

AD-A103 314

RAND CORP SANTA MONICA CA

F/G 5/11

INCREASING EFFICIENCY IN THE CRIMINAL JUSTICE SYSTEM: THE USE O--ETC(U)

SEP 80 J A RATKOVIC

RAND/P-6546

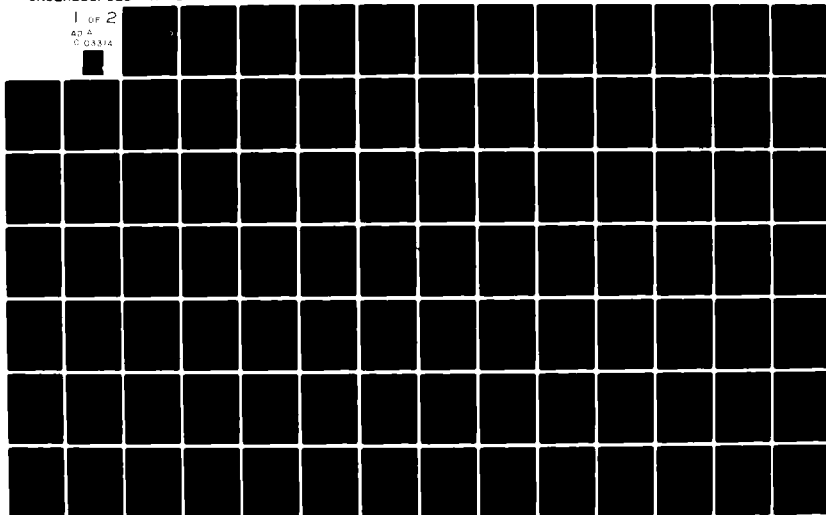
NL

UNCLASSIFIED

1 OF 2

AD A

Q 0334



AD A103314

LEVEL ~~II~~

(1)

INCREASING EFFICIENCY IN THE CRIMINAL JUSTICE SYSTEM:
THE USE OF NEW TECHNOLOGY FOR CRIMINAL
IDENTIFICATION AND LATENT PRINT PROCESSING

Joseph A. Ratkovic

DTIC
DATE

AUG 26 1981

H

September 1980

DMC FILE COPY

DISTRIBUTION STATEMENT A

Approved for public release
Distribution Unlimited

(14)

P-6546

81 8 25 102

MANUSCRIPT

The Rand Paper Series

Papers are issued by The Rand Corporation as a service to its professional staff. Their purpose is to facilitate the exchange of ideas among those who share the author's research interests; Papers are not reports prepared in fulfillment of Rand's contracts or grants. Views expressed in a Paper are the author's own, and are not necessarily shared by Rand or its research sponsors.

The Rand Corporation
Santa Monica, California 90406

PREFACE

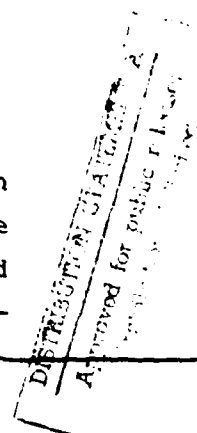
The original version of this study was prepared as a dissertation in partial fulfillment of the requirements of the doctoral degree in policy analysis at The Rand Graduate Institute. The faculty committee that supervised and approved the dissertation consisted of Dr. Cullen M. Crain, Chairman, Dr. Gene H. Fisher, and Dr. C. Robert Roll.

In today's society, where resources for addressing urgent problems are often in short supply, it is critical that these resources be expended wisely. The role of policy analysis is to see that this happens--that resources, even if not employed optimally, at least are not allocated to relatively unimportant or unsolvable problems. More specifically, policy analysis should:

1. Identify important problem areas where something can be done with a reasonably high payoff.
2. Examine all reasonable alternative solutions (technical, economic, political, and organizational) and list the more attractive alternatives.
3. For each alternative solution, specify the uncertainties and describe a research process for clearing up these uncertainties, or design into the solution hedges against uncertainty.

↓

The purpose of the present study is to apply these methods of analysis to the problem of identifying criminals by way of their fingerprints. The report examines the utility of systems for improving the processing of identification and latent prints, and concludes that the possibility exists for significant advances in the ability to apprehend wanted criminals and identify suspects in unsolved crimes. The report also examines a number of alternative solutions (including economic, political, and technical ones), and determines the most promising to solve the entire fingerprint processing problem. The author specifies the general approach to a



system, identifies the major uncertainties in solving the problem, and defines the research required to resolve uncertainties. Organizational, political, and social constraints for the solution alternatives are also examined to ensure total system feasibility.

Concept formulation for this work began in early 1977 when Rand was completing a report for the Department of Defense on estimation techniques for use in image correlation. Howland Bailey, Frederick Blackwell, and the present author (all of Rand) believed that the estimation process held much promise for distinguishing true matches from false ones. At this time a number of Rand researchers (including the author) visited Sacramento to talk to staff members of the Bureau of Identification of the State of California concerning the nature and size of their fingerprint problem. The Rand researchers learned that the problem of automated print matching, as expected, had not been overcome with so-called minutiae matching. Soon after, Blackwell also visited a few sites where minutiae matching systems were in operation. It was then that the author decided to put together a small briefing that proposed using digital image correlation to attack the problem. At the same time the author and others also examined optical correlation systems that were being tried in print matching, but felt that they could not accommodate geometric errors associated with prints.

Toward the end of 1977 and early in 1978, Blackwell and the author, with the help of D. M. Landi, Rand vice president and head of Rand's National Security Research Division, briefed this concept to the Law Enforcement Assistance Administration (LEAA), U.S. Department of Justice. LEAA suggested that they discuss the ideas with the Federal Bureau of Investigation's automated fingerprint section, headed by John M. Jones. They found the Bureau totally devoted to developing a minutiae matching system for identification; no interest was expressed in developing an image matching system. So the next nine months or so were spent in talking to local police agencies concerning their needs and requirements for an automated system. Out of these discussions grew the idea of developing a complete system that could not only handle the entire task of print matching, but could also display and communicate electronically the print imagery to other agencies.

Toward the end of 1978, the author integrated many of his notions of a complete system design into a briefing that was more system-oriented, with emphasis on automating the entire process. About this time Mario Juncosa of Rand started to examine the problem of analytically modeling both the minutiae matching and the image matching processes. It was concluded that the image matching system had a significant edge over the minutiae matching technique. (A paper on the subject is in preparation.) Juncosa and the author briefed the fingerprint package to a number of law enforcement agencies locally, fielding questions about hardware feasibility and cost.

To this point, study had been limited to examining the feasibility of building a processor that could handle a large volume of prints at a high data rate. At the end of 1978, Malcolm Davis of Rand produced a preliminary hardware design that could solve the entire system problem. He also costed the components, thus giving the author a benchmark to go by for a preliminary design. These cost data were used in conjunction with other data to compare the discounted value of automated systems with the cost of present manual systems. In early 1979 the author briefed the package to representatives of the Bureau of Identification. They expressed an interest in the concept and furnished cost data for the manual system. They too had priced out an automated system (both ID and latent systems), one similar in hardware cost to the Rand design. Those data were to prove valuable for the cost/benefit analysis performed by the author in mid-1979 to compare the automated system with the manual approach.

ACKNOWLEDGMENTS

I would like to acknowledge with gratitude the contributions of the following individuals. First, Frederick Blackwell and Howland Bailey were instrumental in initiating some of the technical aspects of the study. Malcolm Davis was responsible for planning the computer software design and for assessing the hardware capability to meet performance guidelines. Mario Juncosa was instrumental in the mathematical modeling of some aspects of the process, and was a valuable aide in preparing and supporting the briefings. Jan Chaiken, William Graham, Peter Greenwood, Hy Shulman, and Willis Ware provided overall guidance and direction to the study. Cullen Crain, Gene Fisher, and Robert Roll provided an excellent review of the study, greatly improving its content. Gene Gritton and David Lyon provided administrative support.

Outside the Rand community a number of individuals provided insight into the overall problem and aid in establishing guidelines. Leonard Berdan of the Santa Monica Police Department was an invaluable asset who provided us with much needed information on the operational aspects of the problem and also provided us with numerous contacts through which much of the system utility data was gathered. Ray Middleton and Gerald Gilbertson of the California Bureau of Identification provided us with cost and requirements data on their automated fingerprint project for a state system. Bob Delahunt (Los Angeles Sheriff's Department), and Connie Speck and Jack Carter (Los Angeles Police Department) provided valuable insight into the operational problems of fingerprint processing in a large city police department. The police personnel who completed our survey questionnaire provided us with first source data on the extent of local fingerprint processing throughout the State of California. Many thanks to all the police personnel who contributed to this effort.

Accession For	
NTIS GRA&I	
DTIC TAB	
Unannounced	
Justification	
By	
Date	
Dist	
<i>de m. f. e.</i>	

PRECEDING PAGE BLANK-NOT FILMED

CONTENTS

PREFACE	iii
ACKNOWLEDGMENTS	vii
Section	
I. INTRODUCTION	1
Criminal Identification Processing	3
Latent Print Processing	8
Roadmap	13
II. THE PROCESS OF CRIMINAL IDENTIFICATION AND LATENT PRINT UTILIZATION	15
The Criminal ID Process	15
The Latent Print Process	18
Print Processing Requirements	19
III. DEFINITION OF AUTOMATED PROCESSING ALTERNATIVES	24
Criminal ID	24
Latent Print Processing	32
IV. HARDWARE FEASIBILITY AND PERFORMANCE CONSIDERATIONS	33
Hardware	33
System Configuration	37
Investment Cost Considerations	39
Anticipated Performance	42
V. COST/BENEFIT ANALYSIS--ID PRINTS	48
Methodology	48
Assessment--Automating the Central Processor	49
Assessment--Automating Local Booking Stations	57
VI. COST/BENEFIT ANALYSIS--LATENT PRINTS	66
Methodology	66
System Benefits	67
VII. INTERNAL AND EXTERNAL CONSIDERATIONS FOR THE PRINT PROCESSING PROBLEM	71
Internal Organizational Solutions	71
Other System Considerations	76
VIII. UNCERTAINTIES	83
IX. CONCLUSIONS	93
REFERENCES	95

Appendix

A. A BRIEF DESCRIPTION OF THE CHARACTERISTICS OF FINGERPRINTS	100
B. MATCHING PROCESS	106
C. DEVELOPING A FEASIBLE MATCHING SYSTEM	119
D. PRINT IMAGERY VERSUS PRINT MINUTIAE	128
E. RELEVANT MILITARY EXPERIENCE	136
F. PROJECTIONS OF FUTURE COMPUTER SYSTEMS	144
G. SURVEY QUESTIONNAIRE	148

I. INTRODUCTION

Policymakers are concerned with the ever-increasing crime rate. Numerous policy options have been examined and some implemented in an attempt to either change or control criminal behavior (e.g., rehabilitation, determinant sentencing, etc.) or to improve the effectiveness or efficiency of criminal justice agencies (e.g., patrol car radios, computer storage and retrieval of criminal files, structuring of patrol car routes, etc.). The spectrum of policy options examined has encompassed organizational changes, economic assistance, and technological aids to federal, state, and local criminal justice agencies. Of these policy options, technological assistance has probably had the greatest variability in impact with some great successes and some large failures. Two criminal justice areas not previously explored, where readily available advanced technology would appear to have a significant impact, are the criminal identification and latent print processing tasks. Technology assistance affords the opportunity not only to make these areas cost effective but also improve the overall effectiveness by which criminal justice agencies apprehend and retain criminals. This report evaluates the role of technology in assisting these two criminal justice areas.

The criminal identification problem requires a suspect to be positively identified at the time of arrest. This process involves taking the prints of a suspect and sequentially checking them against local, state, and federal files to determine the suspect's true identity. By doing so, it can be determined if the suspect has had a previous criminal history or is presently wanted for a crime by some law enforcement agency. Criminals often leave clues at the site of crime scenes which can be used to identify them. One of the best clues left at crime scenes is latent fingerprints. If properly processed against local, state, and federal files they could significantly aid in solving crimes.

Currently the criminal justice system is faced with two problems in the ID area. First, rising costs of manpower coupled with the need for more manpower to meet the needs of an evergrowing criminal file are causes for fiscal concern. Automation of parts of the system could potentially be a most cost-effective means of dealing with this problem. The second problem is that the system is not totally effective in retaining wanted criminals even when they have been arrested. Long delays (relative to the time it takes an arrestee to bail out) in positively identifying arrestees makes it possible for criminals wanted for crimes elsewhere to escape the system via the bail process. Automation and communication technology affords the opportunity to deny this escape route making for a more effective system.

Latent prints are a positive means of identifying criminal suspects, and also have significant weight in supporting and shortening the prosecutor's case. Due to the enormous manpower resources required to search criminal files for suspects, they are virtually never used as a means of identifying suspects unless other clues as to the suspect's identity are available. The reason for this is that the present criminal file system is not organized to accommodate (partial or complete) print images of less than a complete set of ten-print images. Even if a separate file was organized to deal with latent prints there is no means of avoiding searching a large subset of the file to locate a subject. Essentially, in the latent print case, the entire criminal file must be searched. Automation of the process affords the criminal justice community with a number of opportunities beyond that of identifying suspects. Such automation also affords the opportunity to reduce police investigation time and, by solving a greater portion of crimes, a reduction in the crime rate is possible.

This section will briefly describe the current "status quo", its deficiencies, and enumerate the benefits of both the ID and latent processes.

CRIMINAL IDENTIFICATION PROCESSING

Before describing the process associated with criminal ID and latent print investigations it is desirable to lay the groundwork for an automated ID system. This can be done in three stages--examining the deficiencies in the present manual process, understanding the weakness in past attempts to automate the system, and an enumeration of the benefits to the criminal justice system of a fully automated system.

Manual processing of fingerprints has been around for a long time, as indicated in Table 1.1. Up to the 1960s the processing of fingerprints was done entirely manually.

Table 1.1

DACTYLOSCOPY

Chronology		
1000 BC	--	Early Egyptians and Chinese used thumb-prints to identify criminals and record business transactions.
1870-1880	--	Fingerprint identification of criminals begins with Herschel and Faulds.
1890	--	Galton invents fingerprint system similar to Henry system.
1900	--	Henry system emerges.
Mid-1960s	--	Research begins on automated systems.
1970s	--	First commercial semiautomated systems for criminal ID and latent print investigation.

The deficiencies of the present manual process and past attempts to automate the process can be examined in light of the potential benefits from a fully automated system. These benefits, shown in Table 1.2, are broken down by three major system components:

- o An electronic data link to rapidly communicate prints from local agencies to state and federal identification bureaus

Table 1.2

POTENTIAL CRIMINAL JUSTICE BENEFITS OF AN AUTOMATED ID SYSTEM

System Components	Benefits
Electronic Data Links Between ID Agencies	-- Rapid positive ID -- Justice served and deterrence enhanced in retaining want-and-warrant suspects -- Less crime -- Reduced police investigation time -- Reduced ID system complexity, redundancy, and manpower staffing
Computer Matching	-- System less manpower-intensive and constrained
Digital Image Storage	-- High reliability in performing ID task -- Eliminate hardware and manpower redundancy in maintaining multiple files -- Enhance manpower efficiency through computer-aided displays -- Future potential for taking advantage of high technology trends in computer processing and storage

- o A computer to perform the matching of the ID print against the file
- o A digital memory to store print imagery of the entire master file

Present manual systems perform the matching task reasonably well (with a 90-percent accuracy rating); however, they suffer from significant time delays in moving prints from the local agency to the state and, finally, to the FBI. In moving print cards (generally via mail) from the local agency to the state, it may take anywhere from a few days to several weeks. The state, after it completes its search, forwards the print card to the FBI, with resulting elapsed times for an ID to be returned to a local agency from the FBI on the

order of a few weeks to a few months. It would be highly desirable to rapidly obtain a positive ID on a suspect while he is still in custody. The benefits of a rapid ID system are enumerated in Table 1.2 and are discussed below.

Justice can be better served and deterrence enhanced by identifying and retaining want-and-warrant suspects before they can post bail. Posting bail generally occurs within a few hours after arrest, depending on the severity of the crime. Currently a positive ID can only be achieved if the suspect has had a previous arrest at the local agency; otherwise, it is unlikely that he can be positively identified before posting of bail. Rapid suspect identification has a number of implications for the criminal justice system. First, if the suspect has had a previous record, it will generally result in a significantly higher bail being set, making it more difficult for him to bail out. Second, if the suspect has an outstanding want or warrant, it will be much easier to locate him in the want-and-warrant system with a positive ID before he might escape on bail. The present want-and-warrant system is not a "foolproof" system in that a clever criminal can beat the system. A positive suspect ID, before he is available for release on bail, would thus facilitate the want-and-warrant system, possibly preventing the release on bail of a wanted criminal. Third, retaining want-and-warrant suspects, who might otherwise escape without a rapid ID system, and raising the bail on previously convicted felons (identified via rapid ID) should by means of their incarceration reduce the crime rate.

