readings. This ensured a slightly different placement for each reading, and provided a wider range of difference scores. Two test subjects were initially enrolled without removing their

hands between the five enrollment readings. This resulted in difference scores of all 1s. This did not provide any variation to be averaged into the reference template. It was as if one reading had been used to build the template. These two subjects were reenrolled using the hand removal procedure.

### 3. Experiment Sessions

The experiment ran for a period of eight weeks immediately following the enrollment of all 108 subjects. It was conducted in two parts. Part 1 covered the first 3 weeks. During this part, the subjects used the hand reader daily Monday through Thursday of each week. Three identity verification attempts were made each day by following the operating instructions read and discussed during enrollment. These instructions were posted beside the hand reader for easy reference by the subjects. The IBM computer recorded the difference score of each attempt, and also displayed whether the subject had been identified. In addition to the difference score, which was the result of comparing the new hand picture to the reference template, the computer stored the complete hand picture with the time, date, and PIN for every hand reading. All of this information for every access attempt, whether identification was verified or not, was recorded and saved. Storage of this data permitted retrospective analysis of which subjects would have been correctly identified using different threshold settings. This data also enabled reference templates to be built using various numbers of hand pictures, and allowed the experiment to be re-run on these templates without requiring additional hand readings from the test subjects.

Part 1 of the experiment was followed by a three week time lapse during which the test subjects did not use the hand geometry device. Part 2 then began, and covered a two week time period. During part 2, the test subjects made identity verification attempts exactly as they had done in part 1. Three attempts were made each day Monday through Thursday for two weeks. The only instructions given to the subjects at the beginning of part 2 were simplified written instructions as shown in Figure 2.4. As in part 1, the comparison difference scores as well as the complete hand picture, time, date, and PIN were recorded so that retrospective analysis and experiment reconstruction could be accomplished.

## OPERATING INSTRUCTIONS



1. IF WEARING RING, TURN STONE UP.
2. ENTER ID # (Eg. 1234#).
3. SPREAD FINGERS.
4. SLIDE HAND FORWARD UNTIL IT BUMPS AGAINST WEB PIN.
5. PRESS HAND FLAT AGAINST SURFACE.
6. CLOSE FINGERS AGAINST PINS.
7. HOLD UNTIL LAMP GOES OUT.

Figure 2.4 Part 2 Operating Instructions.

### III. RESULTS AND DISCUSSION

The ID-3D Hand Geometry Identifier is one of many different types of biometric access control devices now available. The suitability of this device for C3 applications depends primarily on its Type I and Type II error rates, but is also a factor of other measures of effectiveness such as time to achieve recognition, administration, convenience to user, costs, and equipment reliability.

#### A. TYPE I AND TYPE II ERRORS

As mentioned in section II B, Type I errors are those which falsely reject an authorized user, while Type II errors are those which falsely accept an unauthorized user. These two types of errors must be considered together, and the results of experiments determining these two types of errors can best be discussed by using error curves (FIBS Pub 48, 1977). Error curves are really two curves in one. Figure 3.1 is a plot of the error curves for the preferred performance of a biometric device. These curves are preferred since they show results from a biometric identification device which are as ideal as can be expected. This graph will be used to explain this system of curves. The vertical scale is in units of percent of total access attempts. It is scaled from 0% to 9%. The horizontal scale is in units of the device's particular threshold setting. For the ID-3D Identifier, the horizontal scale is in units of difference between an individual hand reading and its corresponding reference template. This scale ranges from 0 to 150, and each interval is 20 units wide.

The Type I (false reject) error curve slopes downward to the right. It tells what percent of the authorized user's hand readings would be rejected at a particular threshold setting. For example, in Figure 3.1, if the threshold is set at 60, 4% of the access attempts by authorized users would result in false rejects. This also means that 4% of the hand readings differed from their corresponding templates by more than a difference of 60.

The second curve in Figure 3.1 is the Type II (false accept) error curve. It slopes downward to the left, and shows what percent of the impostors would be falsely accepted at a particular threshold setting. In this curve, again representing a preferred performance, 0.7% of the impostors would be accepted at a threshold setting of 120. This also means 0.7% of the impostors had a hand reading which differed from an authorized user's reference template by less than 120.

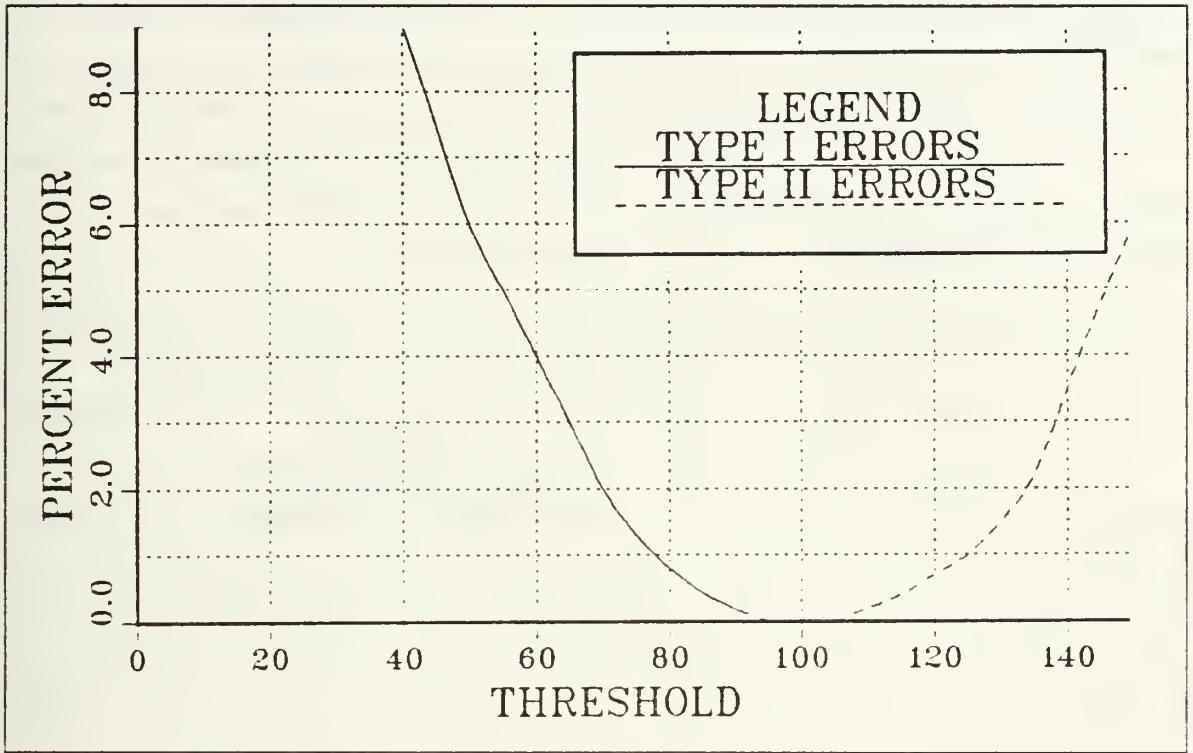


Figure 3.1 Preferred Performance of Biometric Access Device.

