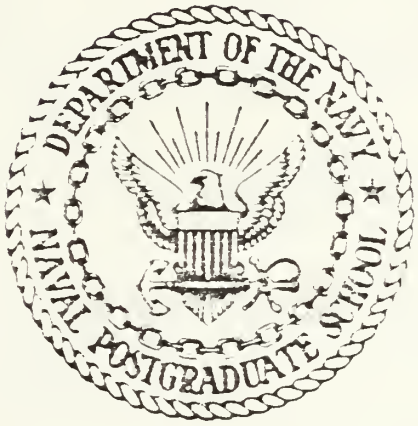
NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

EXAMINING THE RELIABILITY OF A RETINAL RECOGNITION DEVICE AS DATABASE SIZE AND THE NUMBER OF ENROLLMENT SCANS ARE VARIED FOR APPLICATIONS IN COMMAND, CONTROL AND COMMUNICATIONS (C^3)

by

Anthony M. Leigh, Jr.

December 1986

Thesis Advisor G.K. Poock

Approved for public release; distribution is unlimited.

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b OFFICE SYMBOL (If applicable) Code 39
7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School	
6c ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000	7b ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000
8a NAME OF FUNDING / SPONSORING ORGANIZATION	8b OFFICE SYMBOL (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) EXAMINING THE RELIABILITY OF A RETINAL RECOGNITION DEVICE AS DATABASE SIZE AND THE NUMBER OF ENROLLMENT SCANS ARE VARIED FOR APPLICATIONS IN COMMAND, CONTROL AND COMMUNICATIONS (C^3)

12 PERSONAL AUTHOR(S)
Leigh, Jr., Anthony M.

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Master's Thesis	FROM _____ TO _____	1986 December	36

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Command, Control and Communications, access control retinal blood vessel pattern recognition, computer security, authorization techniques

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

As the amount of sensitive information stored in databases increases due to the current trend to automate Command, Control and Communication (C^3) systems, the impact of unauthorized access could be very detrimental to our nation's security. Access control hardware that uses retinal blood vessel pattern recognition may be the solution to the problem. This thesis looks at one retinal pattern recognition device and attempts to determine it's reliability as a function of the data base size stored in memory and the number of enrollment scans averaged together to form the reference template. The database sizes used consisted of 300, 600 or 1200 templates, and the reference templates tested were comprised of 3, 5 or 7 enrollment scans. The applicability of this technology for protecting C^3 systems is discussed. This study employed the Eye Dentify 7.5 system developed by Eye Dentify Inc. of Beaverton, Oregon, which performed extremely well by producing a low TYPE I error rate and no TYPE II errors in over 1000 trials. This technology has potential for the protection of C^3 systems.

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL G.K. Poock	22b TELEPHONE (Include Area Code) (408) 646-2636
	22c OFFICE SYMBOL Code 55Pk

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

Approved for public release; distribution is unlimited.

Examining the Reliability of a Retinal Recognition Device as Database Size and the Number of Enrollment Scans are Varied for Applications in Command, Control and Communications (C^3)

by

Anthony M. Leigh, Jr.
Lieutenant, United States Navy
B.S., University of Maryland, 1980

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
December 1986

ABSTRACT

As the amount of sensitive information stored in databases increases due to the current trend to automate Command, Control and Communication (C^3) systems, the impact of unauthorized access could be very detrimental to our nation's security. Access control hardware that uses retinal blood vessel pattern recognition may be the solution to the problem. This thesis looks at one retinal pattern recognition device and attempts to determine it's reliability as a function of the data base size stored in memory and the number of enrollment scans averaged together to form the reference template. The database sizes used consisted of 300, 600 or 1200 templates, and the reference templates tested were comprised of 3, 5 or 7 enrollment scans. The applicability of this technology for protecting C^3 systems is discussed. This study employed the Eye Dentify 7.5 system developed by Eye Dentify Inc. of Beaverton, Oregon, which performed extremely well by producing a low TYPE I error rate and no TYPE II errors in over 1000 trials. This technology has potential for the protection of C^3 systems.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

As our Command, Control and Communications (C^3) systems increasingly rely on computers, databases, and secure communications networks, there is a need for accurate and reliable access control hardware. Positive identification of the users is necessary to ensure that only authorized users gain access; and to ensure that an accurate audit trail exists, if a violation occurs. Most automated access control mechanisms don't provide this level of security. Access control hardware that uses retinal blood vessel pattern recognition may be the solution to this problem.

Access controls are designed to protect information in a computer system. There are two major aspects to access control of computer resources (FIPS Pub 83, 1980):

(1) Identification and authentication of authorized users

(2) Authorization for the use of designated resources in the intended manner.

Both of these are critical to maintaining the integrity of a C^3 system. There must be controls to ensure that information is protected from unauthorized access and or manipulation of sensitive information. Through positive identification of the users, there is also the added deterrent from misuse of information when one knows that an accurate audit trail exists linking them to that information.

Access controls are based on identifying an individual through (FIPS Pub 83, 1980):

(1) Something that they *know* (i.e., passwords)

(2) Something that they *possess* (i.e., tokens, keys, security cards)

(3) Something *about* the person (i.e., physical or dynamic characteristics).

There are advantages and disadvantages to each of the above methods with regards to expense, administration, and amount of security provided.

1) SOMETHING A PERSON KNOWS

Passwords are the most commonly used and least expensive means to control access to computer networks. The advantage of no extra hardware requirements decreases the start up costs when implementing the system. The amount of administrative work associated with the generation and selection of passwords is a function of the level of security one desires for the material being protected. The disadvantage of passwords is the possibility that the password can be compromised,

either intentionally or unintentionally. A password can be used by an unauthorized user to gain access and this violation may not be detected until after damage has been incurred on the C^3 System.

2) SOMETHING THAT A PERSON POSSESSES

Special tokens, keys, or security cards can be used to control access and identify an individual. Since these items can easily fall into an unauthorized persons hands through loss or theft, they are usually used in tandem with a password or a Personal Identification Number (PIN). This method is more costly than the use of passwords alone due to the additional hardware and administrative requirements. Even when Security Cards are used with a PIN or password, the possibility still exists that the system can be accessed by unauthorized users.

3) SOMETHING ABOUT THE PERSON

Since there are inherent drawbacks associated with the other two methods of identification, much emphasis has been placed on positive identification through personal attributes or characteristics. Biometric recognition devices have been developed which can identify a person by hand geometry, fingerprints, signatures, speech and retinal blood vessel patterns. One of the major problems with biometric recognition is the difficulty in performing precise and repeatable measurements on the human body. An optimal recognition device can distinguish between the interpersonal variation and minimize the effects of intrapersonal variation. Due to the curvilinear nature of the human body and the lack of precise reference points to measure from, the intrapersonal variation can become exceedingly large. Most biometric recognition devices deal with this problem through the use of tolerance thresholds and allowing the user several attempts to get within these limits. Biometric recognition devices can be expensive, but are capable of the best security and the lowest administration costs since password and security card maintenance are not required.

There are two types of errors that a biometric recognition device can make:

(1) TYPE I ERROR - This is when an authorized user is falsely rejected, usually due to intrapersonal variation that is too large and falls outside the tolerance threshold limits.

(2) TYPE II ERROR - This occurs when an individual is falsely accepted and allowed access, usually due to the tolerance threshold limits being too large, coupled with an individual with a small interpersonal variation with an authorized user. This situation can cause overlaps which can result in TYPE II errors.

Obviously, one would want a system that minimizes errors, which can be costly. TYPE I errors tend to hassle and demoralize authorized users by not allowing them

access to the system. There are additional costs associated with these errors through work lost and the added requirement to have security guards nearby to allow these authorized users access. In the C^3 environment TYPE II errors are unacceptable due to the potentially high security risks associated with sensitive information.