Not being capable of identifying want-and-warrant suspects at the time of arrest also increases police staffing and investigation time as additional staffing and investigation time is required to follow up on these cases. Presently in Los Angeles County alone the understaffing of law enforcement agencies has led to a backlog of 816,297 arrest warrants of which 30,000 are for felonies. An automated system potentially could eliminate much of this enormous backlog and reduce the manpower requirements on want-and-warrant follow-up work.

The major historical reason for local police agencies to develop an ID bureau along with a master file print was that they wanted a rapid ID system and found the long delays in obtaining results from the state level unacceptable. A rapid electronic link between local and state agencies would eliminate the necessity of local ID bureaus and files, thus eliminating much redundancy and reducing staffing requirements in the ID system.

To indicate the magnitude of the identification problem, the FBI in Los Angeles handles about 400 cases monthly. This local office receives about six to eight teletypes a month back from Washington Headquarters, indicating that a suspect wanted by the FBI is being held in custody by a local police agency. Since the time it takes between arrest by the local agency and the identification reaching Washington is on the order of months, in virtually none of these cases is the suspect still in custody. [11]

The State of California has indicated that, between January 1977 and the first quarter of 1979, 6500 criminals lied about their identity and had warrants outstanding. [1] It is possible that all of these individuals could have bailed out of the system before any outstanding warrants could have caught up with them since they were not identified by the local arresting agency. Based on the first quarter of 1979 rate of 900 criminals lying about identity and who had warrants outstanding, and factoring in the 10-percent error rate in identifying criminals, it appears that in California there are potentially 4000 to 5000 criminals who could escape warrants in 1979 even though they were arrested by some other police agency. Generally these warrants are of a more serious nature and, when considering these magnitudes relative to the prison population of California of 20,000 such a process could be extremely significant. Presently an individual can be out on bail within a few hours after arrest. Thus, if one is going to improve identification speed, it is necessary to get this time down to a couple of hours, which would require electronic data links between the local arresting agency and the State Bureau of Identification.

Previous attempts, begun in the mid-1960s as shown in Table 1.1, at automating the process have concentrated on the matching aspect of the problem. In the era when this automated processing research work was started computer memories were not large enough to store digital representations of fingerprint imagery. In that era there was also an emphasis on trying to replicate on the computer the manual methods of print processing. These two factors had two important effects on the nature of the processing. First, without the fingerprint imagery, the only phases of the fingerprint processing problem which could be attacked were the matching and classification phases. Second, the emphasis was shifted away from working with the imagery toward working with a subset of the total information contained within the print, known as minutiae. The automated approach taken back in the 1960s, which has led to the automated system we see commercially available today, did not and probably could not consider a systems approach to attacking both the ID and latent print problems. These past approaches concentrated on making the system less manpower-intensive by substituting computers for fingerprint technicians in the matching process. These approaches have not improved the effectiveness of the system which can only be achieved by a rapid ID system using electronic links. The nature of the approach using minutiae and discarding imagery has eliminated completely the possibility of these systems effectively employing electronic data links from the local level to higher level ID bureaus.

The use of minutiae to the exclusion of imagery also limits the amount of manpower substitution which can be achieved. The use of digital image storage can enhance manpower efficiency through the use of computer-aided displays in the final phase of matching where verification must be achieved manually. In a minutiae-based approach a separate file must still be maintained containing the fingerprint images for final verification, whereas an image storage system requires only one file and can either store minutiae (if required) as a subset segment of the file or via algorithm retrieve minutiae from the imagery. Thus electronic image storage can eliminate hardware and manpower redundancies associated with keeping and maintaining

multiple files. Systems designed around digital imagery also offer the potential for taking advantage of favorable high technology trends in computer processing and storage. They also offer the potential of higher reliability in performing the matching task.

To summarize, the benefits of a fully automated ID system listed in Table 1.2 indicate (1) significant advantages attributed to a rapid ID system which cannot be achieved using manual or past automated approaches, (2) some marginal advantages over present-day manual processes in automating the computer matching process alone, and (3) some present and potentially high future advantages in using electronic imagery of the print.

LATENT PRINT PROCESSING

Latent prints, while offering the potential, are in fact rarely used to identify suspects, the reason being the massive manpower effort required to search files in turning up suspects. For poor quality prints it would take approximately 100 million fingerprint technicians to handle the daily anticipated workload for a large state like California (see note 1). Even for excellent quality imagery it would require approximately 5000 fingerprint technicians to perform this workload (see note 2).

Technology affords the opportunity to automate this search process giving law enforcement officials the means for identifying suspects from latents. Such a capability could revolutionize the criminal justice community by affording the following benefits beyond the present "status quo":

1. Increase in felony arrests
2. Increased recovery of stolen property
3. Increase in utility of latent prints lifted
4. Reduced crime rate
5. Reduced investigation time

We shall attempt to quantify some of these benefits as they might be reflected in a large state such as California.

1. Increased Felony Arrests

In a state like California, with an estimated 1000 latents from 1000 crimes available for cold search identification per day,* the payoff would be (according to Greenwood's study [3]) an additional 200 to 400 suspects identified per day. Presently only about 10 to 20 percent of these estimated 1000 latents actually are identified on the basis of a cold search; thus, it appears that the payoff can be significant. Burglary is the crime for which latents are most often lifted. Presently in California about 10,000 suspects are identified annually via latents lifted from the crime scene. A California study [16] indicates that an additional 23,000 burglary suspects and 2000 other major criminals could be identified if an ideal automated latent print system were to be developed (see Tables 1.3 and 1.4). This would mean an increase in suspects identified by means of latents from the present rate of 5 percent of all crime scenes searched to 16 percent based on a projected cold search hit rate of 36 percent for an ideal system.

2. Increased Recovery of Stolen Property

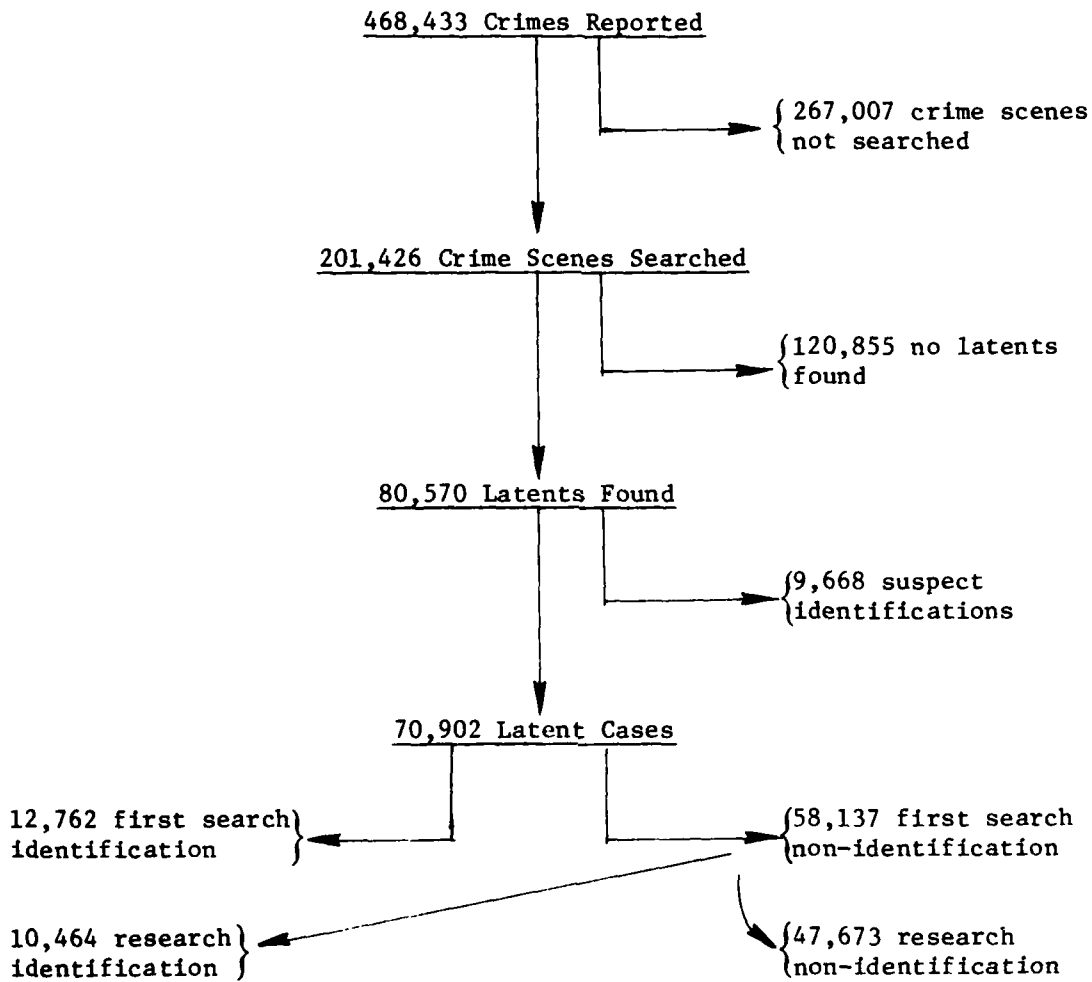
The latent print system (with its potential for rapid identification of suspects in burglary or robbery cases) is more likely to locate stolen goods before they are fenced. The State of California has estimated this benefit at \$2.72M/yr. If we were to use this as a mean estimate for the number of burglaries eliminated annually via a latent system and take the average property loss given by FBI statistics [6] to be \$292/loss then this translates into an even higher potential annual saving to consumers of \$10.8M.

An additional benefit of such a latent print system would be in identifying the owners of recovered stolen property. Much of the stolen property does not get returned to its proper owner because of a lack of positive means of identifying the property. At the time of

*The term "cold search" indicates searching the fingerprint file with no information other than the fingerprint image itself.

Table 1.3

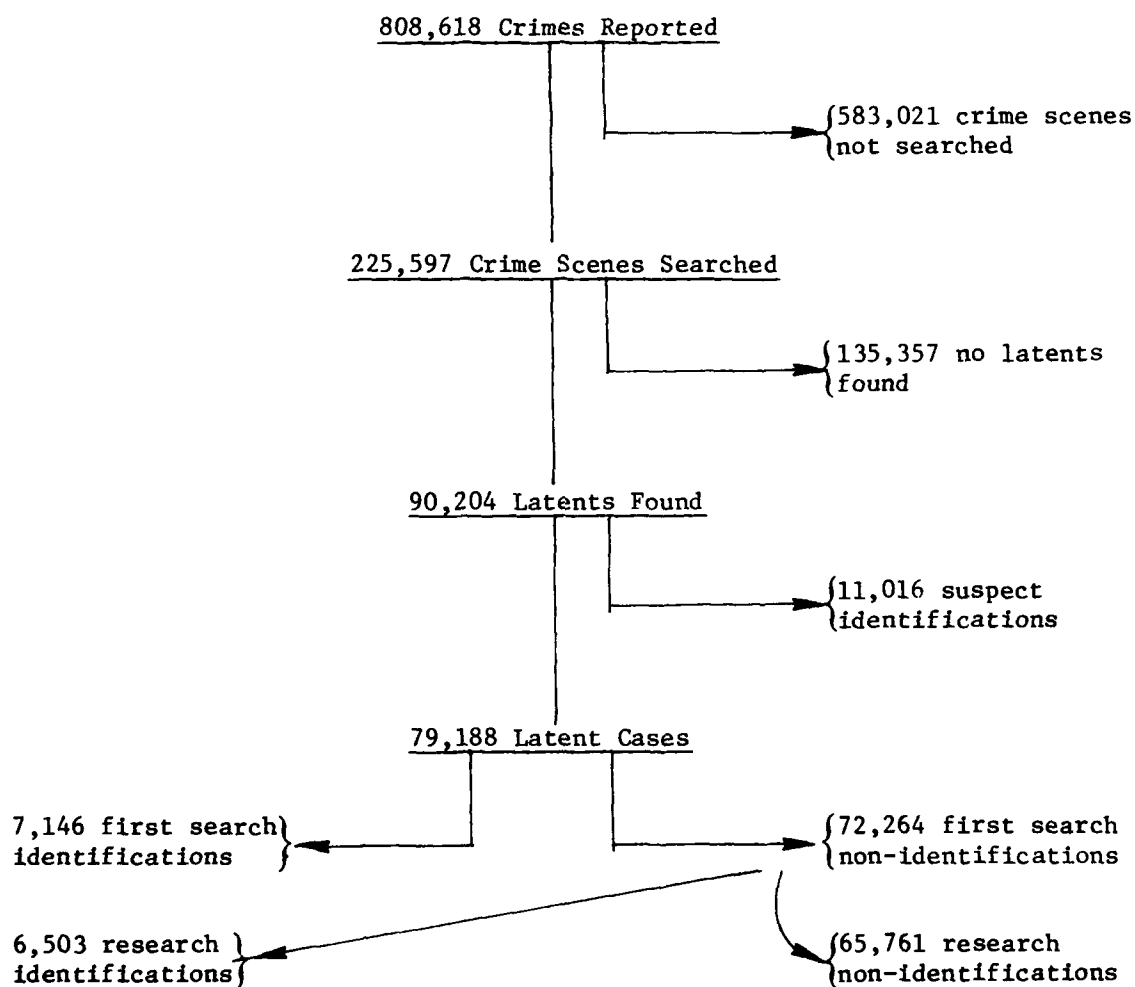
IDEAL LATENT SYSTEM VOLUMES, 1975 (BURGLARY)



Source: Reference 13

Table 1.4

SYSTEM VOLUMES FOR MAJOR CRIMES (1975 VOLUMES)



Source: Reference 13

the property loss report, the fingerprint imagery of the owner could be taken and compared to those fingerprints lifted from recovered property (of a similar description) for a possible match.

3. Increase in the Utility of Latent Prints Lifted

It is estimated that about 20 percent of all latents lifted are actually utilized in request searches or manual cold searches; thus, a fully automated latent print system could potentially increase the utility of latents by a factor of 5 (20 to 100 percent). [1,14]

Latent prints may also have utility in other parts of the criminal justice system. For instance, such a system could solidify the prosecutor's case when the suspect goes to court, lessening the opportunity for plea bargaining and reducing overall court workload. Additionally, a latent print processing system might tie a suspect into a number of crimes, making it tougher for the criminal to get off with a light sentence. Such a system could also have some negative impacts. If the system were successful in identifying and convicting more criminals it could require more prison facilities be constructed to house the additional criminals.

4. Reduction in the Crime Rate

The total number of burglars operating annually in the state can be estimated (based on the 90,000 burglary total) [7] to be somewhere between 5700 to 30,000 depending on the mean annual number of offenses (estimates vary from 3 to 15.59). [3] If, for an ideal automated system, all additional arrests (23,000) never involved the same suspects, then using the high estimate for the number of burglars in the state, this would represent capturing 77 percent of the burglar market (a high estimate). If, on the other hand, we consider that only those highly active criminals (i.e., those with a mean annual offense rate of 15.59) were actually netted in the 23,000 figure, then this would mean a low capture rate of approximately 1500 burglars (a low estimate) which is an estimated 5 percent of the burglar market capture. Using the mean estimate for the fraction of the burglar market captured would indicate that the ideal latent system could potentially remove 37,000 additional burglaries from the books even though only 23,000 burglary suspects were identified if

these burglars were locked up for one year. These numbers should be considered significant when viewed relative to the California prison population of 20,000.

5. Reduced Investigation Time

The state has indicated that a proposed small system making only 13,600 identifications per year would reduce the amount of investigation time spent in California by 2.04 million hours and have a dollar value of \$20.4M per year. However, this is based on a cold search identification saving of an average of 150 investigative hours. In actual fact, many of the burglaries are never investigated, i.e., reports are taken and placed in a folder in the hope that someone confesses or a tip is given. Thus, it is difficult to assess the time value of this benefit in monetary terms. For the sake of later analysis, we shall assume 50 percent of the state's value as an arbitrary evaluation of this benefit.

ROADMAP

This section of the report has briefly described the current "status quo", its deficiencies, and enumerated the benefits of both the ID and latent processes. In the next section of this report we shall examine in more detail the current process of criminal identification and latent print investigation. Processing requirements will also be discussed in order to obtain a baseline set of requirements for developing a fully automated system. In Section III we will show alternative automated system designs for improving the ID and latent print processes. We shall also present new technology advances (primarily in the computer display and matching algorithm areas) and show their roles in a new system design in Section IV. The methodology for comparing the current processes with alternative automated designs will be developed and the results of this comparison presented in Sections V and VI. In Section VII the organizational impact and problems associated with implementing an automated system design will be discussed. Uncertainties about the system design and system utility will be described in Section VIII, with the report's conclusions being presented in Section IX.