The preferred performance curves of Figure 3.1 show that the Type I and Type II error curves do not cross. This means that for a threshold setting anywhere between 95 and 105 no authorized users would be rejected, and no impostors would be accepted. This is an ideal situation. Usually this situation cannot be obtained, and error curves like those in Figure 3.2 are more realistic. This figure shows that the Type I and Type II error curves cross over. This means there is no threshold setting which will eliminate both types of errors. In this situation,

if the threshold is set at the point where the two curves cross over, this is referred to as the "equal error" setting. This is the point at which the Type I and Type II error rates are equal, and the percentage of correct individuals being falsely rejected will equal the percentage of imposters being accepted. The error at this point is a single number which is to be used in describing the performance of such devices. (FIBS Pub 83, 1980, pp. 17)

In Figure 3.2, the equal error rate exists at a threshold setting of 90, and the equal error point is 1%. This means 1% of the authorized users will be rejected, and at the same time, 1% of the imposters will be accepted with the threshold setting at this equal

error point. This single number, the equal error point, describes the performance of a biometric device. Settings above and below will favor one error rate at the expense of the other. Error curves like those in Figure 3.2 will be used to examine the various Type I and Type II errors which resulted from different threshold settings, a time lapse in use by the test subjects, and construction of the reference templates from different numbers of hand readings for the ID-3D Identifier experiment.

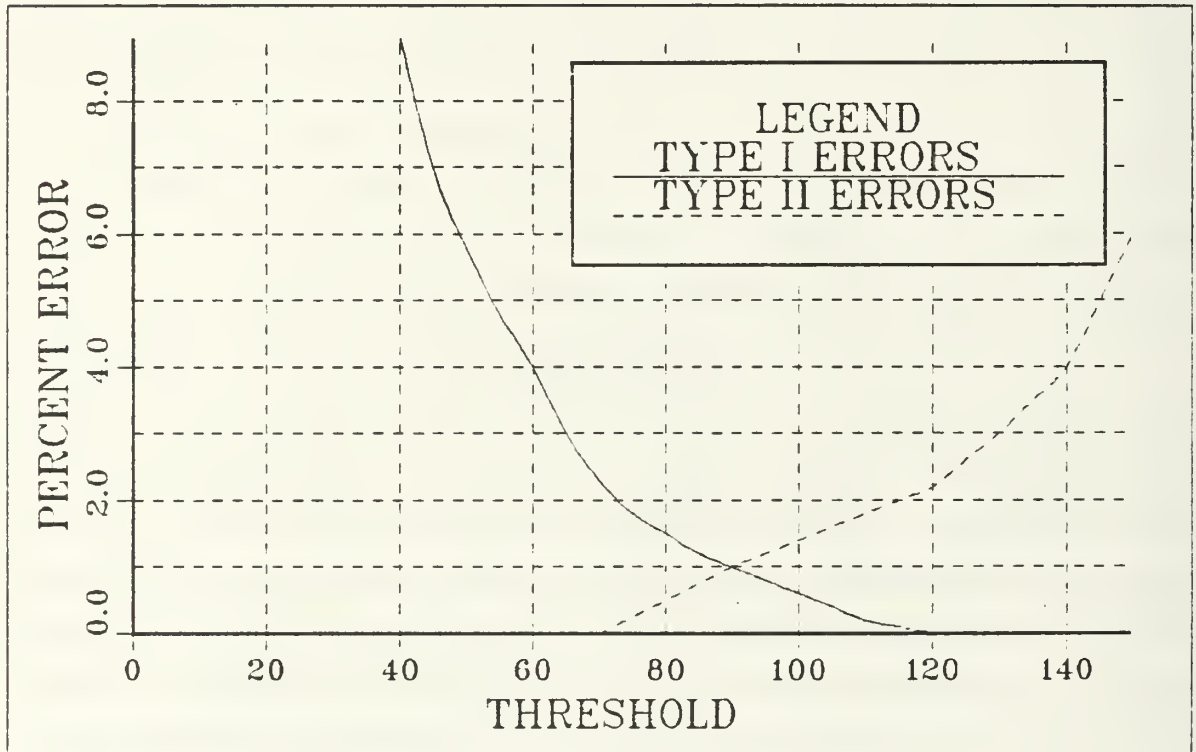


Figure 3.2 Realistic Error Curves For Biometric Access Devices.

### 1. Different Threshold Settings

The major factor in determining the reliability of a biometric access control device is its Type I and Type II errors at various threshold settings. In this ID-3D Identifier experiment, the Type I errors for the entire range of threshold settings from 0 to 150 were obtained. The actual threshold setting for this experiment was always 100, but this setting was not significant since the difference scores of all hand readings were recorded. The percentage of these recorded differences above a particular threshold provided the Type I errors for that threshold. Operationally, the threshold setting can be adjusted by the system operator. This is done through a menu formatted control

program in the enrollment terminal. The operator selects 'diagnostics and setup' from the main menu, and then selects 'change setup values' from the diagnostic menu. The new threshold value is then prompted for. Once the threshold setting is entered, it is automatically transmitted to the hand reader.

The Type II errors were able to be obtained through a comparison process since all of the reference templates were stored. To do this, the hand reader test system was configured so that each individual reference template could be used as a single hand reading. Each individual reference template, as a single hand reading, was compared to each of the other templates as if it was an access attempt using the PIN of the other templates. A difference score for each comparison was obtained, and any difference below that of a particular threshold constituted a Type II error for that threshold. The entire range of threshold settings from 0 to 150 was again considered. This method of obtaining Type II errors provided results as accurate as if each subject used the PIN of all other enrollees to make access attempts, and was much more timely.

The total number of Type I and Type II errors for all hand readings for the entire experiment are plotted in Figure 3.3. These errors, calculated from all readings for the entire experiment, are also summarized in Table 1. Figure 3.3 and Table 1 show that the threshold setting which produced equal Type I and Type II errors was 100. The error rate at this equal error point was 0.62%. These error curves also show there is a trade off between Type I and Type II errors. If a very low Type I error rate is required, then a threshold setting must be used which gives a higher Type II error rate. Also, the Type I error curve never goes to 0.0%. This is due to the fact that one mistake by a subject in accomplishing a hand reading will give a difference score of 400. This large score will be a Type I error and will always be considered in determining the error percentage. A strategy for dealing with this situation is discussed in section III, A, 5. The Type II error curve does go to 0.0%, but at a threshold setting which gives a very large Type I error rate. In figure 3.3 a threshold setting of 50 eliminates all Type II errors but allows a 7.0% Type I errors. If an operational situation requires security measures to prevent the false acceptance of all unauthorized users, many authorized users would be falsely rejected. This would be inconvenient, and procedures to deal with this situation would have to be developed.