There is a tradeoff between TYPE I and TYPE II error rates. To minimize TYPE I errors by increasing the tolerance thresholds, the TYPE II error rate can potentionally increase. So, a marginal amount of TYPE I errors may be acceptable in order to minimize the possibility of TYPE II errors.

This study looks at a biometric recognition device that uses retinal blood vessel patterns to identify an individual. Retinal blood vessel patterns have been proven to be highly individualistic and stable (Simon and Goldstein, 1935). This device compares your digitized retinal pattern to one that has been stored in memory. If the difference between the scan of your eye and the one in memory is within the tolerance threshold limits, then you gain access. Otherwise, access is denied.

The reference template of one's eye is formed through an enrollment process that involves averaging several pictures of your blood vessel pattern. Averaging is used to build a more robust reference template to compare against when allowing one access. This allows for a degree of intrapersonal variation caused by differences in head and eye positioning.

The Eye Dentify 7.5 system has two basic modes of operation, VERIFY and RECOGNIZE. In the VERIFY mode, the user inputs a four digit PIN by pushing those numbers on the keypad just before taking the eye scan. The 7.5 system compares the template associated with that PIN and the users eye scan. In the RECOGNIZE mode, no PIN is required. The 7.5 System searches through the entire memory for a match that is within the tolerance threshold limits.

For the purposes of this study, the RECOGNIZE mode was used. The experiment was designed to determine the effects on TYPE I and TYPE II error rates when the database size and the number of enrollment scans used to form the reference template are varied. Also considered is the applicability of this technology in C^3 systems.

II. THE EXPERIMENT

A. EQUIPMENT USED

The Eye Dentify 7.5 system is a retinal blood vessel pattern recognition device. Scientific studies dating back to 1935 support the premise that retinal blood vessel patterns are unique to the individual and very stable. Dr. Carleton Simon and Dr. Isodore Goldstein published a paper in 1935, which discussed the results of their study on using retinal photographs as a means to uniquely identify an individual.

> What is true of the fingerprint system is also true of this new system, in that no two individuals have the same identification patterns. The many and great variety of blood vessel configurations makes it a mathematical certainty that no two retinal formations are identical. In thousands of photographs, none have been found to be the same. Age or disease may change in tortuosity the lumen of the blood vessels, but their position and their correlation remain unchanged through life, and what is of greatest interest, they cannot be altered or effaced. . . . (Simon and Goldstein, 1935)

In 1955, Dr. Paul Tower confirmed this previous study when he published a paper which concluded that the greatest dissimilarity between Identical Twins was in their retinal blood vessel patterns (Tower, 1955).

1. Hardware

This system is composed of an eye camera (ICAM), monocular eyepiece, 8 character LED display, 12 digit keypad (0-9, #, *), SCAN button, 68000 microprocessor, and bubble memory all enclosed in a cast aluminum housing (See Fig. 2.1). There is an I/O interface for a terminal which enables control of the internal software functions and operations. An additional I/O auxiliary port is provided to allow computer and printer interface. A microcomputer was used in this experiment to up and down load the databases from a floppy disk. A printer with a serial to parallel converter was used for documentation of collected data.

2. Eye Camera (ICAM)

The ICAM scans a fovea-centered circle on the back wall of the eye, which includes the retina and choriod (See Fig. 2.2). The light source is an infrared light emiting diode, which has been proven safe for this level and duration of exposure to the human eye (Eye Dentify Inc., 1984). The spectrum and power level used is similar to that of a common television remote control device. When in operation, the ICAM

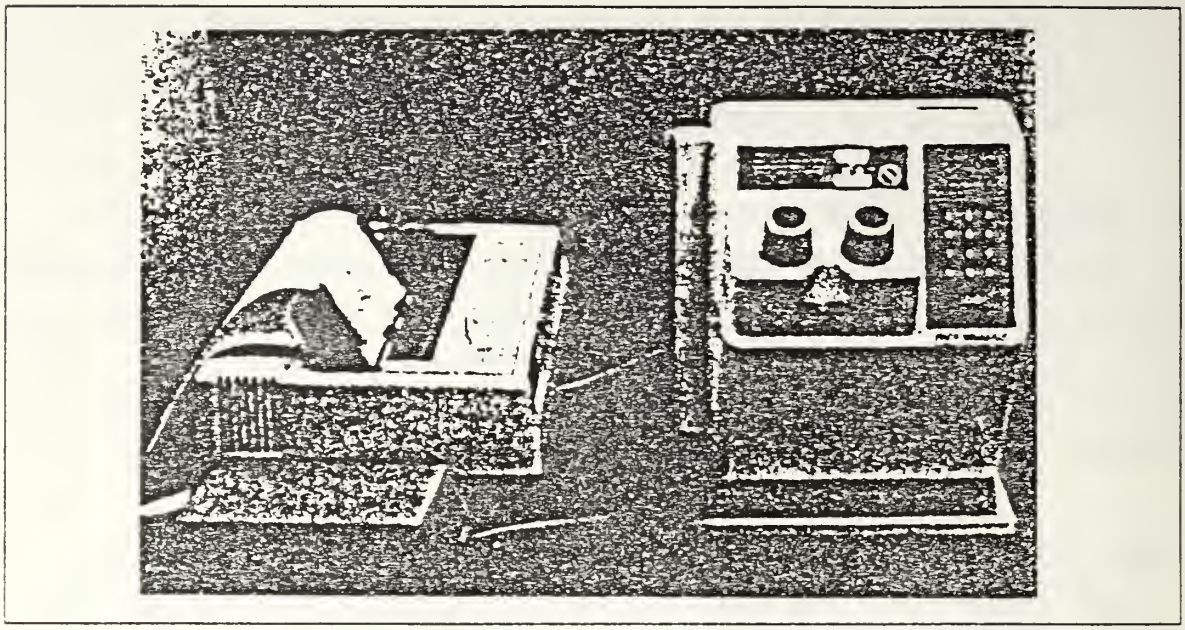


Figure 2.1 The Eye Dentify 7.5 System Hardware.

performs a 450 degree circular scan (1.25 revolutions of the scanner) which detects and digitalizes contrast-relative light and dark areas on the scanning circle.

3. Recognition Mode

When operating in the RECOGNITION mode, the 7.5 system uses a proprietary algorithm that searches the entire database in bubble memory for the five closest templates, then picks the best match. This "best match" must then be within the tolerance threshold limits for one to gain access. This process was designed to increase the SPEED OF RESPONSE. The SPEED OF RESPONSE is then a function of the database size stored in bubble memory. Up to 1200 eye templates can be stored in bubble memory (Eye Dentify Inc., 1984).

B. OBJECTIVE OF THE EXPERIMENT

The objective of the experiment was to compute the TYPE I and TYPE II error rates when subjects were tested in nine different situations, where database size and the number of enrollment scans that formed their reference template were varied. A secondary objective was to monitor the SPEED OF RESPONSE in each situation. The database size in bubble memory was varied by using 300, 600 and 1200 eye templates. Each subject was enrolled three different times. Each reference template was formed in an averaging process that was composed of 3, 5 or 7 eye scans.