NOTES

1. In latent print processing, a fingerprint technician might be able to compare about 60 file prints an hour to a latent. The exact number of prints that a fingerprint technician can match will depend on the number of fingerprints lifted (e.g., all ten prints for a burglar taking out a jalousie) and the print quality. In the case of lifting all ten prints with good image quality, this situation can be reduced to an ID problem. Most of the latents lifted do not fall into this category. Let us first consider the worst case situation where the print quality is poor and images from only one or two fingers have been lifted. Considering that a fingerprint technician can handle about 500 print comparisons in a day on poor quality imagery and working with our standard file size of five million prints, it would take an individual on the order of 10^{*5} days (273 years) if he did not know from which finger the image came, and 10^{*4} (2.73 years) if the finger number were known for the image. This estimate presumes also that no classification is used in prescreening the file before a search is undertaken. It would thus take (worst case) 10^{*5} fingerprint technicians to check the one latent print against the file in one day. Considering, as estimated previously, that the number of latents to be processed in one day is on the order of 1000 for a five-million file size, it would take 10^{*8} fingerprint technicians (again, worst case) to check these prints one-on-one against the entire file. Obviously, employing 100 million fingerprint technicians is not realistic nor an economically attractive alternative to automated processing systems.

2. Choosing a more optimistic task environment for the normal processing of latent prints we shall presume that the fingerprint image can be identified as to which finger number it belongs, and if it cannot be identified it will not be processed. Let us presume also that the file has been broken down by a single print index (generally referred to as a ten-print card system since each of the fingerprints is separated from the ID card and placed and classified individually into the system). The classification process is unlikely to reduce the fraction of the file to be searched by more than 100 because part of the print image may be missing, which would not allow the roughly 1000 categories of the Batley system to be utilized completely. Even if we take the best case in which all 1000 categories can be utilized, and that there is a uniform distribution of prints among the categories (which is not the case), this still requires a search time for one man of ten days to complete a search of the file. If only 50 percent of the prints met the criterion (good image quality and finger number known) a staff of 5000 fingerprint technicians would be required to do latent print processing under rather optimistic circumstances.

II. THE PROCESS OF CRIMINAL IDENTIFICATION AND LATENT FINGERPRINT UTILIZATION

In the criminal justice area there are distinct roles for fingerprint processing. The first and foremost application is in criminal identification. Fingerprints are one of the few means for uniquely identifying an individual. As such, the print card taken at the time of suspect booking can (1) link an individual to a previous criminal history and (2) uncover any outstanding wants and warrants on the suspect. The other role of fingerprint processing is to identify suspects at the crime scene. Here fingerprints can be lifted from objects in the vicinity of the crime scene and from a crime victim. These prints, called latents, can then be utilized to identify suspects.

This section describes both the criminal ID and the latent print processes as they exist today. Later we shall discuss new technology and its role in expediting these processes by creating improved alternative means of performing these tasks. The end of this section is devoted to establishing print processing requirements that can be used in a baseline design for an automated system.

THE CRIMINAL ID PROCESS

The ID fingerprint card taken at the time of arrest is used by the local arresting agency, the state identification bureau, and, finally, the FBI in a long chain of events which, hopefully, will lead to a positive identification of the suspect. The entire process is described in Fig. 2.1. As indicated in the figure, when a suspect is arrested and his fingerprints have been taken at the police station, the job of identifying the suspect has just begun at the local level. The fingerprint card contains the "alleged" name of the suspect, and this is the first basis by which the master print file at the local police station is checked (if the police station contains a master print file; some local police departments rely solely on the

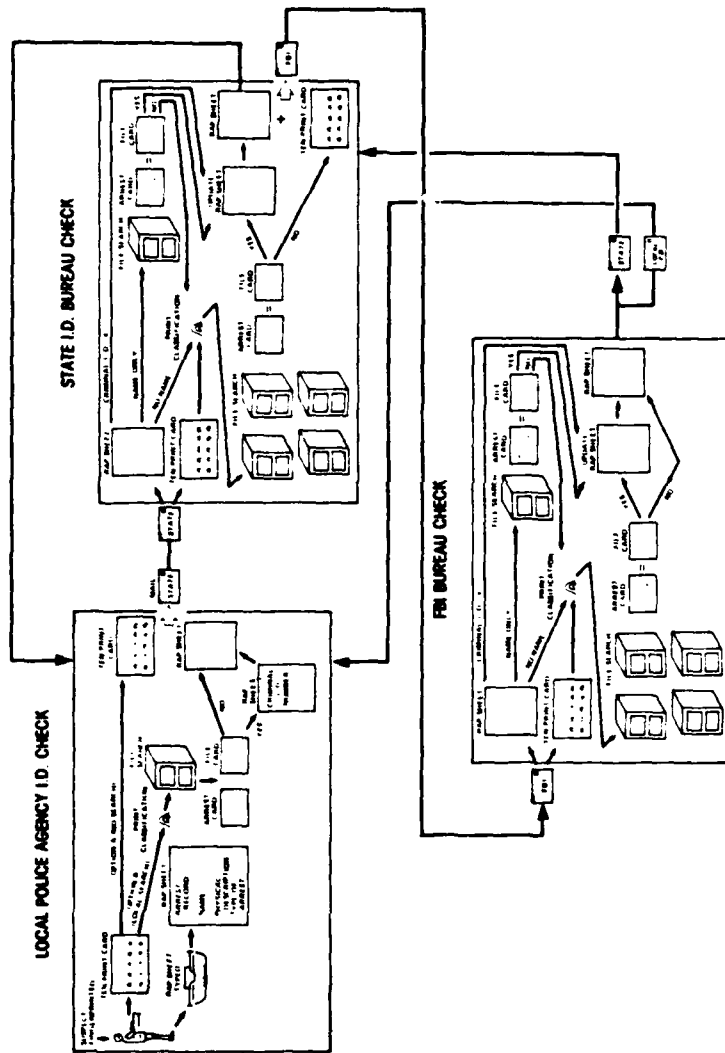


Fig. 2.1—Criminal ID Process

state law enforcement agencies to perform the ID task). Since it is quite easy for a suspect to lie about his identity (to hide either a past criminal identity or to escape from an outstanding warrant), it is generally necessary to search the file again using information contained within the print if a name check is unsuccessful. This extended search is a two-phase manual process. First, the print is classified via the Henry system or some other equivalent classification system.* Once the print has been classified, it is then manually checked for a match against all other prints in the master print file which have the same generic classification. If the suspect cannot be found in the master file at the local police agency, the ten-print card is then forwarded, along with the rap sheet (arrest record), to the state (generally via mail) for an ID check at that level. If the suspect has been identified at the local level then the card is forwarded to the state with a criminal ID number attached.

The state file will contain all the print files of all local police agencies within the state. As shown in Fig. 2.1 there are three different initial routes that can be used at the state level to identify a suspect. If a print card enters the state system with a criminal ID number attached (i.e., the local agency has located the suspect in its file) the state will check its file for this ID number and update the suspect's card and rap sheet with the new arrest. It will then be sent to the local arresting agency and (depending on the severity of the crime involved) the print card will be forwarded to the Federal Bureau of Investigation (FBI) to check for out-of-state criminal activity. If a print card enters the state system unidentified, the state will first initiate a name search. If this fails it will then utilize the classification process to check its files. The results of this check are then sent back to the arresting

*See Appendix A for a brief discussion of fingerprint classification.

agency with a copy of the suspect's rap sheet if he is found. The print card is then forwarded to the FBI for a further check.

The FBI files consist of everybody who has ever been fingerprinted and is still alive.* Thus all state and local files are contained within it.

It should be noted that the master print files of all police agencies consist of two separate groupings--one for criminals and one for applicants. The latter grouping refers to individuals who have been fingerprinted due to the sensitivity of their jobs (handling of classified documents, dangerous drugs, etc.), and as a condition of employment (generally for governmental positions). The purpose of this applicant fingerprinting and file is to ensure that the individual does not have a previous criminal record at the time of employment, and to inform employers of a criminal arrest of an individual. Applicant files make up a considerable portion (over 50 percent at the local level) of the total master print file and must be searched every time a suspect is arrested.

THE LATENT PRINT PROCESS

When a serious crime has been committed, a laboratory technician will be sent to the crime scene to record evidence that may prove useful in identifying suspects if none has been captured at the scene, or in solidifying the prosecutor's case at the time of the trial. The exact nature of which crimes are investigated by laboratory technicians, including fingerprint experts, will vary from one police agency to another, being primarily dependent on work load. Specifically, when prints are recovered at the scene of a crime, they are first checked against the prints of those individuals who would have been expected to be at the crime scene and would not expect to

*Files are generally purged upon receipt of notification of death of applicant or criminal and may be occasionally purged of older individuals and nonrecidivists, individuals who have committed less serious offenses.

be suspects (e.g., victim, police officers, etc.). These prints are often referred to as "elimination prints." The prints taken at the crime scene are then examined and those matching elimination prints are discarded. The residual prints can then be considered to potentially belong to the suspect.

What generally becomes of these prints? The answer depends on the quality of the latents and the size of the police agency and its work load. If the quality of the print is poor, nothing further is done with the print other than putting it in a crime jacket in the hope that, if further information becomes available, it will prove useful in solving the crime.

In the case of a small police department (with, say, less than 100,000 prints in the master file) it may be possible to perform some limited searching of the file to identify a suspect from a latent print. In this situation a separate file is created which will contain cards on which there is only a single print. Using a single-print classification scheme similar to the Henry system in principle, it is possible to search a small subset of this file (screened by classification) for a mate to the latent print provided the file size is not too large. Large police organizations generally do not search files for matches to latent prints and thus as indicated in Fig. 2.2 latent prints are just generally filed forever. The only times latent prints are used here are if there are definite suspects who have been identified via other means, or as a means of verification for a suspect who has confessed.

PRINT PROCESSING REQUIREMENTS

At the national level the FBI processes something on the order of 25,000 ID print checks per day on a file size of about 86 million.* These print checks include both criminal and applicant

*This is the total applicant and criminal file size. Normally, criminal checks are only made against an active file of 22 million.

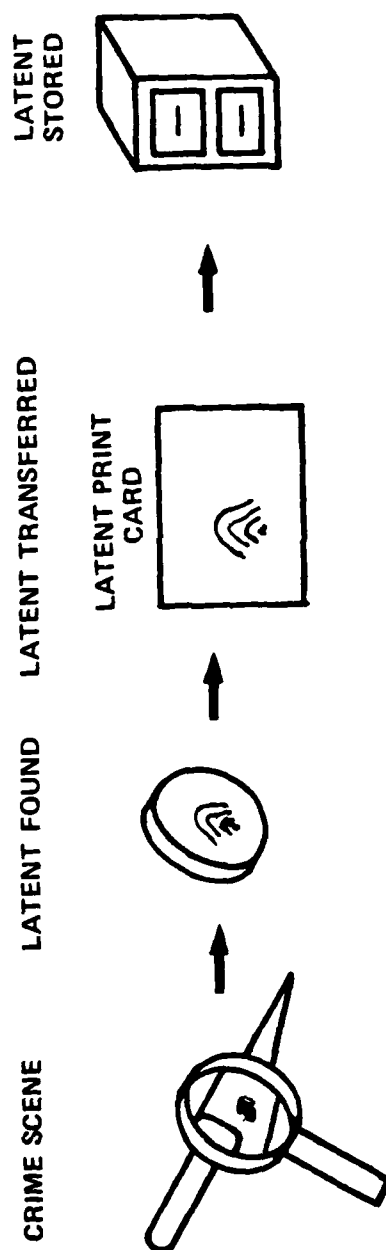


Fig. 2.2—Latent Print Process

requests. At the state level, a large state such as California would process on the order of 6000 checks per day against a file size of approximately 6 million. A small police department with, say, a 100,000-print file would be processing on the order of about 50 to 100 ID checks per day. [20] To place things in an order of magnitude perspective, the daily processing rates for the state and local police agencies can be considered a percentage of their file size (approximately 0.1 percent). Since all the local files are contained within the larger state master file it would be expected that these percentages would be about equal for the two police agencies. These processing rates, however, would be greater than those of the FBI since the FBI will only accept prints for crimes of a more serious nature. Thus, the FBI daily processing rates are on the order of 0.03 percent of its master file size. Figure 2.3 summarizes an estimate by Swanger and Jackson [17] of the overall identification requirements (file size versus inquiry rate) for criminal ID, access control, and fraud prevention. This report will concentrate its focus on examining the print processing problems (ID and latents) for a large state such as California.

The processing rate on latent prints is a more difficult number to estimate because so few police agencies actually do any print processing at all. One could infer an estimate based on the Greenwood study [15] which stated that between 20 and 40 percent of all crime scenes investigated yielded latent prints which could be used to identify a suspect. In the United States, there are about 11,000 crimes committed each day for which latent prints will be searched (murder, rape, robbery, aggravated assault, and burglary). [7] With only 20 to 40 percent of the crime scenes yielding prints of adequate quality, this would yield between 2000 and 4500 prints which would have to be processed daily in the nation. Since several latents are generally taken from each crime scene, the number of latent prints would be considerably more than this figure. A Santa Monica Police Department statistic indicates that the number of latents lifted is about equal to the total number of serious crimes committed. [21] So that even though there are only 2000 to 4500

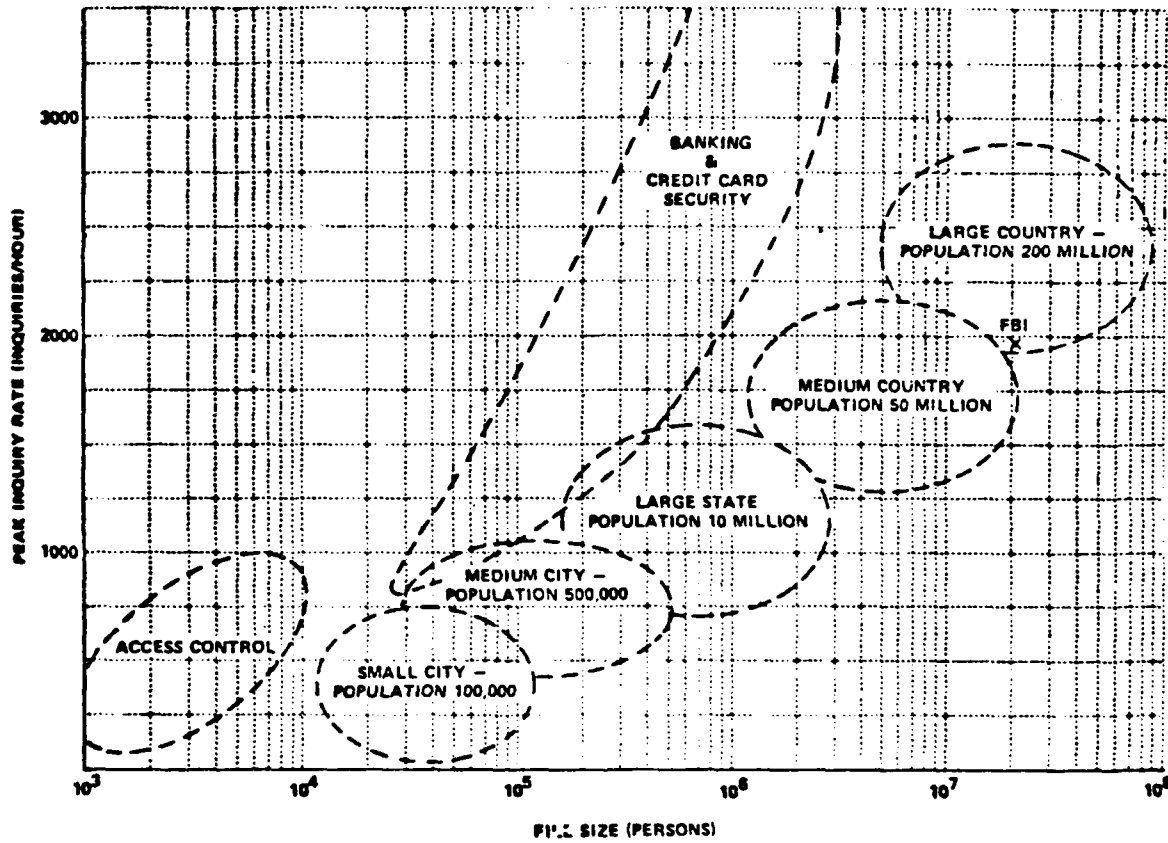


Fig. 2.3—The spectrum of personal identification environments (Ref. 17)

crime scenes a day from which latents are likely to yield useful clues to the identity of the suspect, there may be multiple latents lifted, resulting in an estimated 11,000 latents to be processed daily at the national level. This would translate to about 1100 latents to be processed daily in the State of California. This estimate agrees with an estimate generated within the California Department of Justice (DOJ) that an operational latent print processing system would have to handle about 900 latents per day. [16] Thus, a ball park estimate for latent processing in California would be around 1000 per day.