A number of factors influenced the percentages of Type I errors. First, a significant number of the subjects wore large class rings on their identified hand. These

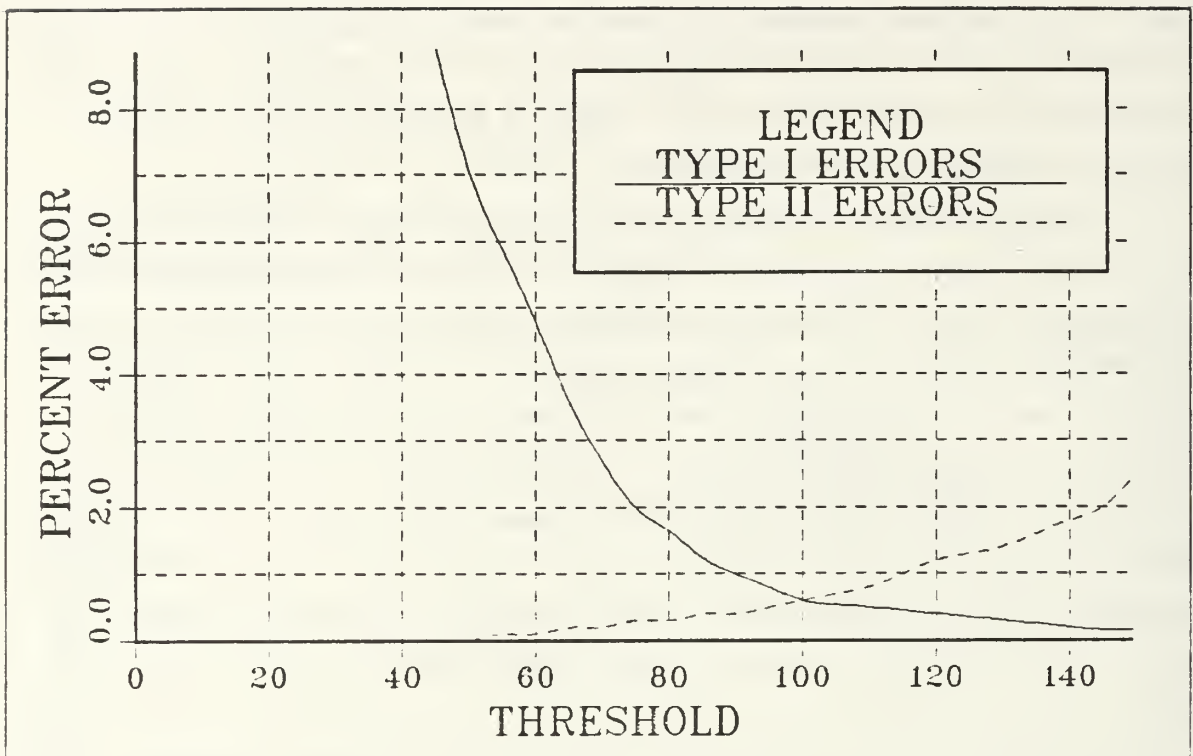


Figure 3.3 ID-3D Identifier Test Results.

TABLE I  
TYPE I AND TYPE II ERROR RATES

| Threshold Setting | Type I Errors | Type II Errors |
|-------------------|---------------|----------------|
| 40                | 13.29%        | 0.00%          |
| 60                | 4.87%         | 0.07%          |
| 80                | 1.65%         | 0.37%          |
| 100               | 0.62%         | 0.62%          |
| 120               | 0.44%         | 1.15%          |
| 140               | 0.31%         | 1.96%          |

rings presented a problem since the ring often rotated towards the little finger. The ring's stone then formed a false web between the ring and little finger. This resulted in large dimensional measurement errors and inflated difference scores. Subjects who saw these large difference scores on initial readings were able to correct the problem in later

readings by rotating the ring's stone upwards before taking the hand readings. This alleviated the problem.

A second factor which caused variation in the hand readings and large difference scores was frequent 'playing' with the system by the test subjects. Since use of the hand reader was totally unsupervised, subjects often experimented on their own. They tried other subjects PINs, used incorrect hand positions, moved their hand during the reading, and placed foreign objects on the measuring platen along with their hand. This 'playing' with the system was easily detected, but did cause inflated difference scores, and would not occur in an operational setting where identification is required to gain access.

A third factor was the prevalence of hand readings where there was a significant rotation of the hand on the measuring platen. This happened because the hand reader occasionally moved to squarely face the subject and became centered on his body. This forced the wrist to be cocked at an angle, and encouraged hand rotation. All subjects were seated while making hand readings, and the location of the chair may have contributed to this problem. In an operational situation, users would use the hand reader while standing to eliminate this problem.

One factor which shifted the Type II error curve to the left, that is caused a higher rate of errors at all threshold settings, is the narrow range of hands in the test population. The Naval Postgraduate School subjects, coming from a narrow age group, being predominately male, and having very similar vocational backgrounds, were less diverse than a normal test or operational field would be. This caused lower difference scores when comparing one reference template to all other templates to determine Type II errors.

## 2. Time Lapse

A second factor in determining the reliability of a biometric access device is the changes in error rates after a time lapse during which the device is not used. This is especially important in a device that measures an attribute which is subject to change. To examine this factor, a time lapse of three weeks occurred between parts 1 and 2 of this experiment. Type I and Type II error rate curves for each part were then calculated separately. Error curves for part 1 are in Figure 3.4. Error curves for part 2 are in Figure 3.5. The equal error point for Type I and Type II errors during part 1 was at a threshold difference of 98 with errors of 0.52%. The equal error point during part 2 was at 104, with equal errors of 0.75%.