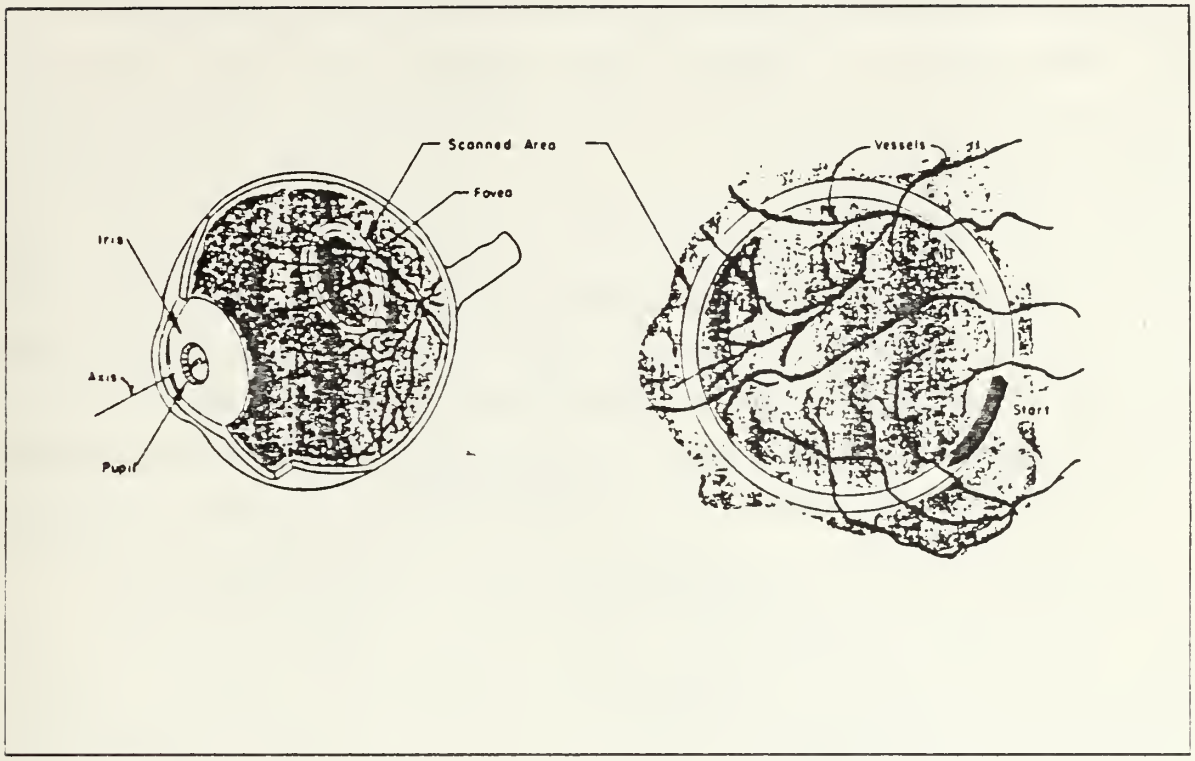


Figure 2.2 The Scanning Circle.

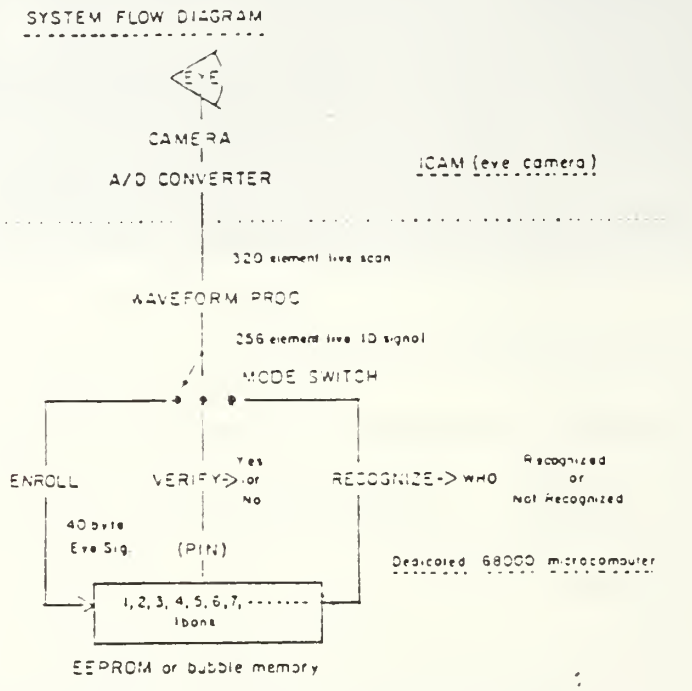
C. EXPERIMENTAL PROCEDURE

1. Participants

Twenty two subjects participated on a volunteer basis. There were no incentives offered for good performance, just the subject's interest and competitiveness were sufficient. All were military officers, between the ages of 25 and 35, who were assigned to the Command, Control and Communications Curriculum at the Naval Postgraduate School. There was a good cross-section of subjects with vision that required corrective eyewear, either contact lenses or glasses. The high reflectivity of eyeglasses inhibits the ability of the 7.5 system to scan the eye, so those subjects that wore glasses were asked to remove them for the experiment. Contact lenses appeared to have no effect on the person's performance. Most subjects were familiar with the 7.5 system, but had not used it extensively.

2. Enrollment Process

The first step in the experiment was the enrollment process. A system compatible terminal was used to control the internal software functions, allowing one to use the 7.5 system's enrollment function. This is easily accomplished by entering "E", as indicated on the menu.



EYE SIGNATURE - composite of live ID signals acquired during enrolment process. Each eye (left and right) is packed into 40 bytes (320 bits) for storage in the Ibank

ICAM - acquires and digitizes the identification pattern from the subject's eye

IBANK - Storage of all Eye Signatures (reference templates)

PIN - Personal Identification Number. Used in Verify mode to select specific Eye Signature for match

MODE SWITCH - Selects the mode of the 7.5. Enroll mode allows a new individual to be added to the Ibank. Verify compares a live eye with the Eye Signature designated by the PIN entry. Recognition automatically selects best Eye Signature from the Ibank

Figure 2.3 Eye Dentify 7.5 System Operation.

For the purposes of this experiment, three reference templates were formed for each subject. The reference template is formed through an averaging process. The number of eye scans averaged together when forming the reference template could have a significant effect on TYPE I and TYPE II error rates. The three reference templates were composed of 3, 5 or 7 scans. The templates were formed in a random order for each subject and at least five minutes transpired between enrollments. Three floppy disks were used to store and keep each individual's reference template separate, so each floppy disk contained only the 22 subjects whose reference template was formed using the same number of scans. A microcomputer was used to upload and download the templates between the 7.5 system and the floppy disk. The 7.5 system's bubble memory was erased in between each evolution to keep the databases separate. A description of this process can be found in Appendix A.

The USER manual recommends that each subject be enrolled with at least 5 scans and that the average correlation score for all 5 scans be above +0.90. The correlation score is a mathematical representation computed by the 68000 microprocessor in the 7.5 system, which describes how similar the most recent scan is to the template stored in memory. The correlation score could be any number between +1.00 to -1.00. Although we strayed from this recommended procedure to test the significance of the number of scans used to form the reference template, all but one of the twenty two subjects easily averaged above the score of +0.90 during enrollment. The subject that had the difficulty with this criteria wore corrective glasses for astigmatism. This subject described difficulty in visually maintaining similar head and eye positioning between scans. This consistency is necessary for high correlation scores.

To bring consistency to one's approach when operating the 7.5 system, the following guidelines were given to each subject prior to each enrollment session and prior to each session of the experiment.

(1) Square the head perpendicular to the machine, resting the forehead on the headrest provided. Align the head so the right eye is adjacent to the recessed eye port.

(2) By looking into the recessed eye port and moving the head slightly, dots of light can be seen which form a three dimensional cone. Center the head so that the cone appears as a circle. At this point, ensure the head is still perpendicular to the machine. Focus on the center of the circle.

(3) Press the SCAN button gently.

After the SCAN button is pressed (at least two scans are required before a correlation score can be computed during enrollment), the enroller is given the choice of whether the latest scan is averaged into the reference template or discarded. The criteria for accepting or rejecting the latest scan was dependent on whether the correlation score was above +0.90 or below, only scans above +0.90 were accepted.