To summarize, the processing rates for a state like California will require that 6000 ID and 1000 latent prints be compared daily against a master file size of 5 million.*

*The actual file size of California is 6 million but purging of the files should eliminate about 1 million cards.

III. DEFINITION OF AUTOMATED PROCESSING ALTERNATIVES

In the previous section we have described the present methods by which ID and latent prints are processed. In this section alternative automated processing techniques will be discussed for both ID and latent print processing. Having described these processes in this section we shall discuss the relevant technology and demonstrate its feasibility in the subsequent section of this report.

CRIMINAL ID

In Fig. 2.1 the present process for identifying criminals was shown going from the local to the state level, and from the state to the federal level. For the purpose of this report we shall limit ourselves to developing an automated system capable of accommodating the processing needs of a large state, such as California. Such a system might also be developed on a regional basis to accommodate the needs of a number of smaller states located in the same geographic area. Figure 3.1, adapted from Fig. 2.1, shows this baseline system which will serve later as a basis for comparing alternative automated systems.

Two alternative systems will be examined. In the first system we shall consider automating the central station where the prints are processed at the state level. Here, as shown in Fig. 3.2, the process retains the status quo at the local level and is only automated at the central state processing facility. Another option which was considered and depicted in Fig. 3.3 was to automate the process at the local level, the advantage being that the process would not only benefit from automated processing of matching IDs at the state level but, by electronic communication of the print to the state level, rapid turnaround time could be achieved. This rapid turnaround time could prevent suspects from escaping a want-and-

Fig. 3.1--Criminal I.D. Process--State Level

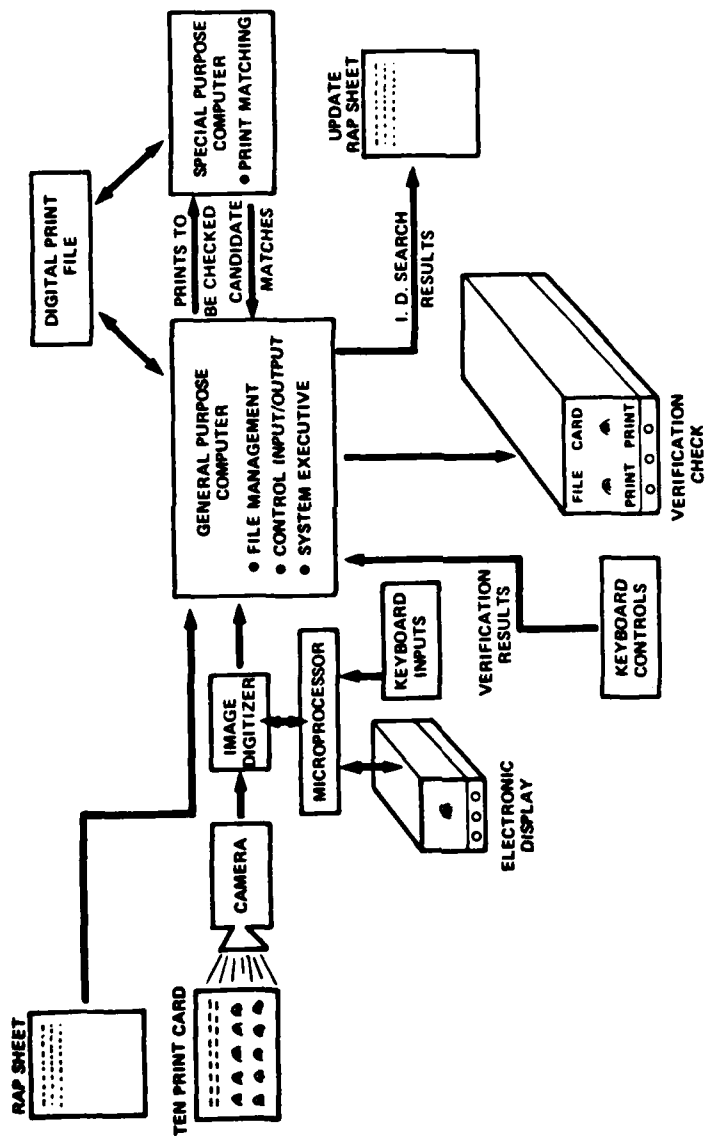


Fig. 3.2—Automated I.D. Check

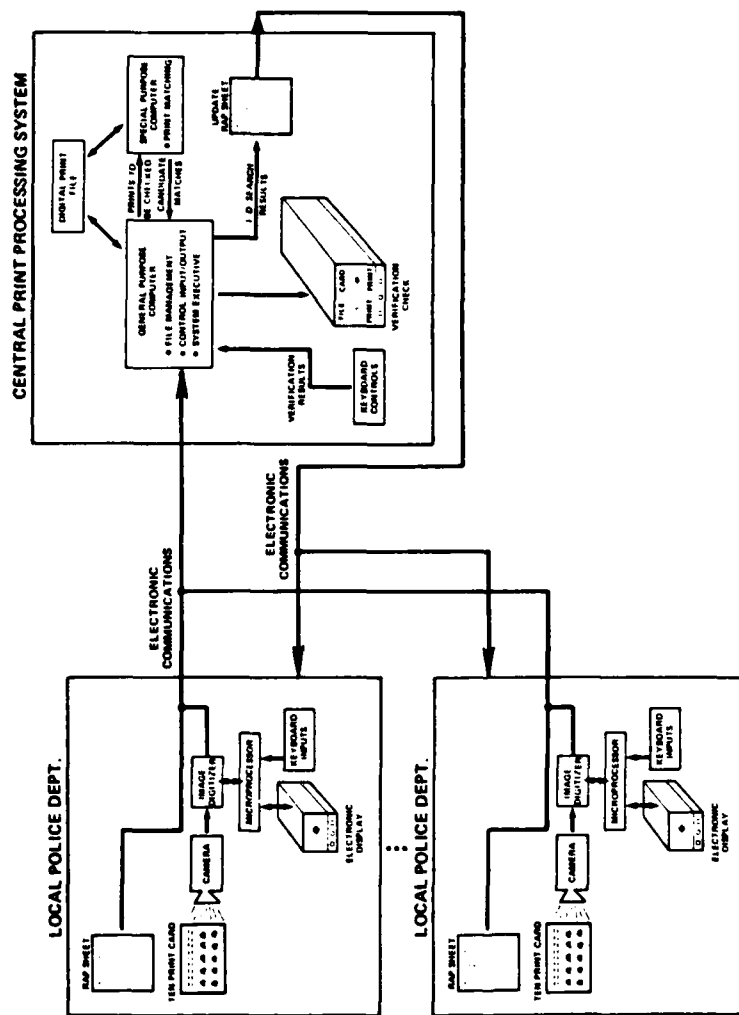


Fig. 3.3—Automated Distributed Fingerprint I.D. Network

warrant check and would eliminate the need for local files and ID checks. This elimination of redundancy in files and checks at the local levels could lead to sufficient cost savings as to be cost effective.

Returning to Fig. 3.2 the automation process begins when the print card and the rap sheet arrive at the mailroom of the state bureau of identification. First, the print must be converted to a representation with which a computer can work. This is done by scanning the fingerprint with a TV camera type device. The print is now in analog format and must be converted to digital format in order for the computer to operate on it. An analog-to-digital converter accomplishes this task. Simply put, the fingerprint image is broken up into a matrix of segments with the total number of segments depending on the resolution of the camera. Each segment can then be described by a numerical representation. The numerical representation represents the ridge/valley ratio contained within the segment. If, for instance, we considered everything as black or white with the ridges being black and the valleys being white, then in the extreme case we could weigh the amount of ridge area contained within a segment and, if it exceeded the valley area, could assign a numerical value of one to that part of the print segment. Thus, in this case we could describe a print image by a zero/one matrix representation.

If we wished to consider grey shadings (actually compute the amount of ridge area to valley area in a sensor resolution element) then the print would be described by a digital scale of intensity values with the maximum value designating a sensor resolution element being composed entirely of ridge structure and the minimum intensity value representing the total absence of a ridge pattern (i.e., the presence of a valley).

Having converted the print image into digital format and checked on an electronic display to ensure no irregularities, then the print is ready to be checked against the file to see if the file contains a like one. Here a general purpose computer can be used for managing the file. It can perform the following functions:

1. Provide queueing for both prints that need to be matched and those that must be verified.
2. Provide a basis for systematically searching the file, i.e., name search followed by classification search (if used), and finally a general file search.
3. Coordinate communications of the outcome of the ID search to the appropriate agencies.

The general purpose computer also controls the reading in and out of storage of the print imagery into a display for visual verification of a match, and into the special purpose computer either the digital representation of the print or some subset of features contained within the print imagery.

The function of the special purpose computer is to perform a high speed matching of the ten-print card against the file prints. Basically there are two different techniques for performing the matching--matching some feature contained in the print image (generally referred to as minutiae matching) or matching the entire image (generally referred to as image correlation). Basically minutiae matching techniques use the relative locations of features contained in the print (see Appendix A for description of print features) as the basis for computing the degree of similarity between prints. Image correlation systems use the print image itself and by overlaying and displacing the two images (by mathematical manipulation, not optical) one can locate the position at which the two prints have the highest degree of similarity or correlation. This correlation then becomes the basis for determining which prints (if any) are candidate matches. Appendix B contains a more detailed discussion of the matching process along with a description of the problems encountered in matching real-world prints.

The outcome of our investigation into the matching process has led to the first-order design concept for the matching process shown in Fig. 3.4. The detailed rationale for developing this first-order

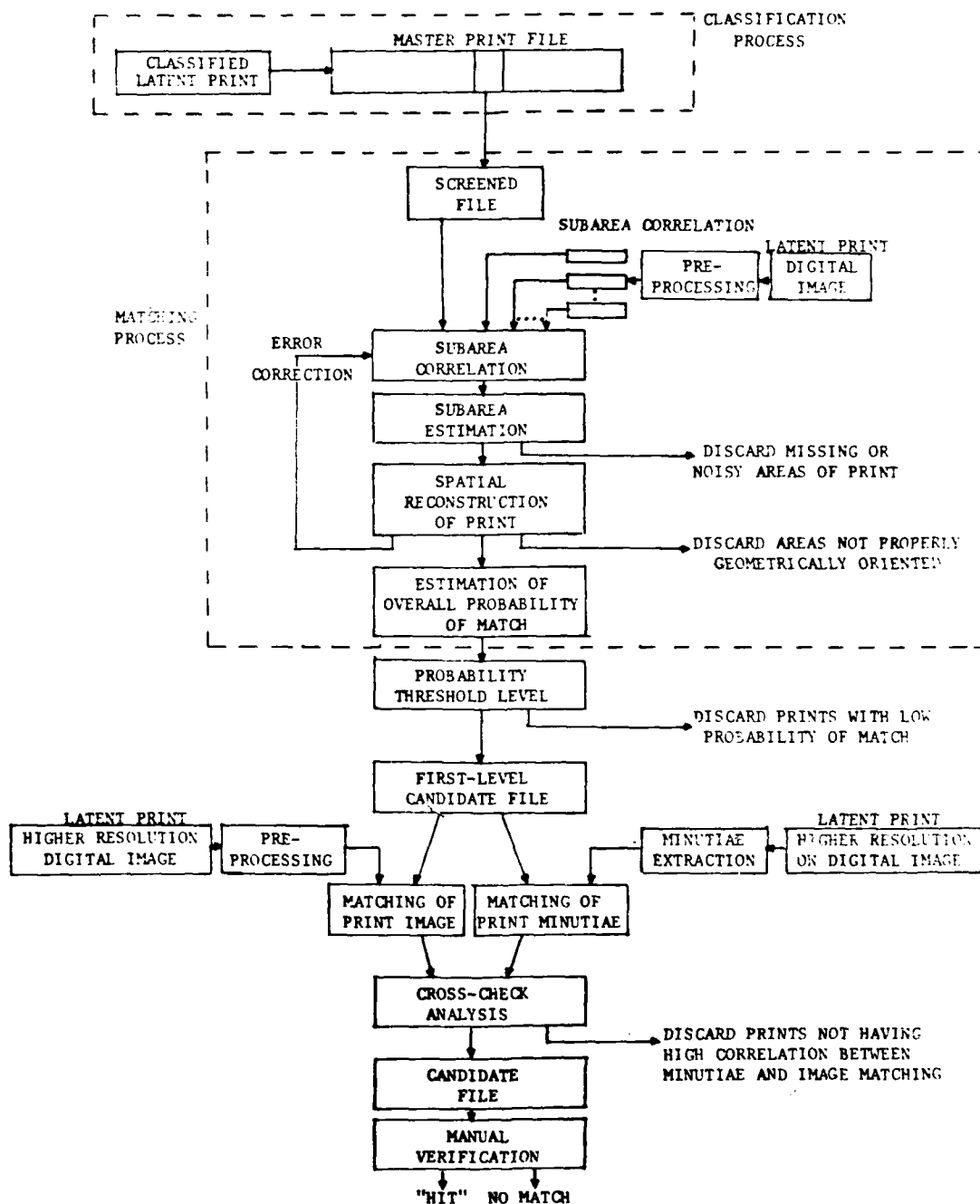


Fig. 3.4—Overall Block Diagram of Fingerprint Matching System

design is contained in Appendix C. The basic concept shown in Fig. 3.4 consists of a multilevel matching process. The first level uses an image correlation technique to overcome the two most difficult hurdles in the matching process--accommodating errors and generating an absolute measure of confidence that two prints do in fact match--and generate a first-level candidate file. This technique would use (probably) low resolution imagery to reduce the processing time, break the print image into a number of subareas to accommodate system errors (rotation, stretching, noise and missing areas), and then compute an overall estimate of the probability of match. Once this candidate list of matches was generated the second phase would consist of higher level screening using both the print features and the print image to develop a cross-check analysis to ensure agreement between the features and imagery. This second-level process would generate another candidate file which would be sent back to the general purpose computer to await verification by a fingerprint expert.

The general purpose computer, once candidate matches were generated, would pass on the ten-print card image and the candidate matches to an electronic display where a fingerprint technician could perform the verification task. The electronic display unit could (in addition to eliminating much of the manpower expended in searching files for candidate cards) ease the fatigue problem suffered by technicians through the use of computer-aided graphics.

This alternative system, shown in Fig. 3.2, does not allow for automation at the local level; consequently, much manpower and file redundancy remains in the process and the benefits of rapid criminal ID cannot be attained. In Fig. 3.3 we have considered an alternative system which has moved the print conversion task down to the local level. By doing so the print image could be transmitted electronically via phone lines to the central processor located at a regional or state facility. This would shorten the turnaround time from arrest to ID at the state level to probably less than two hours. With a drastic shortening of the time from a week(s) to hours there

would be little need to do any processing at the local level. Thus the local files and manpower required for local print processing could be eliminated and considerable resources saved.

In order to achieve a completely automated system down to the local level and to make full utilization of computer-aided graphics in the verification process it is necessary to utilize digital print imagery. With such imagery print minutiae can either be extracted directly from the imagery or stored with the imagery as a small subset file. The converse is not true--having only print minutiae does not lend itself to a complete systems approach. Appendix D reviews the system considerations associated with print and print minutiae in more detail.

LATENT PRINT PROCESSING

The latent print investigation process was depicted in Fig. 2.2 and described in Section II. The ID system developed in Fig. 3.4 is capable of accommodating both the ID matching task and the more difficult latent print problem. Basically this matching process is incorporated into the state system shown in Fig. 3.2 with a few modifications which can be used for solving both problems. In the latent print problem there generally is not a time urgency associated with moving the prints rapidly from the local level to the state level so that automation down to the local level does not appear to be a requirement. However, if the system were automated as depicted in Fig. 3.3 there is no reason why the latent process could not use the same electronic links (possibly during the off-peak hours) as the ID process.

In the next section of this report we will crystalize the hardware and technology required to develop the ID and latent systems we have generically described in this section. We shall also estimate the cost of this equipment so that cost/benefit comparisons can be made between the manual print process and the alternative ID automated processes presented here.

IV. HARDWARE FEASIBILITY AND PERFORMANCE CONSIDERATIONS

In this section we shall explore the hardware and software components necessary to build the automated systems described previously to see if they are currently available. With the answer to this question being shown here to be affirmative, and the processing speed (using current generation hardware) also being adequate (meeting specifications in Section II) for the ID and latent print tasks, we can then use this preliminary hardware layout to estimate some of the major system costs. These costs will be used in the two subsequent sections of this report to examine the relative costs and benefits of a system for solving the ID and latent print processing problems.