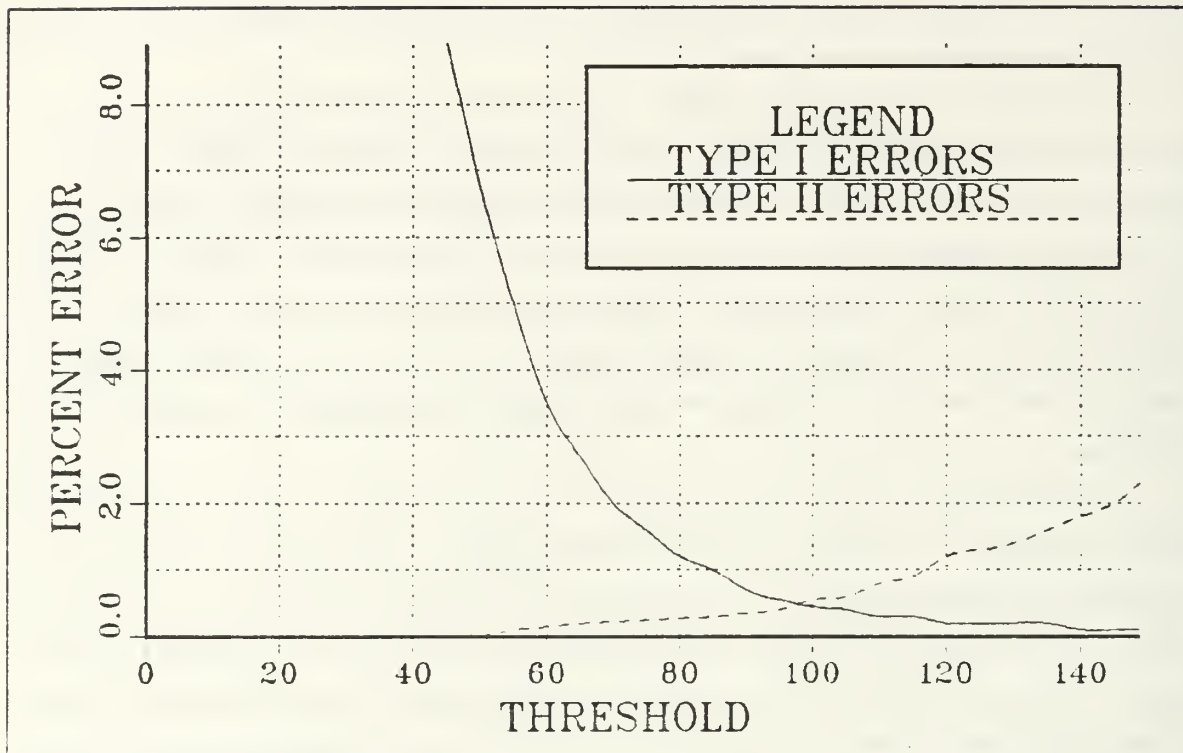


Figure 3.4 Type I and Type II Errors During Part 1.

The number of Type II errors could not be recalculated for part 2 since Type II errors were determined from the reference templates made during enrollment. Those reference templates were not reaccomplished during part 2. Therefore, the Type II error curves for both parts 1 and 2 in Figures 3.4 and 3.5 are identical.

A comparison of the Type I errors for parts 1 and 2 of the experiment is in Table 2. This comparison shows that the percentage of Type I errors at each threshold setting increased after the three week time lapse during which the test subjects did not use the device. Two factors must be considered in accounting for this change. First, the learning curve came into play after resuming use of the hand reader. As part 2 began, test subjects were given only limited written instructions to remind them of the necessary procedures. Certain subjects took a number of access attempts to reacquaint themselves with the necessary techniques to use the hand reader. This caused an increase in the difference scores, and thus an increase in Type I errors. A second factor affecting the Type I error rates was changes in the subjects hands. In two cases, hand injuries had occurred which caused significant changes in the hand's geometry. In other cases, different rings were being worn which also affected the hand readings and

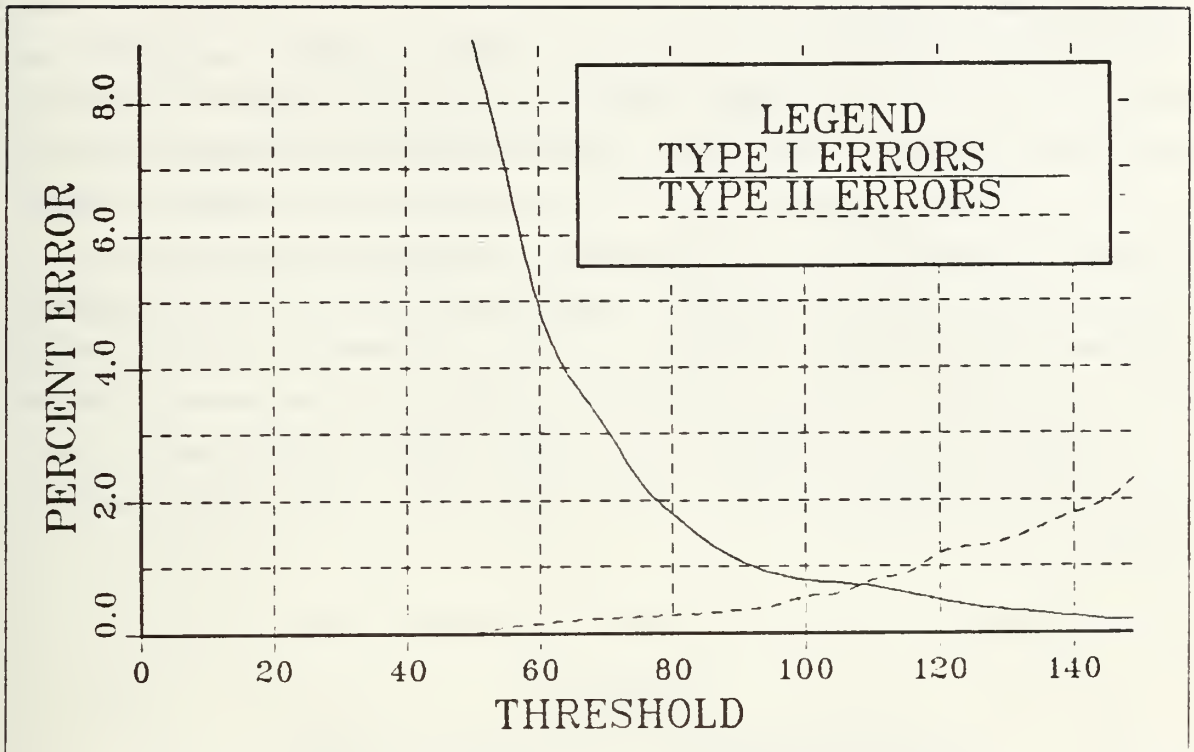


Figure 3.5 Type I and Type II Errors During Part 2.

increased the difference scores. The effect of these factors could have been overcome by providing more explicit instructions and reenrolling select individuals at the start of part 2.

TABLE 2  
TYPE I AND TYPE II ERRORS FOR PARTS 1 AND 2

| Threshold Setting | Part 1 Type I Errors | Part 2 Type I Errors |
|-------------------|----------------------|----------------------|
| 40                | 9.80%                | 25.60%               |
| 60                | 3.53%                | 4.78%                |
| 80                | 1.23%                | 1.75%                |
| 100               | 0.45%                | 0.79%                |
| 120               | 0.23%                | 0.46%                |
| 140               | 0.18%                | 0.37%                |

### 3. Template Construction

In normal use of the ID-3D Identifier, a reference template is constructed by averaging five individual hand readings. That is what was done during the enrollment process of this experiment. Those reference templates, made from five hand readings, were then used to determine all of the Type I and Type II errors which have been discussed to this point. However, it is possible to make reference templates from any number of hand readings. Since all of the dimensional data from every hand reading was recorded in this experiment, templates were later constructed from 1, 2, 4, 5, 6, 8, and 10 hand readings. The entire experiment was then rerun against each of these newly constructed reference templates. The results provided threshold settings and rates for equal errors while using each of these new templates. These results are shown in Table 3.