At this point the enroller is given four options:

(1) Continue the enrollment process so more scans can be averaged into the reference template.

(2) Restart the process. By activating Restart, all but the latest scan is retained in memory. All previous scans are discarded.

(3) Cancel the process. This terminates the enrollment process and discards all scans acquired for that individual during that session. Any templates previously stored in memory for that individual are not effected.

(4) Finish the enrollment process. This allows the enroller to input the subjects identifier and the threshold limits for the VERIFY and RECOGNITION modes. The threshold limit for this experiment in the RECOGNITION mode was set at 0.71 for each individual.

If a subject consistently scored low, then the restart function was activated. This action usually resulted in higher correlation scores. If the first scan from an individual was poor, this tended to pull the correlation score from all subsequent scans down. By activating the restart function, this first poor scan would be discarded allowing the consistency of the later scans to result in higher correlation scores.

3. **IBANK Database**

To determine the effects of database size on TYPE I and TYPE II error rates, a large database of 1150 subjects was obtained from Eye Dentify Inc. This database was used to obtain the 300, 600 and 1150 template databases used in the experiment. This process is described in Appendix B. These databases were stored separately on three floppy disks.

4. **Experiment Sessions**

All twenty two subjects were tested in each of the nine situations that can be formed when combining the 3 database sizes with the 3 reference templates for each of the 22 subjects. Each trial consisted of 5 samples per subject. For each session, a randomly selected combination would be stored in the memory of the 7.5 system. The subject would go through the scanning procedure five times, looking up between scans. The response (accepted or rejected) and the time for the system to respond were recorded after each scan. A stopwatch was used to determine the time between the pushing of the SCAN button and when the response was displayed.

D. RESULTS

The three-way factorial experiment was designed to determine whether the number of TYPE I and TYPE II errors were significantly affected when database size and number of enrollment scans are varied. The level of significance was set at $\alpha = .05$ during the design phase of the experiment. An analysis of variance was performed on the data using the statistical package by SAS Institute Inc.. The analysis of variance test allows one to statistically determine if there is any significant effect on the outcome caused by one or several factors.

During the course of this experiment, there were no TYPE II errors or false recognitions observed. Not one subject was misrecognized in over 1000 trials conducted in this experiment.

TABLE I
TYPE II ERRORS

THERE WERE
NO TYPE II ERRORS

Data was collected to find the recognition rates and times to response in each cell. The recognition rate is the number of recognitions for that cell divided by the total number of trials for that cell. The recognition rate distribution was expected to be binomial in nature, since one is either recognized or not recognized. The variances for each cell was computed, and the F_{max} statistic was applied to determine if the variances could be considered as coming from the same population. This is an

underlying assumption that must be fulfilled before the results of the analysis of variance can be considered valid. The variances fell outside this criterion, so the ARCSIN transformation (Y' = 2*ARCSIN(SQRT(Y)) was applied to stabilize the variances (Winer, 1971).

TABLE 2
ANALYSIS OF VARIANCE

SOURCE	DF	SS	MS	F	SIGNIF
SCAN	2	.6239	.3120	2.0109	
DB(SIZE)	2	.1368	.0684	.4409	
PERSON	21	13.7162	.6532	4.2100	p< .05
SCAN*DB	4	1.2929	.3232	2.0831	
SCAN*PERSON	42	9.5647	.2277	1.4676	
DB*PERSON	42	6.9857	.1663	1.0718	
POOLED ERROR					
SCAN*DB*PERSON	84	13.0333	.1552		
TOTAL	197	45.3532			

The recognition rate for each cell consisted of 5 samples for each subject. By using recognition rate, there was only one data point per cell which made the calculation for the 3-way interaction impossible. By pooling the 3-way interaction with the error term the F-statistics were calculated.

To determine if the calculated F-statistic is significant, one needs to see if it is greater than the F-statistic found in a book of statistical tables. As can be seen from Table 2, the only significant F-statistic, was that which related to person. Database size and number of enrollment scans were not statistically significant when $\alpha = .05$.

Figures 2.4 and 2.5 show the recognition rate *means* and 95% Confidence Intervals for scan number and database size. There appeared to be an interaction between DB SIZE and SCAN that proved statistically insignificant, but was interesting. This interaction is highlighted by Figure 2.6, as one can see the line depicting 5 scans with a 98% recognition rate at the 300 template database drop down to 93% at the 600 database, when the 3 and 7 scan lines are increasing. This can be attributed to random deviations that can occur and are statistically insignificant.

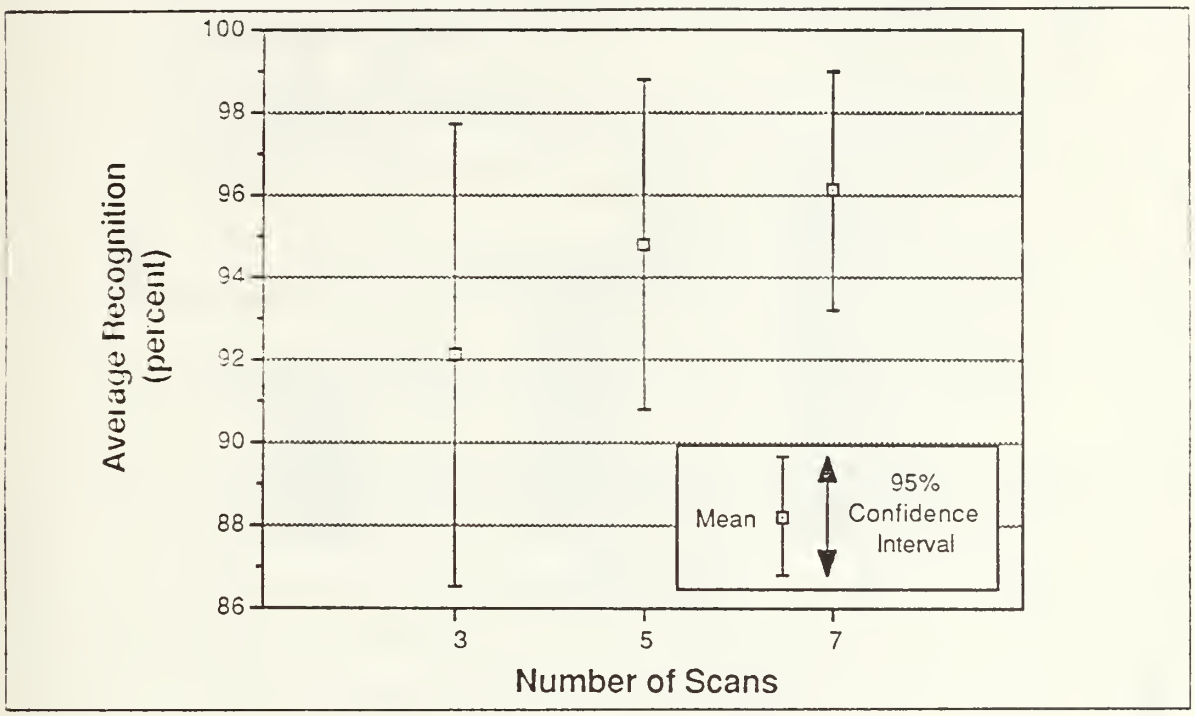


Figure 2.4 Effect of Number of Scans on Average Recognition.

The average times to response can be seen in Figure 2.7. Time of response was effected by the size of the database and whether the individual was recognized or not. The distributions appeared to be linear-log in nature, as the time rate of change remained constant at 3 seconds as the database size doubled. The time of response for NOT RECOGNIZED was consistently about 4 seconds longer than a RECOGNIZED response.