HARDWARE

A preliminary evaluation of currently available hardware has been made to determine the feasibility of designing and operating the automated fingerprint system that is suggested by this report. The principal equipment areas are:

1. Equipment for digitizing fingerprint images
2. Machine addressable storage for creation of digitized fingerprint data files
3. Data processing equipment for fingerprint data manipulation, analysis, file reading, and file management
4. Soft and hard copy display equipment for visual display and analysis of images
5. Data communications equipment for transmission of fingerprint images to a central location for analysis
6. A special purpose computer dedicated to the matching process.

We shall briefly describe the availability of these hardware components and then return to the total hardware system configuration and examine its cost.

1. Equipment for Digitizing

There are a number of commercial systems for digitizing images that are capable of achieving the required resolutions and at a modest cost. For the purpose of a study, we chose the DS-20F Quantex System that can digitize 20 images per second. This unit is suitable for a remote station, or a number of them could be used to create the original digitized image file. If the Quantex Digitizer is combined with a video camera, lenses, display, keyboard, card handler, and a microprocessor, a fingerprint digitizing terminal can be assembled for less than \$25,000.

2. Machine Addressable Storage

The approach to fingerprint analysis and identification proposed here requires that the complete digitized fingerprint image be stored as opposed to fingerprint features such as minutiae data. To select an approach for digitizing fingerprints, a number of things were considered, e.g., the resolution required, the number of gray levels, the media used for collecting fingerprints.

The data storage requirements depend upon (1) the master file size, and (2) the resolution required to describe an individual print image. For a fingerprint the resolution requirement would depend on the task. For matching low resolution, something on the order of 100 x 100 pixels per fingerprint image is probably adequate for a first-level matching process (applying the Shannon Sampling Theorem to an average fingerprint image containing about 40 ridges and valleys across it). For display purposes the resolution requirements of fingerprint imagery would be on the order of 512 x 512 pixels per fingerprint. With several gray levels being required for each pixel and ten prints per fingerprint card, the total number of bits required is on the order of 10^{*6} to 10^{*7} per ten-print card. When one considers that even small police departments have master file

sizes on the order of 100,000 ten-print cards, the total storage requirements are on the order of 10^{11} to 10^{12} data bits. This storage requirement is quite large even for today's large general purpose computers which only have disc storage capacities on the order of 10^7 to 10^8 bits. Thus, in the mid-1960s it did not look feasible to store sufficient data to perform correlation matching.

There have been within recent years a number of technological breakthroughs which now make the correlation approach as well as image storage for electronic display look technically feasible. These have been primarily in the area of mass storage devices and correlation chips which hold at a minimum 10^{11} data bits. Relative to mass storage units for creating an operational fingerprint file, there are three systems that have been developed that seem to meet the requirements of handling 500,000 fingerprints or more: the IBM-3850, the CDC mass storage system, and the Ampex TBM system. [25] Of these systems, the CDC system initially seems the most attractive because of price and operational features. The smallest CDC system handles 16 billion bytes (130 billion bits) of information, and is priced at \$200K. This unit would handle close to 2 million medium resolution images. For our hypothetical system we selected a master file of 5 million people (50 million individual fingerprints) based on the fingerprint processing requirements of a large state as established in Section II and estimated the purchase cost of the mass storage device at \$5M.

3. Data Processing Equipment

The general purpose computing power needed for a full-time operational system is not completely known at this time. Both IBM and Control Data recommend the use of a large main frame computer for the management of the mass storage unit. However, most mass storage systems contain a wide variety of data bases and many diversified users. Because of the unique nature of a fingerprint data file and the fingerprint matching method, it is felt a large-scale mini-computer can probably handle the file management input-output and the system supervisory functions. Machines of this class are generally in the \$100K range.

Current estimates indicate that a resolution of 512 x 512 lines (262,144 picture elements, sometimes referred to as pixels) is more than adequate for reproducing good quality images. It is further estimated that 128 x 128 lines (16,384 pixels) are adequate for computerized matching. The use of two gray levels seems sufficient for both computerized matching and for reproducing good images. These assumptions were used as a basis for evaluating equipment and determining costs. There still exist, as will be discussed later, some uncertainties as to the exact resolution required for matching and display; however, it is felt that these resolution numbers are close enough to be representative of an actual system requirement.

4. Display Equipment

Soft and hard copy devices for either research purposes or for a full-blown system present no special problems. High quality monitors can be purchased for from \$400 to \$1000 depending on size and quality. Also commercially available are hard copy devices with resolution of 100 lines per inch which can be purchased for about \$4300.

5. Data Communications Equipment

If terminals are used in remote locations as envisioned, then a communications channel is required to link the remote terminal to the central file and processing location. 9600-BAUD communications lines are available at about \$800 per month for a 400-mile line, e.g., Los Angeles to Sacramento. Shorter distances cost proportionately less money. Such a system is capable of transmitting over 100 high-resolution images (10 fingerprint cards) an hour or about 1500 (150 fingerprint cards) low resolution pictures per hour. If higher transmission rates are required then parallel lines can be used, or satellite communication is available at 50 kilobits per second for about \$10K per month. Slower communication lines (say 4800 BAUD) would probably be adequate for most remote terminals. Higher resolution imagery would take considerably longer to transmit and might require some dedicated microwave links which would add to the system cost but are certainly available.

6. Special Purpose Computer

A special purpose computer is needed to gain the speeds needed to perform the number of fingerprint matches anticipated. The proposed matching methodology has some similar aspects to that of fully analyzing the data from spacecraft images of the earth; Goodyear is currently studying the design of a special purpose computer for such applications using currently available high speed correlation chips produced by Rockwell and TRW. The application suggests a parallel architecture, and the Goodyear design incorporates 16,000 chips in parallel. [26] In our hypothetical system we considered 5000 chips in parallel. At a cost of about \$100 a chip, [66] the total cost of the special purpose computer is expected to be \$500K. Expectation is that this price may drop by an order of magnitude (see Appendix F). A speed of better than 10^{*9} operations per second has been claimed for this device.

SYSTEM CONFIGURATION

As mentioned previously, we need a method for digitizing the prints, a means for communicating them, a storage device, a processing scheme for doing the matching, and a display for verification of the match. The preliminary system design (a modification of Fig. 3.3--a generic representation of the system) shown in Fig. 4.1 is configured to perform all functions required of a fingerprint process. To summarize, the system consists of a number of remote terminals which feed via communication links to a master processing center. In the remote terminal there is a camera which is used to digitize, followed by an image digitizer which takes the fingerprints and converts them to a zero-one representation. We also have a microprocessor for displaying the print and possibly creating hard copies. The data from this remote terminal is fed to the master storage device to check the master fingerprint file to see if a match condition exists. Because of the number of bits of information required to describe the fingerprint, the master print file will require a mass storage device to store the large number of data bits required for a five-million card system. If we con-

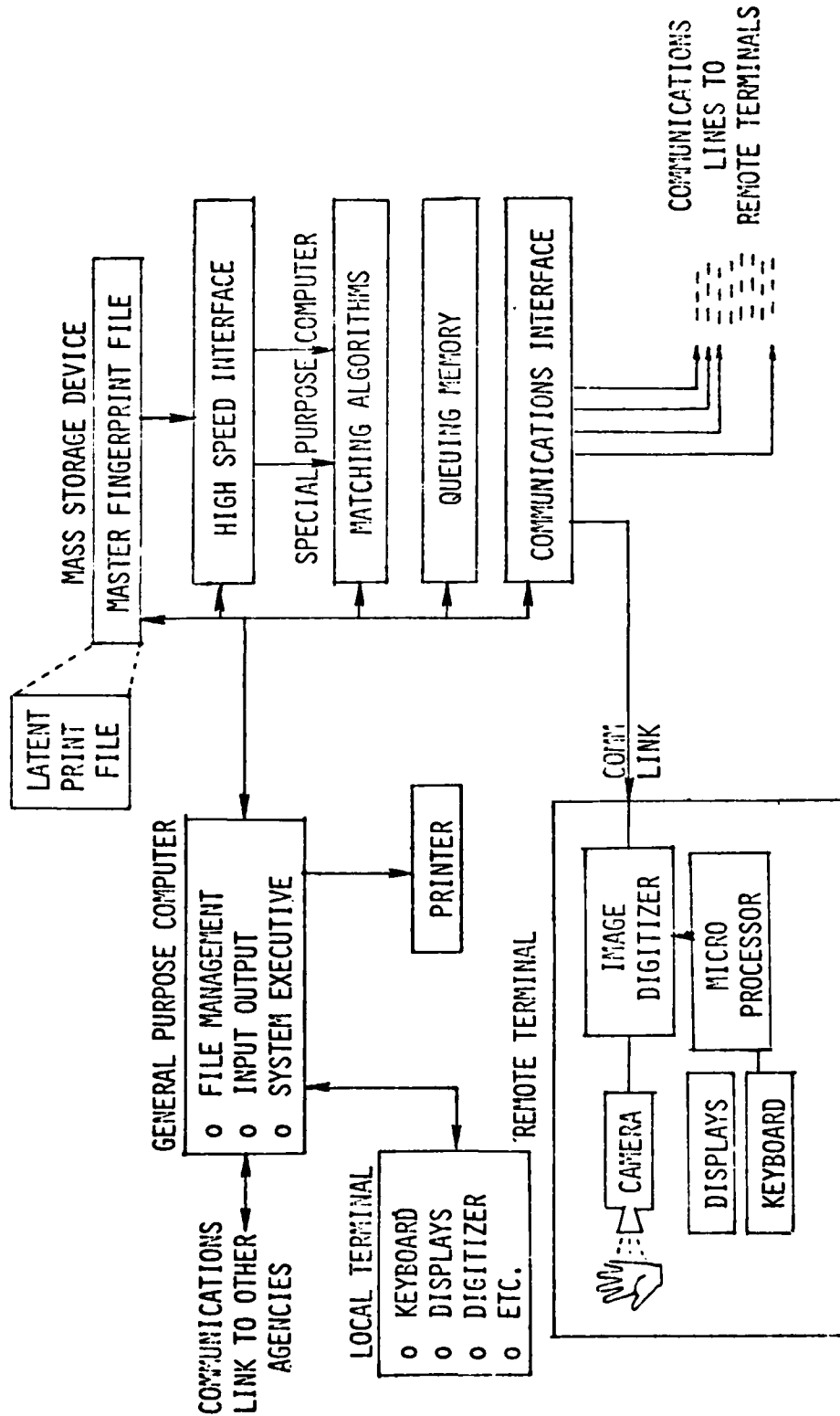


Fig. 4.1—Hardware System Preliminary Configuration

sider that each print requires 10^{*5} or 10^{*6} bits to describe it at the high resolution required for display, we are considering on the order of 10^{*12} to 10^{*14} bits of information required to store imagery of a five-million card file at a high resolution. We are fortunate, however, that new mass storage devices are available which have this capacity. The contemplated system includes a general purpose computer which accomplishes several missions. It provides assistance to manage the file, it provides input-output interfaces, and provides communications links to other law enforcement agencies. The actual matching takes place in a special purpose computer. This system, because it is designed to accommodate large print errors, would afford the capability of comparing a suspect print or latent print against the ID print file.

One could also consider capability in the system for storing latent prints for later searches. That is, if the latent print is not found in the file it can be stored and, as new latents arrive, they can be compared to existing latents in order to either (a) improve the quality of the latent image by finding other match latents, or (b) tie new latents to previous unsolved crimes. The approach for researching the file for old latents would be able to identify an additional 40 percent of the prints. [3]

INVESTMENT COST CONSIDERATIONS

We have examined the hardware feasibility and found that hardware is currently available to do the job of both ID and latent print processing. The next question is how much would it cost, and is the processing rate consistent with the demand established in Section II. Before discussing the cost projections it should be noted that there are several factors such as criminal mobility, budget considerations (to be discussed later), and economies of scale in the hardware costs which drive a fingerprint system to a large data base. The costs of (1) digitizing print cards, (2) storage devices, and (3) parallel processors are among the major nonlinear cost factors which drive the system toward large data

bases. For instance, the cost of digitizing one or two card runs is on the order of \$50/card, [27] while the cost for millions of cards is in the neighborhood of \$0.30/card. [18] Storage devices also exhibit an economies-of-scale phenomenon. Attempting to store 10^{*5} data bits (ten fingerprints on a single print card) in a microprocessor would require 100 10K ROM (read-only memory) devices at about \$100/memory, which translates to about \$10,000/card. Disc packs for general purpose computers cost on the order of a few hundred dollars and can store around 10^{*7} bits which is about ten print cards. With large mass storage devices, the cost of storing prints drops to about \$10/card. It should be noted that these devices start with storage capacities of 10^{*12} bits and there is a void between the mass storage devices and the general purpose computer storage of 10^{*7} to 10^{*8} bits. Similar economies of scale are expected to hold for the correlation chips where several thousand will be needed.

In Table 4.1 we have broken the investment cost into hardware and software development, and the cost of digitizing. For the file size we are talking about and the processing rates we have indicated earlier, we expect that the main computer with the appropriate components listed on the chart would cost on the order of \$5.9M (based on the discussions in the text). We are designing a system originally for 20 satellite facilities which would have the ability to digitize, copy, display, and transmit the data. At a cost of \$25K each, this leads to a total cost for the 20 facilities of \$0.5M. Thus, the total hardware cost is approximately \$6 to \$7M. We expect, based on previous studies, that the design development costs would be on the order of \$1 or \$2M. Included in the table are the costs of digitizing fingerprints. These costs reflect taking the entire card file, digitizing it, and storing the prints in the master print file before the system becomes operational. Our costs for digitizing these cards are based on the FBI costs [18] for doing large file sizes. If we were to consider bringing the system on gradually, we might reduce this cost considerably by digitizing these cards on an ongoing basis and thus reduce the

Table 4.1

INVESTMENT COST ESTIMATES FOR EITHER ID OR LATENT SYSTEMS

5 MILLION CARD SYSTEM		PROCESS RATES	8600 I.D./DAY or 860 LATENTS/DAY
0	HARDWARE		
	1 MAIN COMPUTER		\$5.9M
	-- MASS STORAGE	~\$5M	
	-- 5000 CORRELATION CHIPS	~\$500K	
	-- FILE MANAGEMENT	~\$100K	
	-- INTERFACES	~\$400K	
	20 SATELLITE FACILITIES		\$0.5M
	-- DIGITIZER	\$25K/EACH	
	-- HARD COPIER		
	-- DISPLAYS		
	-- COMMO EQUIPMENT		
	TOTAL HARDWARE		~\$6-7M
0	DESIGN AND SOFTWARE DEVELOPMENT		\$1-2M
0	COST OF DIGITIZING (\$0.30/CARD x 5 MILLION)		\$1.5M
			\$8-9.5M

Source: See text discussion, Section IV.

overall cost of the system. When considering the cost of present systems which are on the order of \$400K and can only handle file sizes on the order of 50K with very slow processing rates, the economies of the situation look attractive relative to these systems.

The investment cost presented herein is only one element of the total cost picture. There are also operating, maintenance, and transition costs (involved with running the manual system while phasing in the automated system) associated with the development of an automated system. We are fortunate that the State of California [2] has examined some aspects of the automation problem and provided data appropriate for estimating these (operating, maintenance, and transition) costs. These data will be used in conjunction with the investment cost data presented here to compare the costs and benefits of an automated system to the present manual system. This issue will be examined in Section V for the ID process and in Section VI for the latent process. In the remainder of this section the software capability of the proposed system will be examined to see if it meets the requirements described in Section II.

ANTICIPATED PERFORMANCE

The system must accommodate the processing requirements at a reliability level which is equal to or better than that which is being achieved by the present manual process. We will quantitatively assess the capability of our preliminary system design in terms of processing speed and qualitatively discuss the system reliability, drawing heavily on military experiences.

In Table 4.2 we have estimated the processing speed associated with an automated system which might be accomplished by today's hardware when working with a five-million card file (roughly the file size of the State of California). [16] The computations indicate that by using high-speed parallel processors (we have done the analysis required to determine the number of computations per match for the case of the prints which are distorted and rotated) it would require on the order of 100 seconds to match a single unknown latent print against all of the prints in the file. In the case of

- o PROCESSING SPEED

$$\frac{(10^7 \text{ BITS/MATCH})}{\text{REQUIRED COMPUTATIONS/PRINT MATCH}} \times \left(\frac{5000 \times 10^9 \text{ BITS/SEC}}{\text{PARALLEL PROCESSOR SPEED}} \right) \times (50 \times 10^6 \text{ MATCHES/LATENT}) = 100 \text{ SEC/LATENT} \rightarrow \text{LATENT SEARCH}$$

500 MILLION FILE PRINTS = 10 SEC $\rightarrow$ I.D. CHECK
- o DAILY CAPACITIES FOR 5 MILLION CARD FILE
 - 850 LATENT SEARCHES
 - 8600 I.D. CHECKS
- o HIGHER PROCESSING SPEEDS AVAILABLE
 - VIA PRINT CLASSIFICATIONS
 - HIGHER SPEED PROCESSORS
- o SEARCHES AVAILABLE
 - SUSPECT VERSUS I.D. FILE
 - LATENTS VERSUS I.D. FILE
 - LATENTS VERSUS LATENT FILE

Table 4.2—Estimated daily processing rates for latent and I.D. prints

ID searches, since we know the finger from which the print is taken, this time would be reduced by a factor of ten, thus requiring only 10 seconds to perform a search of an ID print to find an appropriate fingerprint in the file. A simple computation indicates that the system could perform either 8600 ID checks per day or 860 latent searches per day based on a 24-hour operation. There are methods for improving this speed. A conservative estimate was used for processing speed. There are currently higher speed processing techniques available and higher search rates are achievable by using them. The advantages resulting from possible use of classification have also been excluded from this computation of processing speed. Relying on print classification information might improve the speed by another factor of ten. However, this would inhibit the system design from having the capability to search an ID print or a latent print against every print in the file and would possibly introduce print classification errors into the process. The system design is such that it can perform suspect versus ID file searches, or latent versus ID file searches, as well as possess the potential for doing latent versus latents.