TABLE 3  
CHANGES IN TEMPLATE CONSTRUCTION

| Readings Per Template | Equal Error Threshold | Equal Error Rate |
|-----------------------|-----------------------|------------------|
| 1                     | 112                   | 0.85%            |
| 2                     | 105                   | 0.73%            |
| 4                     | 104                   | 0.63%            |
| 5                     | 100                   | 0.62%            |
| 6                     | 100                   | 0.61%            |
| 8                     | 99                    | 0.58%            |
| 10                    | 99                    | 0.56%            |

The data in Table 3 shows that a template made from 4 to 6 readings is a good compromise between convenience and performance. One or two readings do not provide enough variation to form a suitable template. Using up to 10 readings continues to increase performance, but not at a rate great enough to offset the additional time required to make such a template.

### 4. Updating Algorithm

The performance of a biometric identity verifier is dependent upon the quality of the template created during the enrollment process (Stein, 1985). This is the time when the user is most unfamiliar with the verifier, and is apt to be nervous and tense.

Consequently, the template is not as likely to accurately represent the users biometric characteristics, as compared to the accuracy of measurements taken after the device has become familiar and a habitual pattern of use developed. Also, there may be some long term changes in the biometric attribute which would cause a loss in performance of the device over a period of time.

In order to accommodate these possibilities and thereby improve performance, the makers of the ID-3D Identifier developed a reference template updating algorithm for their device during this experiment. This algorithm adjusts the template after each successful verification to accommodate changes in the measured hand. This new algorithm was installed in the Test System. an initial reference template made from the first 5 hand readings, and the experiment rerun. This was possible because all of the hand readings had been stored. The results of this new test are shown in Figure 3.6.

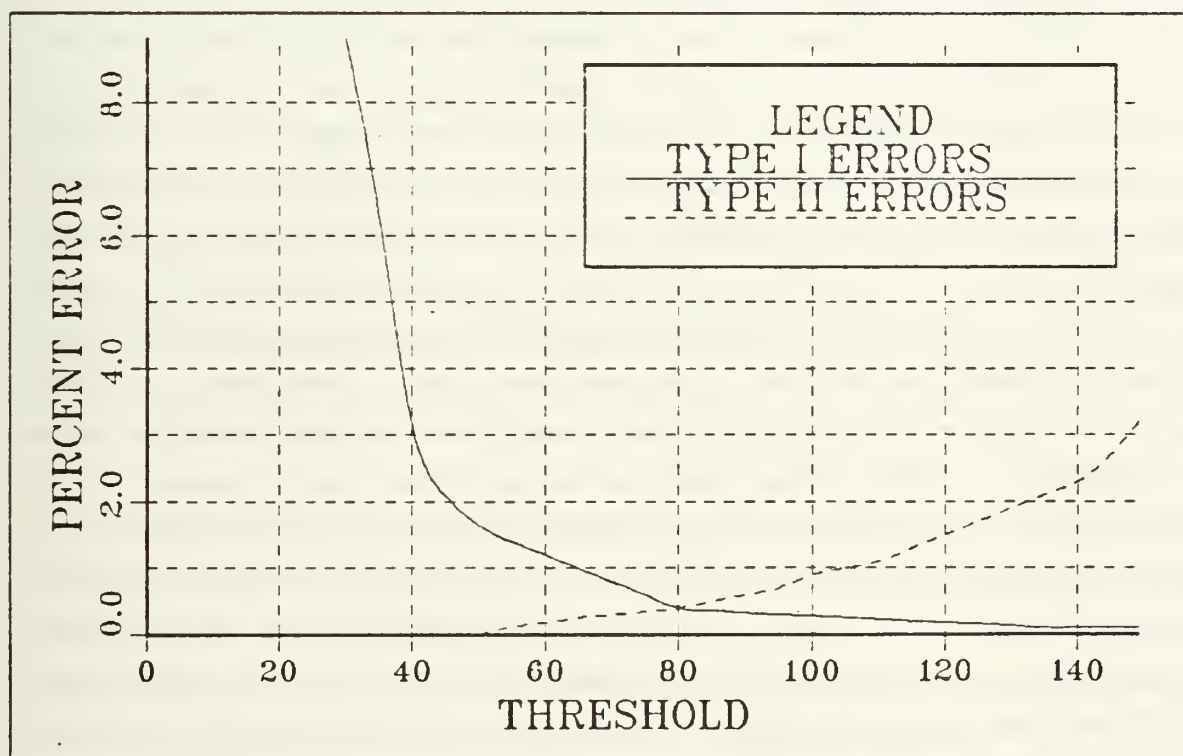


Figure 3.6 Test Results With Updating Algorithm.

The information in Figure 3.6 is directly comparable to that in Figure 3.3 as the identical data set was used. This data includes all hand readings for the entire experiment. Use of the updating algorithm reduced the equal error rate from 0.62% to

0.40%. Similar results can be seen by looking separately at each part of the experiment. With the updating algorithm, the equal error rate for part 1 dropped from 0.52% to 0.31%. For part 2, the drop was from 0.75% to 0.51%.

With the updating algorithm, the number of hand readings used to make the initial reference template is of little importance over the long run. When initial templates were made from 1, 2, 4, 5, 6, 8, and 10 readings, and the data from the entire experiment rerun using the updating algorithm, equal error rates of 0.39%, 0.41%, 0.38%, 0.40%, 0.39%, 0.37%, and 0.38% were obtained. There was little change in these equal error rates since all errors in the template were overcome by the updating algorithm. With this new algorithm, initial reference templates can be made from one hand reading.

### 5. The Three Try Strategy

Operational identity verifiers are frequently programmed so that no penalty is invoked until after three consecutive rejects (Maxwell, undated). This allows a careless user a second and third try to be correctly identified. All of the experiment results reported so far have been based on a single try basis. However, each subject did make three hand readings at each daily measurement session. The recording of each of these readings allowed retrospective determination of error rates in the case of a three try strategy.

The consequences of a three try strategy were examined for threshold settings of 50, 60, 70, 80, 90, and 100. To do this, all hand readings with a difference of less than 50 were first removed. Next, any session which now contained less than three trials was removed. This was able to be done because, if one trial in a session had a difference below 50, that session would have been successful at a threshold setting of 50. What remained was records for all sessions in which all three readings for a session were greater than 50. For each of these groups of three readings, the minimum difference was then noted. If the decision threshold had been set below this minimum, then all three tries, and thus the group, would have been rejected. The group would then be classified as a false reject (Type I error). This procedure was done for both the case of template updating and fixed template operation, and the results are in Table 4.