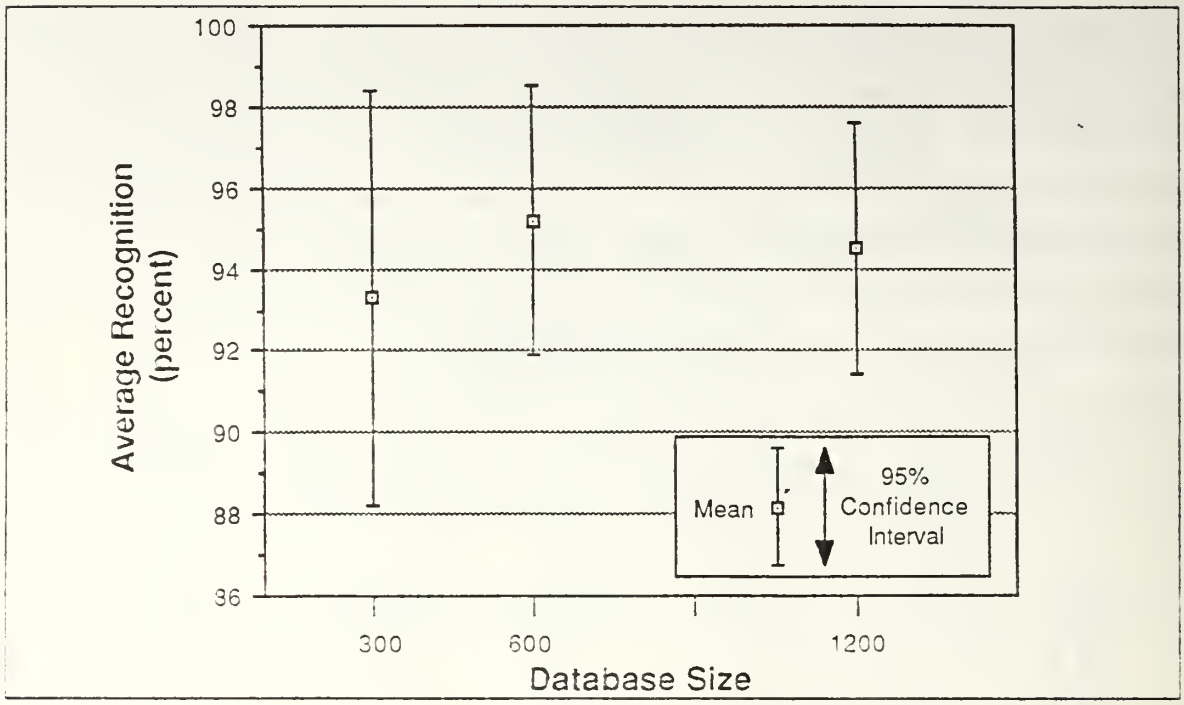


Figure 2.5 Effect of Database Size on Average Recognition.

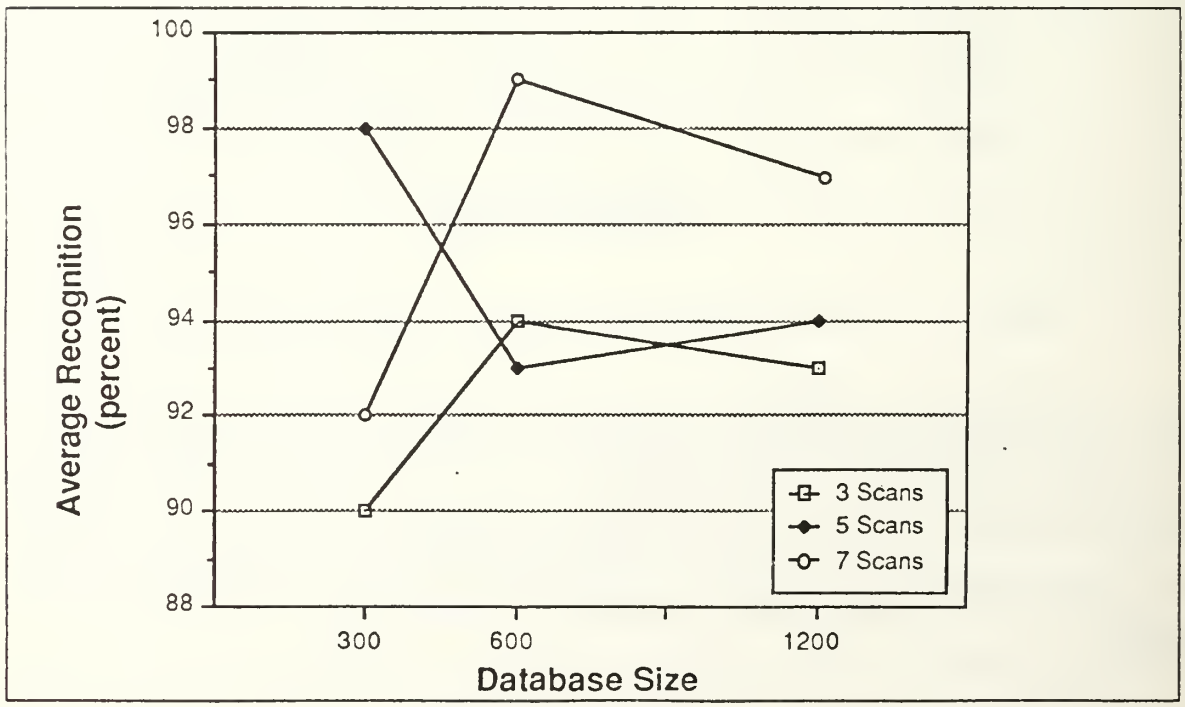


Figure 2.6 Scan Number - Database Size Interaction.

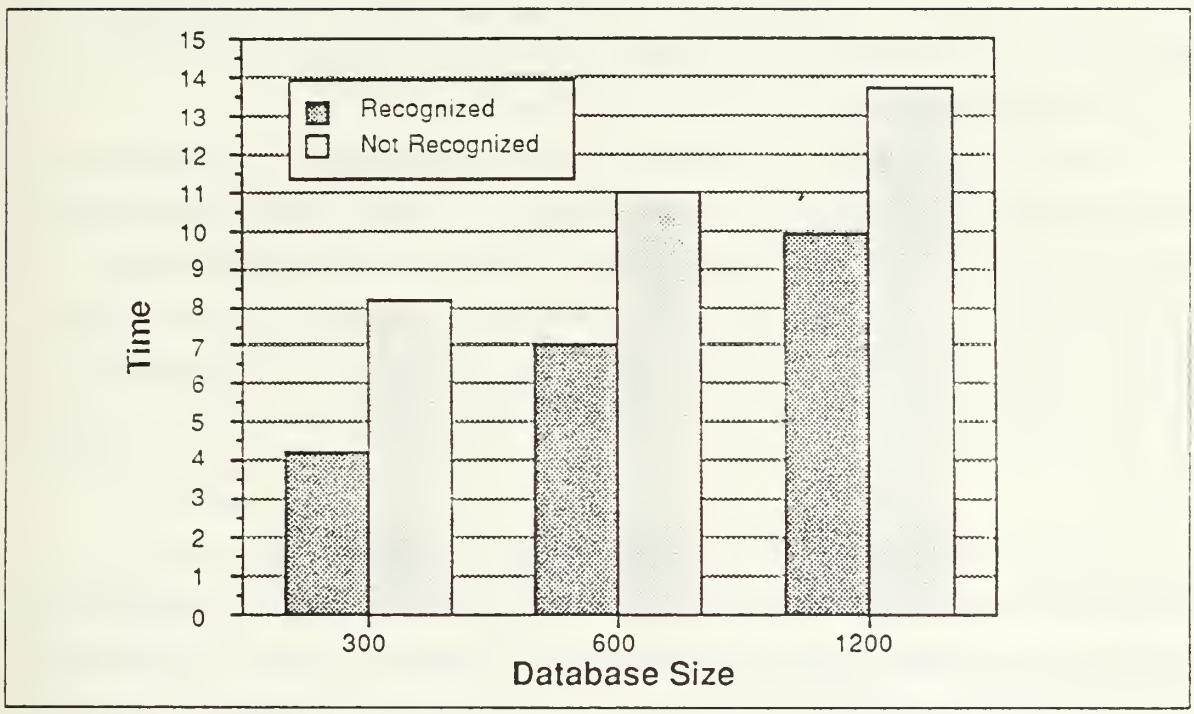


Figure 2.7 Time of Response.