Table 4.3 compares estimates of the speed and reliability of present manual, semiautomated systems (past attempts to automate the process using only minutiae matching techniques), and our design for a totally automated system (indicated by future capability in the table). Manual systems, as indicated in the table, can handle the ID problem with adequate speed and reliability; however, because of manpower limitations discussed previously, they have no capability in performing latent print processing. Present semiautomated systems are not expected to do as well as the manual systems in terms of reliability for both the ID and latent print problems. [64,65] We do not have any good estimates on the ID processing data file. For the latent print problem results to date indicate not only difficulty in obtaining good reliability but also extremely slow processing, as indicated in the table. The totally automated design described in Fig. 4.1 does appear to meet the processing needs of a large state such as California by accommodating in

Table 4.3

SPEED AND RELIABILITY OF FINGERPRINT SYSTEMS

Criminal ID (5 Million Print Cards)

System	Time to Complete Search	Reliability
Manual	15 min	93%
Present Semiautomated	?	80-90%
Future Capability	10 sec	Better than current manual systems.

Latent Prints (5 Million Print Cards)

Manual	Years	90%
Present Semiautomated	Months	50%
Future Capability	100 sec	Better than current manual systems.

excess of the 6000 ID checks and almost meeting the roughly 1000 latent investigations required daily. We expect the reliability (based on military results--see Appendix E) to be on the order of 90 to 95 percent for the ID problem and better reliability than currently achievable via either the manual or semiautomated systems in performing the ID task.

Some technical uncertainties exist in achieving these processing speeds. The primary problem area lies in moving the data out of the mass storage device into the special purpose correlation computer. Presently access rates are limited to about 10^{*7} bits/sec--this is two orders of magnitude below the rate at which the processor can be driven. However, some hardware and system architecture solutions are available for alleviating the reading rate bottleneck. Increased throughput can be achieved by utilizing multiple reading stations or by queueing tape cartridges, with data being accessed at the maximum reading speed of approximately 1 million bytes per second. Parallel systems can be provided; however, this is fairly expensive. About \$60K is needed for each additional system to provide another 1 million bytes per second (approximately equal to 10^{*7} bits/sec) reading rate. Such a solution would require in the neighborhood of 100 additional stations which, even with some economies of scale, would add several million dollars to the acquisition cost of the hardware.

Another approach to the access rate bottleneck is to queue prints to be matched against the file. Thus, each time a digital image is brought from the master fingerprint file it would be matched against all the prints in the queue. Latent or other prints entering the queue would remain there until it has been matched against all 5 million cards on file. Other architectures may be possible to run the system at maximum speed.

Major points to be made here are that (1), based on military experience, high system reliability can be anticipated using image matching, and (2) current computer hardware, with some bootstrapping, can support a relatively high processing rate on a large master file data base of fingerprints. Since the system we are proposing will not be operational for a number of years to come, it is anticipated that additional software techniques will be developed to improve the

system reliability and to more efficiently accommodate the error sources. In the computer hardware area, historically, memory costs have been dropping rapidly, with memory speeds increasing. New technology on the horizon for mass storage are magnetic bubbles and optical technology. They are both expected to reduce cost and improve performance.

If we look at the technology forecast for the performance of new bubble and optical memories relative to storage capacities, access rates, and costs (see Appendix F), there appear to be advances which would significantly improve the capability of an image matching system. For a five-million person system data storage requirements for high resolution (512 x 512 pixels/print image) display would require in the neighborhood of 10^{13} bits. Bubble memories should afford a 10^{12} bits/ m^3 capacity while optical storage devices would be on the order of 10^{14} bits/ m^3 . With this latter storage density it would be possible to store the prints of almost everyone in the United States within a cubic-meter device. Access rates of magnetic bubbles are not likely to improve over existing memory access rates; however, optical systems may, in the future, support access rates up to 10^{10} bits/sec, which would eliminate the bottleneck problem of reading into a special purpose processor which can be driven at rates from 10^9 to 10^{10} bits/sec. Storage costs are also likely to decline by several orders of magnitude (see also Appendix F).

This section has shown the technical feasibility of the automated system design presented in the previous section. The technical feasibility involved the availability of hardware, the capability of achieving the required processing rates, and the ability to obtain high reliability. The costs of an automated system capable of performing the ID and latent print processing have been estimated. These system cost estimates will be used to judge the cost effectiveness of developing an automated system relative to "status quo" manual processing methods. The following section will analyze the cost/benefits of automating the ID process followed by a section on the latent print process.

V. COST/BENEFIT ANALYSIS--ID PRINTS

In this section we shall develop a methodology for comparing the automated ID print system to the present manual process and shall assess the cost/benefits of each to determine if the development of an automated system is warranted.

METHODOLOGY

The basic approach (as has been done in the previous section) is to develop an automated system which has the same capacity (file size) and processing rate capability as the present ID system. Having generated equally capable systems one can then examine the stream of payments required to develop and operate each system over the anticipated lifetime of the automated system. Using this stream of payments one can compare the costs of the two systems in terms of present discounted value (PDV). [62] There are additional benefits accrued to automating the system which are difficult to (1) quantify, and (2) attribute a monetary value. In comparing the two systems we shall use a "scorecard" approach proposed by Goeller [63] for dealing with complex public works projects. In the "scorecard" approach we shall present the PDV costs associated with each system and assess in nonquantitative terms the additional benefits associated with automating the system. For the ID system these benefits are listed in Table 1.2 and described in detail in Section I.

The costs of operating and maintaining the present manual system were obtained from the State of California. The investment, maintenance, and transition costs (phasing in automated system while retaining manual system) will draw largely from data generated by the automated fingerprint project of the State of California. This project estimated these costs for an automated system using a minutiae-based design; however, the investment costs of the State system turned out to be very similar to those determined in Section IV for our design. We will also draw on

the State's implementation schedule which gradually phases in the automated system over a two-year period while retaining the manual system until the automated system is completely operational. The benefits enumerated for the automated system are above and beyond those currently being achieved by the current "status quo" in the criminal justice community.

The process of automation will be examined in two stages. In the first stage, automating only the state ID bureau will be compared to keeping the status quo. We will thus be comparing the automated system shown in Fig. 3.2 to the manual system shown in Fig. 3.1. In stage two an incremental comparison will be made between automating the local processing stations and retaining their present structure.

For purposes of analysis we shall assume a system lifetime of 15 years beginning in 1980 and ending in 1995. By this time period new technology in the communication, computer, and display areas will probably replace the technology developed for this generation of automated systems. We will compute the discounted value for discount rates of 5, 10, and 15 percent (held constant over the period) to determine if the decision to develop the automated system changes in assumptions regarding time preference. Estimates for costs and benefits are expressed in constant 1979 dollars.

ASSESSMENT--AUTOMATING THE CENTRAL PROCESSOR

We are fortunate that the California Department of Justice, Bureau of Identification, has completed a thorough study [2] of several alternative modifications to their identification system. The ongoing costs of operating the California manual system for an approximately 5-million print file are shown in Table 5.1. The State also costed out incorporating several different levels of automation into the system. Included was a fully automated system similar in function to the automated system described in Fig. 3.2. The proposed California system differs from our system in that it assumes a microfilm storage media as opposed to a digital mass storage device and assumes a minutiae-based matching processor.

Table 5.1
ONGOING COSTS OF CURRENT CALIFORNIA MANUAL SYSTEM IN 1979 DOLLARS,
SIX-MONTH INTERVALS

Six-Month Period Beginning	July 79	Jan 80	July 80	Jan 81	July 81	Jan 82	July 82	Jan 83	July 83
Current ^a FP System	2,137,152	2,137,152	2,137,152	2,137,152	2,137,152	2,137,152	2,137,152	2,137,152	2,137,152
Soundex (FP Name Searches)	133,716	133,716	133,716	133,716	133,716	133,716	133,716	133,716	133,716
TOTAL	2,270,868	2,270,868	2,270,868	2,270,868	2,270,868	2,270,868	2,270,868	2,270,868	2,270,868

Source: Ref. 2

^a Figures taken from FY 1978/79 budget based on annual receipts of 1,380,000 documents.

The State report also determined the staffing changes anticipated by automating the system--these are shown in Table 5.2. The operating, maintenance, and transition costs of automating the California system are shown in Table 5.3 and will be utilized as being representative of our proposed design. The California study priced out the equipment at \$6.4 million paid out over a five-year period. The California investment cost is similar to the \$6-7 million estimate shown in Table 4.1. The only cost not directly accounted for in the California design relative to our design would be the onetime cost of digitizing the file. If we assume that the system is gradually phased in over a five-year period and that automated fingerprint personnel can perform the conversion process, then the microfilm costs assumed by the California design should just about cover the cost of digitizing the file. Thus, Table 5.3, with a two-year implementation schedule, can also represent financially the automated system design described in Fig. 3.2 for solving the identification problem.

The present discounted value (PDV) of the system costs for operating the manual system over a 15-year period, and the costs of developing, procuring, and operating an equivalent automated system are shown in Table 5.4 (also included here are the transition costs). The manual system is shown for both the status quo case and for the case where a 5-percent growth is required to meet the the additional demands of a growing file size.

Also shown here is the PDV of an automated system where equipment costs are varied to see the effect of hardware cost uncertainty. As seen in the table, the PDV of the automated system is less than that of the manual system indicating (nominal cost) that the automated system is a preferable option to the manual system for all three discount rates. If the hardware procurement costs were to be twice that estimated in Table 4.1 then the manual system would be slightly preferable to the automated system for the higher discount rates of 10 and 15 percent if the benefits were equivalent (which they are not). In actual fact, this preference is probably negated by the fact that manpower costs are rising with time due to growing file size. This study assumed constant manpower costs. As the

Table 5.2
BUREAU OF IDENTIFICATION STAFFING
CHANGES SUMMARY

Program	Classification	FY 1978/79	Post Implementation
Fingerprint Program	Administration	9	6
	Supervision	22	9.3
	Technical	153	67.5
	Clerical	19	10
	Data Processing	0	9.5
Record Control Program	Administration	8	8
	Supervision	34	32
	Technical	0	0
	Clerical	217	197
Total		462	339.3

Source: Reference 2.

Table 5.3

CALIFORNIA COST ESTIMATES⁽²⁾ FOR ACQUIRING AND OPERATING A
FULLY AUTOMATED I.D. SYSTEM

SIX MONTH PERIOD BEGINNING	JUL 79	JAN 80	JUL 80	JAN 81	JUL 81	JAN 82	JUL 82	JAN 83	JUL 83
Current ¹	2,137,152	2,137,152	1,239,797	1,239,797					0
FP system									
Soundex (FP Name Searches)	133,716	133,716	66,858	66,858	0	0	0	0	0
Conversion	440,918*	240,918	224,820	224,820					
Equipment	640,000	720,000	1,068,700	1,068,700	1,068,700	1,068,700	428,700	348,700	0
Maintenance	96,000	228,000	344,610	344,610	344,610	344,610	344,610	344,610	344,610
Film	53,365	106,826	42,780	42,780	42,780	21,428	21,428	21,428	21,428
Personnel ²									
FP system									
Automated System			792,256	792,256	1,056,340	1,056,340	1,056,340	1,056,340	1,056,340
Quality Control			29,688	29,688	29,688	29,688	29,688	29,688	29,688
TOTAL	3,501,151	3,566,612	3,742,651	3,742,651	2,520,766	2,520,766	1,880,766	1,800,766	1,452,066

Annual savings beginning JUL 83 = (2,137,152 + 133,716 - 1,452,066)2 = 1,637,604

¹ Figures taken from FY 1978/79 budget based on annual receipts of 1,380,000 documents.

² Figures based on FY 1979/80 projected volume of \$1,460,000 documents.

Table 5.4

PRESENT DISCOUNTED COSTS FOR MANUAL AND AUTOMATED SYSTEMS^a
(1979 Dollars--15-yr Period)

System		Discount Rate (percent)		
		5	10	15
Manual	Status Quo	\$47.1M	\$34.5M	\$26.5M
	5 Percent Cost Growth	68.1	47.9	35.4
Automated ^b	\$6.4M Equipment Cost	40.9	31.8	25.8
	\$12.8M Equipment Cost	46.5	36.9	30.4
	\$12.8M Equipment Cost and 5 Percent Growth	56.6	43.7	34.8
	\$19.2M Equipment Cost and 5 Percent Growth	62.3	48.8	39.4

^aBoth systems have the same file size and processing rate capability.

^bIncludes development, procurement, and operating cost with an allowance for a transition period where both the manual and automated are being used.

manual system is more manpower-intensive than the automated system, it is most likely that any significant rise in the file size will shift the PDV of the manual system above that of the automated system even with twice the hardware cost.

Presuming a modest growth in the manpower costs of 5 percent per year due to file size growth results in a PDV for the manual system of 47.9 million. This cost increase can be viewed as a reasonably conservative assumption when considering that manpower costs have risen as much as 20 percent in one year (1975-1976) [2] in the State of California Bureau of Identification. As indicated in Table 5.4, with comparable manpower cost increases in the automated system, the equipment cost would have to rise to almost \$18 million before the automated systems become unattractive relative to the present manual system at the higher discount rate.

Having estimated the PDV of the cost of both the manual and automated systems, it is now possible to assess the relative merits of each by a comparison in the "scoreboard" format. Table 5.5 summarizes the costs and benefits of these two systems in scoreboard format. To simplify comparison purposes we have presented the PDV for the 10-percent discount rate case and the nominal manual and automated system cases (manual status quo and \$6.4 million automated system cost) presented in Table 5.4. The benefits listed here are taken from Table 1.2. The table indicates, as expected, no change in the benefits (rapid ID, want-and-warrant suspects retained, crime rate changes, and changes in police investigation time) associated with rapid identification of suspects via electronic links from local to state agencies. The automated system is expected to reduce personnel at the state identification bureau by 100 to 200 individuals (see Table 5.2), and is also expected to provide slightly better reliability than can be obtained from the manual process. The two major advantages of the automated system are (1) increased manpower efficiency through the use of computer-aided graphics, and (2) future growth potential. This future growth potential is attributed to favorable technology projections in the areas of computer storage, memory, and cost, and in the ability to utilize the same system to perform latent print processing.

Table 5.5

SCORECARD COMPARISON SUMMARY FOR CENTRAL ID PROCESS

MANUAL VS. AUTOMATED SYSTEM *

COSTS & BENEFITS	SYSTEMS	MANUAL SYSTEM	AUTOMATED CENTRAL PROCESSOR
Cost Comparison ** PDV ***		\$34.5M	\$31.8M
Benefits -Positive Rapid ID -Went & Warrant suspects retained -Crime rate -Police investigation time -System complexity & redundancy -Manpower staffing -System reliability -Manpower efficiency -Future growth potential		status quo status quo status quo status quo status quo status quo 93% status quo none	status quo status quo status quo status quo status quo 100,200 less required at state level 93% Better at state processor through the use of computer added graphics Can take advantage of favorable technology projections for computer storage, memories, and cost Can also be used for latent print processing

* Both systems have the same file size and processing rate capability.

** For nominal \$6.4M computer equipment acquisition cost.

*** In 1979 dollars, assumes 10% discount rate over a 15-year period beginning in 1980.

ASSESSMENT--AUTOMATING LOCAL BOOKING STATIONS

Thus far we have not considered the statewide system in which the police departments would possess satellite facilities which would input the fingerprint imagery from the local station to the main computer electronically, as described in Fig. 3.3. The value of this distributed network system can be considered as an incremental add-on to an automated system operating at the state level. Thus, we can evaluate separately the PDV of the distributed system by comparing the cost and benefits of automating the process at the local level (digital equipment to convert image plus communication network to feed central processor) to the cost associated with the manual system.