In Table 4, the **Number** row shows the number of three try groups whose lowest difference score was in the difference range for that column. The **Number Above** row shows the total number of groups that were above the minimum value of the range for that column. This **Number Above** row shows the number of groups of false

TABLE 4  
THREE TRY STRATEGY RESULTS

| Without Template Update |       |       |       |       |       |      |
|-------------------------|-------|-------|-------|-------|-------|------|
| Difference              | 50-59 | 60-60 | 70-79 | 80-89 | 90-99 | 100+ |
| Number                  | 45    | 17    | 6     | 4     | 2     | 0    |
| Number Above            | 74    | 29    | 12    | 6     | 2     | 0    |
| Type I                  | 3.5%  | 1.4%  | 0.6%  | 0.3%  | 0.1%  | 0.0% |
| Type II                 | 0.1%  | 0.1%  | 0.2%  | 0.4%  | 0.6%  | 0.6% |
| With Template Updating  |       |       |       |       |       |      |
| Difference              | 50-59 | 60-69 | 70-79 | 80-89 | 90-99 | 100+ |
| Number                  | 34    | 13    | 8     | 2     | 2     | 0    |
| Number Above            | 59    | 25    | 12    | 4     | 2     | 0    |
| Type I                  | 2.8%  | 1.2%  | 0.6%  | 0.2%  | 0.1%  | 0.0% |
| Type II                 | 0.1%  | 0.1%  | 0.2%  | 0.4%  | 0.5%  | 0.6% |

rejects that would result from using a three try strategy at a threshold set at the minimum of that column. There were 2100 three try trials by authorized users in the test. By dividing the Number Above row by 2100, the percent of Type I errors can be found. This percentage is listed in the **Type I** row. The **Type II** row indicates the Type II error rate corresponding to a difference threshold equal to the minimum range of the column. These Type II error rates were read directly from Figure 3.3 for the algorithm that did not update, and from Figure 3.6 for the algorithm which did.

The three try strategy improved the identity verification performance characteristics. Without template updating the equal error rate dropped from 0.62% to 0.36%, and with template updating it dropped from 0.40% to 0.33% using three tries instead of one. These improvements occurred because the false rejections due to incorrect placement of the hand on the platen or other test subject mistakes were eliminated. No adjustment was made in the Type II error curves to allow for a three try strategy. This is because the difference between the template and the imposter hand reading was so great there was no chance a second or third attempt would be successful. Each Type II error from a single try would also result in an error on the second and third try. Therefore, the number of single try errors based on all attempts would yield the same percentage as all group errors based on the total number of three try groups. The three try Type II curve would therefore be the same as the single try curve.

## **6. Biometric Device Comparison**

In addition to hand geometry, five other human biometric features or actions have been used to develop identity verification devices. They include eye retinal pattern, fingerprint, signature dynamics, and voiceprint. These devices have been under development for about ten years, and were tested by the Sandia National Laboratory, New Mexico in April-June 1985 (Maxwell, undated). This was a laboratory type operational evaluation using 40 Sandia employees making two entry attempts a day for 60 days. This test was totally supervised, with the supervisor present every time a subject made an access attempt. False rejects (Type I errors) were obtained using the threshold settings suggested by the manufacture. False acceptance (Type II errors) were obtained by having each subject key in the PINs of all other enrollees, and presenting the appropriate feature or performance sample for verification. The results from the eye retinal pattern device were the most favorable. A 12.4% Type I error occurred, but 0.0% Type II errors existed. For the fingerprint device, 19.7% Type I and 10.5% Type II errors were recorded. For the signature dynamics machine, 15.1% Type I and 5.8% Type II errors were obtained. The voiceprint device recorded 9.5% Type I errors, and 17.7% Type II errors. These rates all pertain to single try attempts, and the results could be substantially different under different environments and using different procedures. The ID-3D Identifier performed better than all of these devices except for the Type II error testing of the retinal eye pattern machine.

### **B. OTHER MEASURES OF EFFECTIVENESS**

A number of measures of effectiveness in addition to Type I and Type II errors must be examined to determine the suitability of the ID-3D Hand Geometry Identifier. These include time to achieve recognition, administration, convenience to user, costs, and equipment reliability.

#### **1. Time to Achieve Recognition**

The time to achieve recognition is made up of the time required to activate the hand reader, acquire the actual hand reading, retrieve the template, complete the correlation process, and effect acceptance or rejection. These times are important when considering access control to C3 facilities, and could become critical when a number of users must gain access when time is limited. The total time to attempt recognition for each access trial in this experiment was less than 3 seconds. This time

was the same whether identification was verified or not. Of course, if identification was not verified, additional trials would be required which would double or triple the 3 second time requirement. Throughput of persons using the ID-3D Identifier was typically 7 persons per minute for this experiment.

## **2. Administration**

High level security systems in use today can require a great deal of administration. Much of this administration is in controlling and changing the entrance artifacts, whether they be keys, passwords, or combination locks. There are numerous precautions which must be taken when passwords and key-cards are utilized under the guidelines of the National Computer Security Center (DODCSC, 1985). Most of this administration could be alleviated through the use of a hand geometry biometric access control device. With this device, the administration would primarily be encompassed in user enrollment. The enrollment time for subjects in this test took less than 4 minutes per subject.

## **3. Convenience to User**

For a personal identification system to gain acceptance, it must be reasonably convenient. Otherwise, it could be regarded as an impediment and may even be circumvented. Convenience also includes how easy it is to learn to use the system. The ID-3D Identifier is very user friendly. It uses a totally noninvasive measuring device which was quickly accepted by all test subjects. A small degree of cooperation was required, but persons of every background quickly learned to use the system. Two subjects did have some difficulty being recognized on their first attempts a number of days. This difficulty can most likely be attributed to the enrollment. If these individuals had been reenrolled after they had become familiar with the equipment, their difficulties would have been eliminated.

## **4. Costs**

The ID-3D Identifier can be used as a self-contained device. It can also be part of an integrated system requiring support functions from a central computer. As a stand alone device, the ID-3D Identifier costs \$3,500. This includes the hand reader, the enrollment terminal, and a tape recorder to store the reference templates. This cost is on the low end of a \$2,000 to \$12,000 price range of per terminal costs for various types of biometric devices (Bakke, 1986).

## 5. Equipment Reliability

Reliability can be defined as the probability that the device will perform its intended function over a specified period of time. As applied to equipment performance, reliability refers to the ability to continue operating at the desired level of effectiveness without drifting out of tolerance or breaking down. There was no evidence that either of these faults occurred in the ID-3D Identifier during this test. The equipment functioned as required throughout the five weeks of the experiment. The only operator assistance required came after a power failure. When this happened, the hand reader's programmable memory lost the reference templates. These templates had to be reloaded from the Test System computer, just as they would have to be reloaded from a tape recorder in actual operation. This procedure takes less than 10 seconds to accomplish. The ID-3D Identifier is designed so that it is fail-safe. That is, it denies access if a failure occurs or the power is shut off. Also, it has built in detectors which warn against any tampering. The ID-3D Identifier will allow for multiple identification attempts as may be needed in the three try strategy, but this number is limited to thwart an imposter who might try to gain access by trial and error.