III. DISCUSSION

A. MEASURES OF EFFECTIVENESS

To evaluate the effectiveness of a system one must consider how that system is to be used, then judge the system in that context. This system was evaluated from the perspective of how it would perform in a C^3 environment. The performance of an access control system is most critical when considered in this arena.

1. TYPE I Error Rate

The recognition rate and resultant TYPE I error rate were based on only one attempt per trial. If several attempts were allowed for one to be recognized per trial, the TYPE I error rate would be significantly lower. For this system's use in the operational mode, it would be advantageous to allow 3 attempts in order to minimize the rejection of authorized users. The overall recognition rate for this experiment in all conditions was 94.3%, when the recognition threshold was set at .71. The TYPE I error rate is calculated by subtracting the recognition rate from one, which in this case is 5.7%.

The TYPE I error rate should be low so to allow access to authorized personnel with a minimum of inconvenience. In this experiment **less than one percent were denied access after 3 attempts.** When time is critical as in the C^3 environment, this system could give some of the personnel problems, since the strongest predictor of TYPE I errors in this experiment was the individual. The subject with the worst recognition rate was recognized 78% of the time. This may be improved through reenrollment since that process is so critical for high recognition rates to be achieved.

2. TYPE II Error Rate

There were no TYPE II errors observed during the course of this experiment in which over 1000 trials were performed. Other studies have reported similar results (Helle, 1985; Masiero, 1986; Maxwell, undated). This is a very critical performance parameter in the C^3 environment. A C^3 system requires protection from unauthorized access, more so than most systems. Eye Dentify Inc. advertises that there is a one in a million chance of a false recognition when one eye is used and significantly better when two eyes are required to gain access. Sandia Laboratories performed operational tests on several biometric devices and reported that the eye recognition device had a

significantly lower TYPE II error rate than all the other devices tested. (Maxwell, undated)

3. Time of Response

Time of response is more important when considering physical access control than computer access control. In physical access control bottlenecks can occur during high volume time periods, which can disrupt operations. For computer access control one is less likely to experience bottlenecks, but a fast time to response enhances user acceptance of the system. From the C^3 perspective, time of response is very important when time is limited. The greatest time of response experienced during this study was 14 seconds for a not recognized response with 1200 personnel in the database. The time for a NOT RECOGNIZED was about 3 to 4 seconds longer than for a recognized response, and the time of response was longer as the database size was larger. It is not known what the effects would be on time of response if the database is maintained in a mainframe computer versus in the 7.5 system's bubble memory as was tested in this case. In any event, there is a definite linear relationship between database size and search time as shown in Figure 2.7.

4. Administration

The administration of a high level security system can be enormous. Most of the administrative time is spent maintaining the integrity of passwords and security cards. There are many precautions for secure systems when passwords are utilized under the guidelines set by the National Computer Security Center (DoDCSC, 1985). A majority of this burden could be reduced or alleviated through use of a biometric recognition device, where passwords and security cards would not be necessary. With a biometric device like the 7.5 system, the administration time would primarily encompass the time spent on enrollment. The enrollment time for this experiment averaged about 3 minutes per subject for all enrollments.

5. User Acceptance

This system is very easy to use. To emphasize the point, the Dade County Jail of Miami, Florida has been using this system on it's inmates (Eye Dentify Inc., 1986). The inmates are enrolled upon entry to the facility and verified when leaving to ensure the correct individual is released. Some degree of cooperation is required of the subject, but as this demonstrates, one's technical background is unimportant.

The subjects in this experiment were very curious about the system, and specifically how the system works. The questions most frequently asked concerned the

safety of the scanning process and how the ICAM collected the information from the eye. The user acceptance of this device by the subjects of this experiment was very high, once a technical explanation of the system was provided.

It was observed that some subjects had more difficulty being recognized than others. Some of this difficulty can be attributed to the enrollment. There appears to be a slight learning curve associated with the use of this equipment that affects some people more than others. By reenrolling these individuals and taking advantage of this learning curve, the individual should achieve higher correlation scores through more consistent head and eye positioning. This was not done in this experiment as each subject retained their original reference template through the entire experiment.

Another cause for lower recognition rates would be from the subject's carelessness when positioning the head and eye for the scan. There were no incentives or rewards given to the subjects for high recognition rates, but generally the subjects had an interest in the technology and therefore tried to do well. The subject might be somewhat careless until they get a NOT RECOGNIZED, then would try harder to get accepted by the system.

6. Cost

The Eye Dentify 7.5 system used in this experiment costs about $9,000, which is fairly expensive. The system is a stand alone physical access control device, which would maintain physical access control of an entrance to an area. This system was designed to work using it's own bubble memory, but some companies have adapted the system so it can use a centralized databank.

When evaluating the cost effectiveness of a security system, one must consider the environment in which it is to perform and the amount of security necessary to enable acceptable risk levels. In the C^3 environment, the risks are very high and the highest performance is required. The 7.5 system has performed much better than others analyzed in previous studies (Jones, 1986; Maxwell, undated).

As can be expected from new technology, the costs are generally higher than in older technology. Once the Research and Development costs are recovered as production increases and competitors get into the market, the costs should come down significantly. This trend is expected to occur with the Eye Dentify system.

B. C^3 APPLICATIONS

Command and control is made up of many subsystems as is portrayed in the Joint Chiefs of Staff (JCS) definition of a command and control system.

> A command and control system consists of facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. (DoDJCS, 1979)

Computer systems are becoming increasingly important for the military commander to fulfill his mission. This reliance on computer systems coupled with the high risks involved if the information is compromised, makes access control to computer systems very important to command and control.

Command and control centers employ many personnel all of which have varying degrees of security level clearances. A person must have the clearance to access classified information and additionally they require a "need to know" that information. Through automation positive identification is possible through retinal blood vessel pattern recognition. This requirement of positive identification, as was pointed out earlier, is not possible with passwords alone. Positive identification enables the computer system to check an individuals clearance and "need to know" before access is given.

Physical access control is equally important for the maintenance of a C^3 system. Currently, mechanisms like cipher locks, keys, security guards or security cards are used for access to C^3 areas. Many command and control centers are compartmented within the physical structure along the lines of security level and "need to know". Positive identification is necessary to ensure these requirements are met. Retinal recognition could be used to control access to a facility and within the facility to take advantage of the added security and avoid the drawbacks associated with the currently used methods.

1. Current Applications

The acceptance of this technology is already widespread as many corporations and military installations have employed retinal pattern recognition devices. The most common application is for physical access security, replacing the need for security guards, keys, or security cards to gain access. Campbell Engineering designed a security access control booth that is used in conjunction with this system (Smart and

Labarile, 1986). The booth allows only one to enter at a time and has an added feature that weighs the individual. This ensures that there is only one person, and that person is within the weight limits previously determined, thus adding an additional criteria for one to enter an area.