Because of the difficulty in obtaining data on costs of all level fingerprint ID stations we shall not compare the costs of automated systems to all phases of the manual process but shall compare the costs (investment, operating, and maintenance) of automating the local system to the cost savings associated with the phase of the manual operation that the automated system replaces.

Let us then attempt to quantify the costs and benefits of the local fingerprint process with and without a distributed network. There are approximately 6000 cards per day processed by the state identification Bureau. Of these, 62 percent or 3700 are criminal with the remainder being applicants. [2] We shall not concern ourselves with the cost or cost savings associated with the applicant cards. The applicants are charged a fee commensurate with the cost of the process and, if a new process is utilized, it will be assumed that the fee will be adjusted up or down in accordance with the cost. Since there are no statistics kept on the number of local personnel involved in print processing, we will have to estimate it based on survey data.

The fingerprinting operation at the local level involves three phases: (1) fingerprinting the suspect, (2) classification of the print, and (3) placing information on the card relative to the suspect's anthropometric properties and the nature of the crime for which he was arrested. The actual fingerprinting process takes about ten minutes to complete the required rolling of three separate sets of cards (one for the local arresting agency, one for the state, and

one for the federal government). In an automated set up, two-thirds of this work could be eliminated as the two additional cards for the state and FBI would not be required. Approximately 25 percent of the local agencies actually classify fingerprints and search their local files with approximately 15 minutes needed to perform this task (five minutes for classification and ten minutes for search). [9] These positions would be completely eliminated if an automated distributed system were developed. Finally, clerks must place information on the print card concerning the nature of the arrest and physical characteristics of the suspect. It is estimated that this task would take approximately ten minutes to complete. The savings would be two-thirds of this time since information on one card would be required in the automated system. Here it is estimated that an automated system (based on eliminating much of this redundancy) would free 100 to 200 individuals throughout the state to perform other tasks.

A survey (survey questionnaire is shown in Appendix G) of 24 police agencies was taken at the annual seminar of the California State Division of the International Association for Identification (held May 24-26, 1979 in Long Beach, California). Of these 24 California agencies, 11 agencies employed personnel for classification and technical search of the print against the local file. The anticipated personnel savings for automating the system down to the local level are described in Table 5.6. This table indicates that approximately 200 personnel would be saved by installing remote satellite facilities. This survey was more heavily weighted toward the larger police agencies; thus, while the survey covered only 26 of the 450 or so police agencies throughout the state, it is estimated that the agencies not surveyed would not have a significant number of personnel involved in positions which would be eliminated via automation. Thus, throughout the State of California, it is estimated that the personnel savings would be around 250 personnel. The personnel cost savings associated with automating this system would be 250 personnel at a average annual salary of around \$15K/yr. [10] There are also some communication savings (in terms of postage and mailing folders) which are estimated at \$0.40/card for a round trip (fingerprint cards mailed in, and rap

Table 5.6

ESTIMATED PERSONNEL SAVINGS INVOLVED IN AUTOMATING SYSTEM
DOWN TO LOCAL LEVEL

Police Agency	Data Source	Personnel Savings Via Automated Distributed System
Los Angeles Police ^a	Connie Speck	90
Los Angeles Sheriff ^a	June Price	20
Alameda County Sheriff	Clive Barnum	24
Fresno County Sheriff	Don Justice	20
Stanislaus County Sheriff	Frank Cross and Daniel Cross	7
Long Beach Police	Harold Wenger and Barbie Pominville	7
San Jose Police	Richard Reneau	4
Beverly Hills Police	Richard Clason	3
Yolo County Sheriff	Charles Murray	4
San Bernardino Police	Mike Massey	8
Riverside County Sheriff	David Pong	2
Richmond Police	Norman Bettencourt	1
Visalia Police	George Jewett	1

^aNot part of survey but interviewed individually.

sheets or no criminal history mailed back). For this 3700 per day volume, the annual cost savings (based on 200 work days/year) would be on the order of \$300K.

The additional costs of the automated distributed system would be primarily tied up in the hardware cost associated with the satellite facilities (estimated from the previous section to be \$25K/facility) and the cost of leasing the communication links from the facility to the central processor. The lease on a 9600-BAUD link from Los Angeles to Sacramento is \$800/month. Shorter distances cost proportionately less. Thus, for the State of California a cost of \$600/month* for a communication link lease is estimated. It may be possible to cut this cost by locating the central processor nearer the majority of users or by having feedlinks tie shorter links together, avoiding the necessity of running every link from the satellite facility to the central processor. However, for this analysis we shall assume no short cuts and fix the average price of a link at \$600/month. Such a 9600-BAUD system is capable of transmitting over 100 high resolution (10 fingerprint cards) per hour or about 1500 low resolution images (150 fingerprint cards) per hour which is quite adequate for our needs.

California contains 461 general police agencies housing about 50,000 officers. [7] There is a size distribution associated with these agencies and some of the larger agencies (such as LAPD) will require a number of satellite facilities. Some of the smaller agencies do not do their own booking, but place the burden on larger county agencies such as the county sheriff's department, and will not be entitled to a satellite facility. We have initially estimated that about 200 satellite facilities would be required to support the criminal ID process. This agrees with an estimate performed by the automated fingerprint project of the California

*This presumes a greater proportion of longer links since the majority of the population is in the southern part of the state.

Bureau of Identification. [16] We have, for the purposes of costing the system, assumed that they would be brought on-line at the rate of 40 per year. Associated with each would be an operating and maintenance cost (typically 10 percent of the equipment cost per year) and cost of leasing the communication link (\$600/facility per month). A transition cost equal to the cost of the satellite facility has also been included in the cost equation to account for the training of personnel to operate the facility. The link capacity would be 48,000 cards/day (10 prints/hr x 24 hr per day x 200 facilities), which is well in excess of the 7000-8000 peak loading of the system.

The cost of purchasing, operating, and maintaining these satellite facilities is shown in Table 5.7, along with the potential savings in manpower and material from implementing the system. The manpower cost savings are based on a 5-percent growth rate in the cost of labor starting in 1980. Using these cost figures and discount rates of 5, 10, and 15 percent, the PDV of the costs (acquisition and operating) associated with automating the system down to the local level was computed and compared (in Table 5.8) to the PDV cost savings associated with reduced personnel staffing requirements for a 15-year system in 1979 dollars. As indicated by these data, the automated distributed network looks to be a more cost effective method for moving the prints from the local police agency to the state for all discount rates. The PDV cost savings of the automated system do not include any monetary benefit of staff reduction in the mail room of the Bureau of Identification (which is a definite possibility), nor can they encompass any benefits associated with rapidly performing the ID task via eliminating the criminal from utilizing a false ID to hide a past identity (estimated to be as high as 5000 criminals annually). This system should also free officers at the local level to perform other duties. Thus, even without including these additional benefits, the automated network could support at the approximately 10-percent discount rate an additional 75 satellite facilities (making a total of 275 satellites) and still be equal in PDV cost to its manpower savings.

Table 5.7
COST COMPARISONS OF AUTOMATED VERSUS MANUAL PROCESSING AT LOCAL LEVEL
(1979 Dollars)

Cost Savings with Automated Distributed System (Millions of Dollars)															
Source/Year	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94
Direct Force Reduction (250 Persons @ 15K/yr)	0.75	1.58	2.48	3.47	4.50	4.78	5.02	5.28	5.54	5.82	6.10	6.41	6.73	7.07	7.42
Mail Savings	0.06	0.12	0.18	0.24	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30

Additional Costs of Adding Satellite Facilities															
Source/Year	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94
Facility Costs ^a	1.0	1.0	1.0	1.0	1.0	0	0	0	0	0	0	0	0	0	0
Operating and Maintenance Costs ^b	0.1	0.2	0.3	0.4	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
Communication Links ^c	0.288	0.576	0.864	1.152	1.44	1.44	1.44	1.44	1.44	1.44	1.44	1.44	1.44	1.44	1.44
Transition Costs ^d	1.0	1.0	1.0	1.0	1.0	0	0	0	0	0	0	0	0	0	0

^a Assumes putting in 40 satellite facilities per year (at 25K/facility) over a five-year period.

^b Assumes operating and maintenance costs at 10 percent of satellite facility purchase cost.

^c Assumes average link cost of \$600 month.

^d Assumes the transition costs including personnel training equal the facility costs.

Table 5.8

COMPARISON OF PDV SAVINGS AND COSTS OF AUTOMATED
DISTRIBUTED SYSTEM AT LOCAL LEVEL
(Computed using costs shown in Table 5.7)

System	Discount Rate (percent)		
	5	10	15
Manpower cost savings associated with automated local system	\$49.3	\$34.1	\$23.2
Incremental cost of automated distributed system	35.3	19.5	15.1

As discussed in the beginning of this section, it is difficult to quantitatively assess the benefits associated with automation. We will again use the "scoreboard" format to express the costs and quantitatively describe the benefits of manual versus automated processing. Table 5.9 presents a scoreboard comparison of the manual system (status quo), the system automated only at the central processor (see Fig. 3.2), and the totally automated system (see Fig. 3.3). The PDV listed in the table is for the 10-percent discount case using the nominal \$6.4M computer acquisition cost for both automated systems.

The PDV costs compare the total cost of automating the system down to the local level (consisting of the cost of the automatic central processors plus hardware and personnel required to operate the system) to the cost of automating only the central processor (cost comparison is made by adding to the central processor cost the additional manpower savings associated with automating the local police agencies), and the cost of maintaining the status quo (cost of manpower at central processor plus manpower savings associated with automating the process down to the local level). Not only is the totally automated system most favorable in cost comparison terms, it also possesses the benefits which accrue from rapid positive ID of criminal suspects. Included among these benefits are: turnaround

Table 5.9
SCORECARD COMPARISON SUMMARY FOR TOTAL ID SYSTEM

COSTS & BENEFITS	SYSTEM	MANUAL SYSTEM	AUTOMATED CENTRAL PROCESSOR ONLY	TOTALLY AUTOMATED SYSTEM
Cost Comparison* PDV**		\$68.6M	\$65.9M	\$51.3M
Benefits				
-Positive Rapid ID	status quo (weeks)	status quo (weeks)	status quo (weeks)	Rapid turnaround (hours)
-Wanted & Warrant suspects retained	status quo	status quo	status quo	Thousands additional retained per annum
-Crime rate	status quo	status quo	status quo	Less due to more wanted suspects in custody
-Police investigation time	status quo	status quo	status quo	Less time spent tracking down wanted & warrants
-System complexity & redundancy	status quo	status quo	status quo	Eliminates need for local print files & local ID bureaus
-Manpower staffing	status quo	status quo	100-200 less required at state level	100-200 less required at both state & local levels
-System reliability	93%	93%	93%	93%
-Manpower efficiency	status quo	status quo	Greater through the use of computer aided graphics	Greater through the use of computer aided graphics
-Future growth potential	none	none	Can take advantage of favorable technology projections for computer storage, memories and cost	Can take advantage of favorable technology projections for computer storage, memories and cost
			Can also be used for latent print processing	Can also be used for latent print processing

*for nominal \$6.4M computer equipment acquisition cost

**in 1979 dollars, assumes 10% discount rate over 15 year period beginning in 1980

Rand

times on the order of hours instead of weeks, up to 5000 additional want-and-warrant suspects retained over the present system, lower crime rate attributed to retaining wanted suspects in custody, less police investigation time spent in tracking down wanted suspects, and less system complexity and redundancy due to the elimination of the need for local files and ID bureaus.

While automation of only the state processing facility reduces manpower by up to 200 personnel, total system automation reduces manpower staffing by about an equal number at the local police levels. Both the automated central processor and totally automated systems have some common benefits over the manual system. Included among these are: slightly improved reliability, improved manpower efficiency (through the use of computer-aided graphics), and good future growth potential (measured in terms of favorable technology forecasts for computer capability and the ability to utilize these systems for performing latent print processing).

To summarize this section, it appears that (1) there are significant benefits which can be obtained from automating the ID process, and (2) the cost effectiveness (measured in terms of PDV) of these systems is also favorable relative to the present manual process. In the next section we shall compare in a similar manner the costs and benefits associated with automating the latent print process.

VI. COST/BENEFIT ANALYSIS--LATENT PRINTS

The generic automated system we have discussed in Section III is equally capable of processing ID and latent prints. Thus the development, procurement, and operating costs for the central ID system developed in the previous section can be applied directly to the latent print problem. This latent system will be examined and assessed in a cost/benefit framework.

METHODOLOGY

It is necessary to base the decision to develop an automated latent capability on the basis of estimated system costs relative to projected benefits. The cost estimates for such a system are based on the system design discussed previously but scaled appropriately to deal with only the criminal portion of the file to the exclusion of applicant file cards. System benefits that went beyond the present "status quo" in the criminal justice community were determined. These projected system benefits were enumerated in Section I and are listed below relative to the present status quo as:

1. Increase in felony arrests
2. Increased recovery of stolen property
3. Increase in the utility of latent prints lifted
4. Reduced crime rate
5. Reduced investigation time

The State of California has outlined these and has attempted to place some numerical values on them. For some of these benefits monetary values were estimated; for others it is difficult to quantitatively assign dollar values. Thus, for the purpose of this analysis we shall again develop a "scorecard" [63] of benefits (quantified in dollar figures where possible) and compare them in a PDV framework to the costs (development, procurement, and operating) associated with an automated processing system.

The fully automated system described in the previous section is estimated to have an operational capability of 860 latents against an entire ID file. The anticipated cost of this system is assumed to be identical to that of the ID system and, for the sake of comparison, we shall use those cost (development, procurement, and operational) figures as being representative of this system. The PDV cost of a system capable of searching the entire file of applicants and criminals for latents is between \$31.8M and \$48.8M* (assuming a nominal 10-percent discount rate) (see Table 5.4). If we consider a latent system operating only on the criminal portion of the file (68 percent) and that the costs are likely to scale proportionately** to file size, then the PDV of this system would be between \$21.6M and \$29.3M at a 10-percent discount rate in 1979 dollars. Similar computations were done for the other discount rates with the results being presented in Table 6.1. Again, we are computing the PDV (based on 1979 dollars) over a 15-year life cycle for the system. The remainder of this section describes the quantitative assessment of monetary values for those benefits listed in Table 6.1.

SYSTEM BENEFITS

It is difficult to numerically quantify the value and cost savings of an automated latent system since there is no precedent to go by as to the potential impact on the criminal justice community. Again, the best that can be done is to estimate the system benefits in monetary terms (where possible) and describe in "scoreboard" fashion the benefits which are not directly quantifiable.

*Depending on variability in equipment cost and manpower growth.

**Most of the procurement costs can be attributed to the computer mass storage device whose purchase costs should scale proportionately.

Table 6.1

SCORECARD OF COSTS AND BENEFITS OF LATENT PRINT SYSTEMS

(1979 DOLLARS - 15 YEAR PERIOD OF SYSTEM OPERATION)

	PDV		
	5 Percent Discount Rate	10 Percent Discount Rate	15 Percent Discount Rate
System PDV Costs*	\$27.8-42.4M	\$21.6-29.3M	\$17.5-26.8M
Benefits**			
1. Increased arrests			
a. 23,000 additional burglaries			
b. 2,000 additional felonies			
2. Stolen property recovered, \$4.6M	\$15.91M	\$11.96M	\$8.95M
3. Increased utility of latents-- close to 100 percent utility			
4. Reduction in crime			
a. 37,000 burglaries/annum	\$37.36M	\$28.10M	\$21.02M
b. Property value saved--\$10.8M	\$35.63M	\$26.80M	\$20.05M
5. Reduced investigative time--\$10.2M	\$88.90M	\$66.86M	\$50.02M
Total			

SOURCE: Text, Chapter 6.

*Includes development, procurement, and operating costs over an estimated 15 year lifetime for the system.

**Relative to present system.

1. Increased Felony Arrests

The major impact would be (presuming, of course, that all suspects identified via a latent system could eventually be apprehended)* an additional 23,000 burglary suspects and 2000 other felony suspects arrested.

2. Increased Recovery of Stolen Property

As pointed out previously, the rapid identification of burglary suspects is likely to locate stolen goods before they can be fenced. The State of California has estimated a small data-base system** could recover \$2.72M/yr in stolen property. [1] We have estimated*** a larger data-base system could (based on the projected number of additional burglary suspects apprehended) recover \$4.6M/yr.

3. Increased Utility of Latents

Latents, as pointed out previously, are used as the basis of suspect identification in only about 20 percent of the crime scenes investigated. An automated system would probably increase the print utility to nearly a 100-percent level as well as afford the opportunity to tie the suspect to a number of crimes and solidify the prosecutor's case.

4. Reduction in Crime Rate

An ideal latent system could potentially, by identifying and facilitating imprisonment of burglars, remove 37,000 additional burglaries from the books per year in a large state such as California. Assuming an average property loss of \$292, [6] this could mean a potential annual savings to consumers of \$10.8M.