## C. C3 APPLICATIONS

Command, Control, and Communications (C3) and its numerous sister terms, Command and Control (C2), Command, Control, Communications, and Intelligence (C3I), and Command, Control, Communications, and Computers (C4) are all somewhat ambiguous. In fact, they can all mean almost anything from military computers to the art of generalship, whatever the user wishes them to mean (Moll, 1978). A good place to start in defining these terms is the official Department of Defense definition for Command and Control.

A Command and Control system consists of an arrangement of personnel, equipment, facilities, communications and procedures that are employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JOPS, Vol I, 1976, pp.6)

C2, and therefore C3, consists of the physical entities of facilities, equipment, and communications. These physical entities must be protected at all times, and the ultimate authority for granting access to sensitive information and facilities rests with the commanding officer (OPNAVINST 5510.1G, 1984). Physical security is the most

important countermeasure to penetration, so access to facilities, equipment, and communications must be tightly controlled (SECNAVINST 5500.31A, 1985).

Access to C3 facilities and systems is presently controlled by security guards, keys, passwords, badges, or key-cards. Technology exists to augment these methods with biometric access devices. If properly used, biometric access devices can ensure positive identification with a high level of confidence, provide an accurate audit of a facilities use, and significantly reduce the administrative burden associated with protecting C3 systems.

The level of security required at a particular facility varies because of the nature of the facility, and the type of threat against it (Barker, 1984). However, positive identification of people using sensitive facilities is always required, and biometric access control devices can meet that need. These devices are not perfect, as this hand geometry test points out, but they eliminate the vulnerabilities of being lost, stolen, or duplicated. Also, the threshold settings on the biometric devices can be set to provide the desired level of security. In using these biometric devices, there is always the trade off of increasing one type of error in order to reduce the other type. If a facility must be protected to the extent that no impostors can be allowed, that is no Type II errors, then the device's threshold setting must be low. This would increase the number of false rejects, Type I errors, and this inconvenience would have to be accepted. Conversely, if the level of security was such that the risk of accepting an impostor was low, but no authorized users could be rejected, the threshold could be moved to a high setting. This decision would have to be made at each facility by the commander upon recommendation of the security officer. The ID-3D Identifier has the capabilities to meet the requirements, regardless of the results of this decision, by using a three try strategy and an updating algorithm.

The US Air Force has been directed as the lead agency to develop equipment to automate physical security access control (DOD Directive 3224.3, 1984). As such, they have provided guidelines as to the capabilities of automated systems. Their guidelines provide performance standards for all advanced entry control systems. These standards state that a goal of 0.0% of both Type I and Type II errors should be sought, but that the minimum requirement for Type I errors is 3.0% and for Type II errors is 1.0% (OCSE, 1984). These are only minimums since the final decision of how stringent the access control must be remains with each individual commander. The ID-3D Identifier exceeded these minimums in every configuration examined in this test. It is a valid

device for use in ensuring positive identification in C3 applications. This technology is a secure way to replace the existing means to gain access and to verify individual identity. If the risk of unauthorized access is high, as it is in C3 applications, a hand geometry biometric device can be installed to replace key-cards, identification badges, and passwords. At command posts, an ID-3D Identifier could be used to ensure only those persons appropriately cleared be allowed to enter. At communication facilities, the device could verify the identity of all who receipt for messages. At terminals tied to the local area network of a command staff, the ID-3D Identifier could ensure only those authorized to use the network gained access.

Access control should include provisions for the logging of access to a facility in order to provide a record of who used the facility and what information was accessed (FIBS Pub 48, 1977). For C3 facilities, information would be very useful in discovering, tracing, and preventing intrusions. If a security violation were discovered at a C3 facility, a log of who used the facility at what times would be very helpful in determining the cause of the violation and the extent of the resulting damages. Presently an audit trail of facility use is seldom accomplished at C3 facilities. If a log is kept, it is done manually at great expense in time and personnel. If set so as to detect all unauthorized users, biometric access control devices can automatically provide a complete list of who used a facility and what information they accessed. The ID-3D Identifier has the capability of printing this log either locally or remotely, and can also provide a complete record of usage in a system computer (Users Manual, 1986). This audit providing capability of the ID-3D Identifier makes it very suitable for C3 applications.

C3 facilities are continually employing increasing numbers of computer systems to assist military commanders fulfill their missions. Access to these computer systems is presently accomplished by using passwords. Since passwords can be easily compromised, their use is very vulnerable. Also, passwords require a great deal of administrative effort. In fact a lengthy guideline has been published which outlines all of the steps that must be taken to correctly use passwords in granting access to classified information (DODCSC STD 002-85, 1985). The steps in this guide are very manpower intensive, and yet do not eliminate all of the vulnerabilities. An ID-3D Identifier can provide the positive identification required to check clearances and grant access to computer systems. This automatic device is very suited to accomplishing these tasks as a stand alone device or when connected to a host computer. The ID-3D

Identifier is well suited to replacing passwords and their lengthy administrative requirements.

With the increased use of computers in C3 tasks, a corresponding increase in the use of databases has resulted. These databases contain large amounts of data from which processors draw to aid commanders make informed decisions. They must be protected from unauthorized reading and unauthorized manipulation. Also, these databases often store information in several classification levels to economize on space and to increase convenience. This information is divided into segments and each segment contains a different type of information accessible by a specific group of people. This requires that a person accessing a segment of a database be in fact the person who he says he is, and also be authorized to use that segment. Positive identification with little administrative involvement is required. This can be done by replacing passwords which are presently used to access database segments with hand geometry biometric devices. These devices can be sequentially used to identify and grant access to various segments of a database. With this approach to positive identification, there are no passwords to be compromised and an audit trail is available to identify who accessed what information at what time.

Hand Geometry identification techniques are very applicable in protecting C3 facilities and systems. Positive identification can be ensured with a high degree of confidence so that access control can be automated. A complete audit trail can be provided which acts as a deterrent to intruders and aids in the investigation if a violation occurs. A significant reduction in the administration of the security aspects of C3 systems would occur if passwords were replaced. C3 facilities must be protected from unauthorized use, and hand geometry access devices can accomplish this priority task.