2. **Computer System Access Control**

Due to the increasing need for better security of computer systems and databases within C^3 systems, this technology can be easily adapted for use as a computer system access control device. Most of the 7.5 system functions can be carried out from the host computer. The scanning of the user's eye can be performed by a small hand held ICAM. Once the scan has been performed, this data can be inserted to the host computer through a jack on the terminal. The host computer would contain the database with the individual's reference template and the algorithm to perform the comparison. This eye scan would be the substitute for the password during the LOGON procedure.

Currently, there is a prototype of a small hand held ICAM under development by Eye Dentify Inc.. By aggregating most of the software functions of the 7.5 system on a host computer and having the hand held ICAM accessible to several terminals at a time, the cost of the system could be very reasonable. When one considers the added security of such a system and the risks involved with passwords, this may be the way to increase C^3 system security.

3. **Possible C^3 Applications**

This technology is basically a very secure way to replace the existing means to gain access, either into a physical area or into a computer system. If the risk of unauthorized access is high as in C^3, then one might want to think about installing a system such as this to replace keys, security cards and passwords. The need for security guards could also be reduced by a secure automated access control system.

Database security is one area that could be greatly improved by a retinal recognition system. As C^3 systems become increasingly automated with new sensors that collect large amounts of data, processors and decision aids draw from that data to help the battlefield commander make informed decisions. The integrity of the database must be protected not only from unauthorized reading of sensitive data, but also from unauthorized manipulation of data.

To economize on space and increase convenience, one database might store several classification levels, this is called a multilevel security database. When a

workspace is occupied by personnel of different classification levels, there is an increased need to ensure that the person entering a password is indeed the person authorized to use that password. In a large system, the need for positive identification of users multiplies and risk increases. Audit trails tracing back to personnel who accessed certain information may be the only way to find the source of a violation. With passwords as the only means to identify the individual, the audit trail may not be correct.

The function of identifying and verifying an individual could be performed within the computer system automatically through use of a retinal recognition device. When positive identification can be achieved, there are no compromised passwords to worry about, and an accurate audit trail is possible. Passwords can be compromised too easily for their use to continue in these high risk environments.

Weapon security could also benefit from this technology. Retinal recognition could be used to activate large and very lethal weapon systems. For nuclear weapons two different individual's eyes would be required before the system could be activated to conform with the two man rule. Such a system could minimize the risks associated with a weapon that falls into the wrong hands.

For a command and control computer system to be beneficial to a battlefield commander, it needs to be accessible near the front lines and have mobility. In a multiservice or joint command there is a constant change of personnel with many unfamiliar faces, more so than within one service. This presents a particularly difficult security problem. Mobility is degradated by security considerations and constraints as it requires a large administrative effort to maintain high standards of security in this C^3 environment. Retinal recognition could be used for physical access controls and computer access controls, which could provide improved security over the existing methods with significantly less administrative effort. Mobility and security are two criteria for a mobile command post that could be improved through use of retinal blood vessel pattern recognition.

The use of retinal blood vessel pattern recognition to protect C^3 systems from unauthorized access is important for three reasons. First, positive identification can be ensured with a high level of confidence, more so than with passwords only. Second, accurate audit trails can exist, which act as a deterrent and generate a possible suspect list if a violation occurs. And third, there would be a significant reduction in the administration of the security aspects of a C^3 computer system as the stringent guidelines concerning passwords would not be required.

IV. CONCLUSIONS

The Eye Dentify 7.5 system proved to be a very reliable, user friendly and timely access control device with many C^3 applications. The results of the experiment demonstrated that most people will be positively identified at least 94.3% of the time on one attempt and 99% on three attempts, regardless of database size and at least 3 enrollment scans. It was found that the difference in recognition rate was not statistically significant for 3, 5 or 7 enrollment scans or for database size used. This points out a significant time savings when enrolling new personnel. This study shows that only 3 enrollment scans is sufficient for most people. There were no false recognitions in over 1000 trials.

Through the necessity to automate many aspects of C^3, there is also the necessity to upgrade the protective mechanisms for these systems. The inherent drawbacks associated with passwords and other devices carried by an individual (i.e., security card) make their use as the sole access control mechanism very risky. Retinal recognition devices like the one used in this experiment, offer greater security, less administrative costs and enable accurate audit trails to exist.

Areas requiring further study:

1) To determine the TYPE I recognition rates when subjects require access while under stress
2) To determine the magnitude of a learning curve associated with retinal recognition devices, and how best to employ this information
3) To test TYPE I and TYPE II error rates when the hand held ICAM is used
4) To operationally test a retinal recognition computer access control system.

APPENDIX A
COMBINING DATABASES

It is possible to upload two separate databases into the 7.5 system's bubble memory to form a database that is a combination of the two. For this experiment, this process has saved time and increased flexibility as the three database sizes and the three files of enrollment scans where mixed in the various combinations. The software package that comes with the 7.5 system indirectly allows one database to be inserted into bubble memory, where another database is already stored.

The 7.5 system has a very simple database management system that uses a Personal Identification Number (PIN) as the primary key that is stored with the individual's reference template data. The PINs are stored in sequential order. The enroller is given the option of assigning the PIN, or the system will assign them automatically by filling up the lower PINs first. The PIN can not be changed once it has been assigned to the reference template data. This allows two or more databases to be combined with out destroying data, if there are no two identical PINs occupied with data between the databases. If there are identical PINs occupied, then the most recently added reference template will replace the previous template. All other data will remain unchanged.

The key to combining databases is to assign PINs during enrollment which are not already assigned in the other database. Unless one intends on combining databases, it is recommended to erase the bubble memory first. This will help to ensure that memory only contains the templates that were last inserted.

For this experiment, a total of 6 floppy disks were used. There were 3, which stored the 300, 600, and 1200 template databases, and 3, to store the 3, 5, and 7 enrollment reference templates for the subjects. The bubble memory was empty for each of the enrollment sessions, so the subjects filled the first 22 PIN locations automatically. The 300, 600, or 1200 template database would be uploaded to memory first, in the manner described in the USER MANUAL. The 22 templates for the subjects would be uploaded second, and would over write these first 22 PIN locations in memory and would not affect the rest of the database.

APPENDIX B
TRIMMING DOWN A DATABASE

These procedures describe how to trim down a larger database to a smaller size, as was required for this experiment. The software will only allow one template to be deleted at a time or the entire memory, there is no in between where a range of templates might be deleted. To delete one template only takes a few seconds, but to delete 600 takes considerable time. This set of procedures will only trim the latter part of the database; which means, one can delete all templates past a certain point. This is due to the way the software sequentially fills the bubble memory starting with the lowest PIN to the highest PIN with a template. By monitoring the system's progress, then halting execution when the desired number of templates have been transferred to memory, any size database can be formed from a larger one without a great loss of time.

Once the upload process has been initiated as per the USER's MANUAL, note the time that the upload started. It takes a little over 2 seconds to transfer one template from a disk to memory, so if 300 templates are to be transferred, plan on about 10 minutes before the next step needs to be performed (2 seconds * 300 templates / 60 seconds = 10 minutes). One can monitor the progress of the transfer by using the list function offered to allow one to display the PINs and identifiers currently in memory. If a range of PINs are inputted, the list function will display 5 at a time until the end of the range is reached or until there is no more occupied PINs to display. One can enter a range of PINs many times to monitor the progress. When the desired number of templates have been transferred, execution can be halted by pushing Control "C" or Control Scroll Lock on the microcomputer's keyboard. This will get one close to the desired number. The exact number can be achieved through deletion of one template at a time.

LIST OF REFERENCES

DoDCSC, Department of Defense Computer Security Center, STD-002-85, *Department of Defense Password Management Guideline*, Washington, D.C., U.S. Government Printing Office, 12 April 1985.

DoDJCS, Department of Defense Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Washington, D.C., U.S. Government Printing Office, p.74, 1979.