## IV. CONCLUSIONS AND RECOMMENDATIONS

The ID-3D Hand Geometry Identifier proved to be an effective biometric identity verification device for a number of specific requirements. This experiment demonstrated that the ID-3D Identifier can maintain a false rejection of authorized users (Type I) error rate of 0.2%, and at the same time a false acceptance of impostors (Type II) error rate of 0.4%. These results were realized at a threshold setting of 80 using the three try strategy and the reference template updating algorithm. The three try strategy with reference template updating is how the ID-3D Identifier should be used since that is how the best results are obtained. However, a single try strategy with an algorithm which did not update also produced an equal Type I and Type II error rate of 0.62%, which is better than the minimum requirement. A period of time when subjects did not use the device increased the equal error rate only slightly from 0.52% to 0.75%. If the updating algorithm was used both before and after this time lapse, the increase was from 0.31% to 0.40%. Constructing reference templates from different numbers of hand readings had little effect while using the updating algorithm. With the nonupdating algorithm, five hand readings is the most logical number to use in making the reference template.

The ID-3D Identifier performed as advertised during this experiment. It exceeded the published and previously tested equal error rate of 0.5% while employing a three try strategy using the updating algorithm. It is also a fast, noninvasive, user friendly identification device. It is of low cost and very equipment reliable. It is a device worthy of consideration for automating access control techniques.

Security requirements have dictated the necessity to upgrade and automate the access control requirements at C3 facilities. There are inherent vulnerabilities in using today's keys, badges, passwords, and key-cards. Hand geometry devices like the ID-3D Identifier have the capabilities to reduce these vulnerabilities. They can ensure positive identification with a high level of confidence, significantly reduce the security administrative burden, and provide an accurate audit trail of facility use. The decision whether or not to use a biometric access control device must remain with individuals at each C3 facility, based on their need, but the ID-3D Identifier exceeds the minimum requirements, and so represents a possible solution.

There are some areas of study which should be accomplished to further verify the capabilities of the ID-3D Identifier. First, the magnitude of the learning curve associated with using the ID-3D Identifier should be determined, as well as how to best employ this information. Second, an operational test should be conducted and the operational performance compared to these experiment results. Third, the Type I and Type II errors when the number of reference templates in memory approaches the maximum of 10,000 vice the 108 in this experiment should be tested. Fourth, a cost benefit analysis should be accomplished at a variety of C3 facilities to determine what savings would result from using an ID-3D Identifier for access control.

## LIST OF REFERENCES

Bakke, T. O., "Foolproof ID With New Body-Language Security System", *Popular Science*, vol 228, June 1986

DOD 5200.1-R, Department Of Defense Regulation, *Information Security Program Regulation*, December 1982

DODCSC, *Department of Defense Password Management Guideline*, Computer Security Center STD-002-85, US Government Printing Office, April 1985

DOD Directive 3224.3, *Physical Equipment Security*, Department of Defense Directive, December 1976

FIPS, Federal Information Processing Standards Publication 48, *Guidelines on Evaluation of Techniques of Automated Personal Identification*, US Department of Commerce, National Bureau of Standards, April 1977

FIPS, Federal Information Processing Standards Publication 83, *Guidelines on User Authentication Techniques for Computer Network Control*, US Department of Commerce, National Bureau of Standards, September 1980

Forsen, G. E., Nelson, M. R., Staron, R. J., *Personal Attributes Authentication Techniques*, Rome Air Development Center, October 1977

*Government Computer News*, US Printing Office, Washington, DC, 19 July 1985

JOPS, *Joint Operations Planning System*, Vol I, Joint Chiefs of Staff, SM-776-76, September 1976

Maxwell, R., *The Status of Personal Identity Verifiers*, Sandia National Laboratories, Albuquerque, New Mexico, undated

Moll, Kenneth L., "Understanding Command and Control", *Defense and Foreign Affairs Digest*, June-July 1985

OCSE, *Operational Concept for Security Equipment Advanced Entry Control Procedures*, Headquarters Air Force Office of Security Police, November 1984

OPNAVINST 5510.1G, *Information and Personnel Security Program Regulation*, Department of the Navy, April 1984

Riganati, John P., *An Overview of Electronic Identification Systems*, Proceedings of Wescon, September 1985

SECNAVINST 5500.31A, *Technical Surveillance Countermeasures (TSCM) Program*, Secretary of the Navy Instruction, OP-009D, June 1985

Sidlauskas, Dave, *Hand Geometry Test System Manual*, Recognitions Systems, Inc., Revision 0.1, October 1986

Sidlauskas, Dave, *The Future Is Now*, Productivity Products, March 1986

Stein, William M., *Standardized Testing of Personnel Identification Equipment*, The MITRE Corporation, March 1985

*Users Manual*, Revision 0.1, Recognition Systems, Inc., ID-3D-ST, 1986

## INITIAL DISTRIBUTION LIST

|     |  | No. Copies |
|-----|--|------------|
| 1.  | Defense Technical Information Center<br>Cameron Station<br>Alexandria, Virginia 22304-6145                             | 2          |
| 2.  | Library, Code 0142<br>Naval Postgraduate School<br>Monterey, California 93943-5002                                     | 2          |
| 3.  | Superintendent, Code 55NI<br>ATTN: Prof. D. E. Neil<br>Naval Postgraduate School<br>Monterey, California 93940-5000    | 1          |
| 4.  | Superintendent, Code 39<br>Joint C3 Curriculum Officer<br>Naval Postgraduate School<br>Monterey, California 93940-5000 | 1          |
| 5.  | Superintendent, Code 74<br>ATTN: Prof. M. G. Sovereign<br>Naval Postgraduate School<br>Monterey, California 93940-5000 | 1          |
| 6.  | Russell Maxwell<br>Systems Engineering Division 5264<br>Sandia National Laboratories<br>Albuquerque, New Mexico 87185  | 1          |
| 7.  | Dave Sidlauskas<br>Recognition Systems, Inc.<br>San Jose, California 95129   | 1          |
| 8.  | Capt Beth Barker<br>HQ AFOSP/SPOSC<br>Kirtland AFB New Mexico 87117  | 1          |
| 9.  | Mr. John Parker<br>RADDC/IRAA<br>Griffiss AFB New York 13441-5700  | 1          |
| 10. | Mr. Neil Anderson<br>Deputy Director of TCD<br>ESD/TCD<br>Hanscom AFB Massachusetts 01731                              | 1          |
| 11. | Daryl C. Bright<br>Rural Route 1<br>Morris, Minnesota 56267  | 1          |















DUDLEY KNOX LIBRARY  
NAVAL POSTGRADUATE SCHOOL  
MONTEREY, CALIFORNIA 95943 8002

Thesis  
B80855 Bright  
c.1 Examining the reliability of a hand geometry identity verification device for use in access control.

26 AUG 88

~~1 SEP 81~~  
1 OCT 81

32800  
35096  
36748

Thesis  
B80855 Bright  
c.1 Examining the reliability of a hand geometry identity verification device for use in access control.

thesB80855

Examining the reliability of a hand geom



3 2768 000 72357 1  
DUDLEY KNOX LIBRARY