Eye Dentify Inc., "7.5 Camera Function Definiton," unpublished, 1984.

Eye Dentify Inc., *The Eye Dentification System 7.5 User's Manual*, Beaverton, Oregon, 1985.

Eye Dentify Inc., "White Paper" to Dept 55PK, Naval Postgraduate School, Subject: Health, Safety and Statistical Performance of the 7.5, 13 December 1984.

Eye Dentify Inc., Videotape to Dept. 55PK, Naval Postgraduate School, Subject: Use of the Eye Dentify 7.5 System in the Dade County Jail, 1986.

FIPS, Federal Information Processing Standards Publication 48, *Guidelines on Evaluation of Techniques for Automated Personal Identification*, U.S. 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*, U.S. Department of Commerce, National Bureau of Standards, September 1980.

Helle, D.K., *Examination of Retinal Pattern Threshold Levels and Their Possible Effect on Computer Access Control Mechanisms*, M.S. Thesis, Naval Postgraduate School, Monterey, California, September 1985.

Jones, A.J., Defense Intelligence Agency (DIA), Letter, Subject: Analysis of Personal Identification and Verification Devices, 30 October 1986.

Masiero, D.A., *Examining the Effect of Transverse Motion on Retinal Biometric Identifiers Relating to Shipboard Security Mechanisms*, M.S. Thesis, Naval Postgraduate School, Monterey, California, March 1986.

Maxwell, R., "The Status of Personnel Identity Verifiers," Sandia National Laboratories, Albuquerque, New Mexico, unpublished, undated.

Simon, C. and Goldstein, I., *New York State Journal of Medicine*, Vol. 35, No. 18, pp. 901-906, 15 September 1935.

Smart, D.C. and Labarile, P.M., "Microcomputer Controlled Identity Verification Processing for Sensitive Area Access," *Proceedings of The 1986 Carnahan Conference on Security Technology*, OES Publications, Lexington, Kentucky, May 1986.

Tower, P., "The Fundamental Oculi in Monozygotic Twins," *American Medical Association Archives of Opthamology*, Vol. 54, pp.225-238, 1955.

Winer, J.A., *Statistical Principles of Experimental Design*, McGraw-Hill Publishers, New York, 1971.

BIBLIOGRAPHY

Bruning, J.L. and Kintz, B.L., *Computational Handbook on Statistics*, Scott, Foresman and Company, Glenview, Illinois, 1977.

Cooper, J.A., *Computer-Security Technology*, D.C. Heath and Company, Lexington, Massachusetts, October 1984.

Miner, D.K. and Eckert, J.H., "Managing Electronic Access Control Systems," *Proceedings of The Second Annual Symposium on Physical/Electronic Security*, Philadelphia Chapter Armed Forces Communications and Electronics Association, August 1986.

Whittle, T.J., "Access Control Today," *Proceedings of The Second Annual Symposium on Physical/Electronic Security*, Philadelphia Chapter Armed Forces Communications and Electronics Association, August 1986.

Cox, A. J., *Management Implications of the Use of Multiple Retinal Patterns as a Means of Personal Identification*, M.S. Thesis, Naval Postgraduate School, Monterey, California, September 1986.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Superintendent, Code 55PK ATTN: Prof. G. K. Poock Naval Postgraduate School Monterey, California 93943-5000	20
4.	Superintendent, Code 74 ATTN: Prof. M. G. Sovereign Naval Postgraduate School Monterey, California 93943-5000	1
5.	Superintendent, Code 39 Joint C3 Curricular Officer Naval Postgraduate School Monterey, California 93943-5000	1
6.	Superintendent, Code 55NI ATTN: Prof. D. E. Neil Naval Postgraduate School Monterey, California 93943-5000	1
7.	Defense Intelligence Agency ATTN: Mr. A. J. Jones DIA / RSE Pentagon, Washington D.C. 20340-3413	1
8.	Lt. Anthony M. Leigh, Jr., USN Box 61 Gibson Island, Maryland 21056	1
9.	Mr. M. Edward Carlson 1800 North Kent Street Suite 1210 Arlington, Virginia 22209	1
10.	Mr. E. Lynn Goldman Westinghouse Idaho Nuclear Co. Inc. P.O. Box 4000 WCB-S1 Idaho Falls, Idaho 83403	1
11.	Mr. D. Khalil Jones Westinghouse Idaho Nuclear Co. Inc. WCB-S1 Idaho Falls, Idaho 83403	1
12.	Mr. John M. Shaffer Rockwell International Rocky Flats Plant P.O. Box 464 Golden, Colorado 80401	1

13. Mr. Everett Scholl 1
U.S. Secret Service
Technical Development & Planning Division
1800 G. Street N.W., Room 941
Wahington D.C. 20223

14. Mr. William J. Stinson 1
Navy Personnel R&D Center
Code 71
San Diego, California 92152-6800

15. Mr. Robert Rumble, L546 1
Lawrence Livermore National Lab
P.O. Box 808
Livermore, California 94550

16. Mr. Jack Garnish 1
Social Security Administration
SSA Systems Security
Room 3-J-5, Annex Building
6401 Security Blvd.
Baltimore, Maryland 21235

17. Mr. Jerry McBroom 1
Aerospace Corporation
P.O. Box 5068
Vandenburg AFB, California 93437-6021

18. Mr. Carl Strode 1
Westinghouse Hanford
Security Applications Center
P.O. Box 1970
Richland, Washington 99352

19. Mr. John Wilson 1
MITRE Corporation/ESD
Bedford, Massachusetts 01730

20. Mr. Mike Fuller 1
Martin Marietta Energy Systems
Building 9720-10, MS T
Y12 Plant
P.O. Box Y
Oakridge, Tennessee 37831

21. Mr. Wendell Ford, MS-E550 1
Los Alamos National Laboratory
P.O. Box 1663, MS-E541
Los Alamos, New Mexico 87545

22. Lt. Debra K. Helle 1
IS Support Division
NMPC 47
Department of the Navy
Washington D.C. 20350

23. Mr. John O'Hare, Code 442EP 1
Office of Naval Research
800 North Quincy Street
Arlington, Virginia 22217

24. Mr. Jesse Orlansky 1
Institute for Defense Analysis
Science and Technology Division
1801 North Beauregard Street
Alexandria, Virginia 22311

25. Mr. Jerry Malechi, Code 442EP 1
Office of Naval Research

800 North Quincy Street
Arlington, Virginia 22217

26. Mr. Russell Maxwell — 1
Systems Engineering Division 5264
Sandia National Laboratories
Alburquerque, New Mexico 87185

27. CAPT. Paul Chetelier — 1
OUSD R&D
Room 3D129 Pentagon
Washinton D.C. 20301

28. Mr. Dave Pallett — 1
National Bureau of Standards
Building A216
Gathersburg, Maryland 20899

29. Mr. Don McKechnie — 1
AFAMRL HEF
Wright Patterson AFB, Ohio 45433

30. Mr. Dale Nelson — 1
Eye Dentify Inc.
Box 3827
Portland, Oregon 97208

31. Bob and Beverly Williges — 1
Department of IE & OR
Virginia Polytechnical Institute
130 Whittmore Hall
Blacksburg, Virginia 24061

32. Dr. Tyce DeYoung — 1
SPAWARSYSCOM, Code 6131
Washington D.C. 20363-5100

33. Mr. Chuck Fargo — 1
7842 Melba Avenue
Canoga Park, California 91404

34. Mr. Dick Chanda — 1
Rockwell International
Rocky Flats Plant
Box 464
Golden, Colorado 80401

Thesis
L4758 Leigh
c.1 Examining the reliability of a retinal recognition device as database size and the number of enrollment scans are varied for applications in Command, Control, and Communications (C^3).