*This depends to a large extent on whether a rapid ID system with electronic data links is developed. If so, it is probably true that a good portion of these criminals will be apprehended; otherwise, the issue is probably in doubt.

**The State has estimated that their system could apprehend 13,600 additional burglary suspects while an ideal system could apprehend 23,000 additional suspects. We have scaled our property recovery benefits proportional to the number of suspects apprehended.

***A master print file of only 340,000 individuals as opposed to several million.

5. Reduced Investigation Time

The State of California has estimated that even a small latent system would reduce police investigation time by 2.04 million hours and result in a dollar savings of \$20.4M per year. [1] Since implementation of a latent system will not likely result in lower police staffing levels, we have arbitrarily valued the benefit at 50 percent of the original estimate.

Table 6.1 summarizes the system costs and benefits. The PDV of system costs and benefits (for those that are quantifiable) are presented here for discount rates of 5, 10, and 15 percent. As estimated the system benefits look favorable relative to system costs. The costs could be considerably less if a latent system were to be developed as an offspring of the automated ID system. Investment cost estimates were given for the ID and latent systems in Table 4.1. As indicated in this table, if joint system development were undertaken then the onetime development costs (\$1-2M) and the digitizing costs (\$1.5M) could be avoided in bringing a latent system on line. In terms of the Present Discounted Costs presented in Table 6.1, this would probably reduce these cost figures on the order of an additional 20 to 30 percent. However, since the discounted values of benefits already exceed the anticipated discount costs by a factor of 2 to 3 (depending on variability in equipment cost and discount rate) further cost reductions should not have a significant impact on the decision to develop a latent system but should encourage the development of a system capable of performing both the ID and latent tasks.

Having developed a system that can meet the needs of an automated ID or latent print processor, and shown it to be cost-effective, it is necessary to examine the problems associated with the system and its implementation. That is the subject of the next section of this report.

VII. INTERNAL AND EXTERNAL CONSIDERATIONS FOR
THE PRINT PROCESSING PROBLEM

In this section we shall examine some changes within the criminal justice community which would aid the fingerprint processing problem. Also issues and considerations which would have a significant impact on the development of an automated fingerprint processing system will be discussed.

INTERNAL ORGANIZATIONAL SOLUTIONS

The following procedures would have a favorable impact on the fingerprint processing problem:

1. Separating applicant from criminal files.
2. Establishment of procedures and priorities for purging the files and processing prints.
3. A merger or reorganization of the local and state identification and latent print bureaus into a regional or statewide network.
4. Holding criminal suspects until ID checks are made.
5. Restrictions on ID.

1. Currently applicant files constitute a little more than 50 percent of the master files at all levels. The time urgency for ID checking is a function of both the file type and the card type as indicated in Table 7.1.

The priority of checking on applicant cards (e.g., a new city employee) against the applicant file (to see if he is listed under some fictitious name) or the criminal file (to see if he has a previous record or is wanted for a crime) is probably quite low since it is unlikely that an individual with a warrant outstanding is likely to register. The harm done by identifying an employee applicant who has

Table 7.1

TIME URGENCY IN ID CHECKING

Card/File	Applicant	Criminal
Applicant	Low	Low
Criminal	Moderate	High

a previous criminal record is not nearly as important as identifying a criminal in custody, and thus a few weeks turnaround time is probably acceptable in most cases. Even in cases where there is an urgency to perform the ID check for applicants (e.g., city treasurer, prison warden) there is generally sufficient lead time to perform the task. The time urgency of the criminal ID check against the applicant file is probably of moderate time urgency. This latter situation would reflect a first-time arrest situation and would indicate that the individual is not a career offender (or, if he were, that he was awfully good at it) and would result in moving the individual's card from the applicant to the criminal file.

The impact of separating the criminal from applicant files would not change the workload requirements but could be useful in prioritizing which prints get checked first and reducing the time it takes to process a criminal print through only the criminal portion of the file. The criminal print could also be checked later (if no hit were made in the criminal portion of the file) against the applicant file. Thus, it appears that a file separation on the basis of applicant versus criminal category could expedite, via a priority system and file reorganization, the criminal ID process. The same types of priorities should hold for the latent print problem.

2. There are a vast number of prints in the master print file whose owners are neither active in the criminal arena nor involved in applicant employment. Essentially, fingerprint cards are kept

forever with the exception of possibly the deceased being eventually removed from the file. Some agencies are purging their files by removing individuals with certain characteristics (e.g., the FBI is throwing out, in the upgrading of their file system, the fingerprint cards of those over age 55 under the assumption that they will probably no longer remain active in crime). [18] These purges are generally one-shot actions and do not happen on a recurring basis. Criminal justice studies [3,61] have shown that criminal activity declines after the age of thirty. Based on these data, it may appear that in order to expedite the identification process the file may be broken down by age (possibly with several age categories or just two--those over 40 and those under) with the younger age categories being checked first and the older categories later. Age may thus form a basis for purging the files or form a basis for file organization and priority with which each part of the file is checked for both ID and latent print processing. There may be other bases, such as sex and locale (see Table 7.2), for organizing and purging the system which may be useful in solving these print processing problems.

All of the above discussion leads to the concept of a structured file in which there is an active portion of the file which is searched with high priority. If a hit is not made on the active criminal portion of the structured file, then searches at lower priority are made on the other portions of the file. Additionally, priorities may be set on latent prints on the basis of crime type and quality of the image.

3. In the fingerprint identification process there are numerous duplications of effort in checking files. For instance, the State of California has approximately six million file prints, and the LAPD has approximately three million file prints, which are also contained within the California State file. When a suspect is arrested by the LAPD or the Los Angeles Sheriff's Department (these organizations maintain separate files but have more or less the same prints contained within), the local file is first searched before it is forwarded to the California Department of Justice for further

Table 7.2

IDENTIFICATION RATE (PERCENT) VERSUS LOCALE

	In Locale	Out of Locale
Initial Search Identifications	44	16
Research Identification	29	11
	73	+ 27 = 100

checking if it is not found locally. The state personnel repeat the search of their larger file, which includes LAPD and the Los Angeles Sheriff's Department as a subset. Three solutions appear to make the system more efficient. The first is to completely automate the system with a rapid enough turnaround time that the local agency is no longer required to keep its own file. The second solution, involving the larger agencies, would structure the file at the state level such that an ID search at the state agency would exclude searching the portion of the file containing the larger local file. For states with large metropolitan areas processing times could be cut almost in half by avoiding redundant searches. The third solution could be used in conjunction with either one or both of the solutions shown above. This solution involves placing all the ID personnel in the state under state auspices. Because of the system redundancy it appears that both personnel could be eliminated and total file storage reduced by folding the local ID (and possibly the records division) into a state or regional organization. There is already pressure on local governments, by the momentum caused by "Proposition 13", to cut back city manpower and costs. Fingerprint file maintenance and checking at the local level is an area where even the police departments themselves would not be adverse to

giving the task totally to the state if they could be assured of a reasonable turnaround time on a request.

4. There are holding periods in which a suspect can be detained before booking for up to 48 hours (depending on the nature of the criminal charge) and 72 hours on the weekend. Once a suspect is booked he becomes eligible for bail. One possibility is to increase that detention time to the point that an ID check, at least at the state level, can be assured. This solution is only feasible if new technology available to move the prints electronically from the booking station to a central ID processor is employed. For an automated system it is estimated that this ID check can be made within a few hours of booking. The impact would then be to prevent the posting of bail until the ID process is completed. Currently, police agencies without evidence to the contrary utilize drivers licenses and social security cards as proof of identity and there is generally no requirement of even completing a search of the local files before bail can be posted by a suspect and he is gone from the system. Requiring an ID search completion (which would also perform a want-and-warrant check) before bail release would be an important aspect to making an automated system work effectively. For any system in which there is no electronic communication of the print from the booking station to the central processor, it will generally not be feasible to hold the suspect for the time it takes (several days to weeks) to complete the state ID check.

5. The major means of false identification by criminals are drivers licenses and social security cards. One way of limiting the need and urgency for true ID is to shore up the loopholes in obtaining these false IDs. However, in order to shore up these false ID routes, it would ultimately require another positive ID means such as fingerprints or voice prints. It is not likely, with privacy issues being a hot topic with civil liberty lobbies, that a positive identification system can be developed to limit the number and availability of false IDs.

It should be noted that none of the political solutions (with the possible exception of a means for reducing the vulnerability of law enforcement agencies to the false ID) are total solutions in themselves. They all still require at a minimum that an efficient electronic communication and display system be developed to reduce the time it takes to get the prints from the booking station to the central processor. Once an element of the system requires a conversion of the image to a digital representation it seems, from an efficiency point of view, that the whole process should remain in the digital mode because it reduces manpower and equipment requirements, and ultimately reduces cost.

In the remainder of this section we shall examine some of the organizational (external), social, and other considerations in getting a system operational. In the next section, we shall enumerate the uncertainties involved, and describe the research required to clear up these uncertainties.

OTHER SYSTEM CONSIDERATIONS

We shall briefly examine some of the following classes of issues and considerations which would have a significant impact on the development of any automated fingerprint processing system:

1. Organizational
2. Social
3. System countermeasures
4. Externalities
5. Perturbations to other parts of the criminal justice community

1. Organizational Considerations

There are two different organizational aspects to be considered--those related to the development of a system and those related to the employment of a system. In the development area a gap exists in the organizational setups that make it difficult for applied research to be undertaken. Presently only two organizations examine the automation of the fingerprint processing. Included here are the FBI and a group of hardware producing com-

panies such as Rockwell, Fingermatrix, and Nippon Electric. The FBI is also hardware-oriented with an interest in developing an automated system to handle its massive task of processing 24,000 IDs through a 90-million print file system which is growing significantly every day. [28] There are two major problems with getting research started in this area. First, funding at the national level is controlled politically, primarily by the FBI which is interested only in purchasing hardware to solve its pressing needs for a system. Second, in performing any research task, whether it be matching, display, classification, or whatever, one requires a common data base of fingerprints (preferably in digital format) which is large enough to provide significant statistics. Relative to the first issue, the major source of potential funding is the Law Enforcement Assistance Agency (LEAA); however, they do not have the technical personnel required to supervise major technical projects such as automated fingerprint processing so they must rely on the FBI for advice. Since the FBI has its own system to develop, it is not generally interested in supporting applied research but only development. State criminal justice agencies generally do not have the funding nor the expertise required to support and monitor technical research in this area. Again, states are more interested in purchasing hardware to do the job and eliminate some of their manpower requirements. This is where hardware contractors with a potentially profitable market come into play. However, it does not appear that hardware contractors have performed a sufficient amount of research (especially in the latent area) to see that the system will work under the real-world environment. Thus there appears to be a void between the specifications of hardware manufacturers of automated systems and the needs and requirements of state and local organizations for a working system. It is unlikely that hardware manufacturers are likely to invest their own funds into understanding the gaps and uncertainties in automated processing (to be discussed in the next section). Thus significant public funds will probably be required before a truly working system can be developed. Whether the research should be done by the hardware manufacturers is also a subject for debate.

On the plus side, such funding might speed up the time at which a good system becomes available. On the other side, giving the research to a nonhardware affiliated group should result in a more objective look at the problem and eventually lead to a better system.

The other research barrier appears to be the lack of a common data file of prints. It would be very desirable to develop such a data file which contained (1) a representative master print file, and (2) a test set of latents and ID prints by which comparisons could be made. Such a file, if established, would provide not only a basis of judging the performance level of any system but would also open the field to more research, since presently every researcher in the field must develop his own fingerprint data base. This is a very costly process requiring specialized hardware to digitize the images. This is especially true of the classification problem when one requires 10 to 20 prints per category for statistical significance with upwards of 1000 categories. Presently the USC Image Processing Institute would charge approximately \$500 to photographically enlarge and digitize a single print; thus the cost of development can be expensive. Thus, a national data base would eliminate this cost, open up the area to more research, and provide a basis of commonality between research programs in this area.

A major uncertainty in the employment of an automated system is the organizational changes likely to occur within the ID and latent print processing divisions of law enforcement agencies. In both the short and long term, the development of an automated fingerprint processing system should reduce manpower requirements significantly. In the short term some of the large metropolitan police forces will probably purchase automated equipment with a resulting saving in manpower. However, in the long run more regional or statewide centers for ID and latent print processing are likely to develop so that much of the redundant searching efforts between local and state (and possibly even federal) agencies will be eliminated with a resulting further cut in manpower and possibly a change in organization, i.e., with the local processing units being absorbed into the regional or statewide system. Organizational impediments to an automated ID system at the local or

state level are not very strong. Practically all manpower utilized in performing this operation, with the exception of the supervisory personnel, are not generally police personnel and are considered more expendable than line officers. Additionally, with budget pressures resulting from Proposition 13, supervisory personnel are looking for ways of cutting cost. Automation appears an attractive answer for solving the budget "crunch" and having fewer personnel headaches. For instance, machines don't leave and create vacancies which require training of new personnel (at a considerable cost). However, since investment dollars are scarce the automated system must be weighed (in terms of PDV) against the alternative of maintaining the status quo.

In the latent print area, since most of the force is involved in crime scene investigation work as opposed to print processing, it is unlikely that any manpower reductions will occur. It is more likely that, if an automated latent print processing system is developed that will work fairly well, additional personnel will be required to process the prints that are recovered by field investigators. Presently, many of the larger police agencies do not send print technicians out to cover minor felonies such as burglary where no violence has occurred. If such an automated latent print system were to be developed and prove to be effective, it is likely that in these larger police departments the field staff will increase significantly.

2. Social Issues

Two social issues of concern are privacy and treatment of juveniles. Privacy is a major national issue with citizenry being concerned with a "big brother" environment. The concern with privacy is unauthorized divulgence of a criminal record on an individual. [58,59] Law enforcement agencies have taken steps to guard against the unauthorized release, primarily by controlling access to master print file areas. Reference 60 provides a good overview of the various techniques for access control. It is anticipated that the privacy requirements can be met for an automated system by

controlling physical and electronic access to the central processor, with physical access limited to authorized personnel, and electronic access requiring code entry.

Another major issue is how to handle juveniles in the system. Presently, it is estimated that juveniles in California account for more than 30 percent of the felony crimes. [1] The juvenile files and fingerprints are restricted by law to remain in a separate folder. Thus the juvenile fingerprint cards are not ordinarily entered into the master file system. This limits the ID process to the local level only, where the police agency can only perform name searches. The only way of performing latent print processing with juvenile prints is to make a separate run of the juvenile print against the "unresolved latent print file" to determine if there is a match. As new latents enter, the juvenile would be excluded from being processed by the system. Therefore, in order to make an effective print processing system (when considering the relatively high percentage of crimes committed by juveniles) it would make sense to change the procedures for handling juvenile prints, possibly by including them in the file under a code name so that they may be processed without readily revealing their identity.

3. System Countermeasures

One of the basic questions concerning the latent print system is the ability of the criminal to defeat the system by wearing gloves. The question can best be answered by breaking down crime into two categories--opportunity and planned crime. It is unlikely that those involved in opportunity or spur-of-the-moment crime will take the time to be cautious and put on gloves or wipe their prints off contact surfaces. On the other hand, planned crime activities are unlikely to result in any latent prints. A Rand study [12] of inmates indicates that two-thirds of criminal activity (at least those who get caught and go to prison, so we may be examining a biased population) fits into the opportunity crime category. Thus it appears that countermeasures may degrade the success of a latent print system but not to the point where the system becomes ineffective.

4. Externalities

It is clear that an efficient automated print matching system would have application for fraud prevention both in the public and private sectors. There are three conceivable types of matching requirements, the most difficult being equivalent to the latent print problem of matching an unknown print of poor quality against a file. This type of matching process might be useful for applications such as return of stolen property (suggested by the state of California). [30] The majority of individuals who suffer property loss do not record the serial number of the merchandise nor do they have a sufficient description of the merchandise to identify it as uniquely belonging to them. One way of identifying recovered stolen property would be to lift latent prints from it and compare these prints to those individuals who have reported similar property stolen.

The second type of print processing would involve comparing a set of prints against the file similar to the ID problem. Application here would involve primarily (1) fraud prevention such as welfare cheating (cross checking to insure that the applicant is not in the master file under more than one name), and (2) identity verification. In this latter case, one could consider (putting aside privacy issues) such applications as using fingerprints for passports, drivers licenses, and social security cards. Making it more difficult for individuals to obtain false ID would have a preventive effect on such crimes as forgery. It would also reduce the percentage of criminals who use false IDs when arrested to escape want-and-warrants (by posting bail before an ID check is completed).

The third and simplest type of print processing would involve comparing the print to a single other print to determine if the two prints were one and the same. In this application the individual's print would be taken along with some other identifier (e.g., bank, social security, or drivers license number). This identifier would then be used to call the print in the file against which to make the comparison. This type of system could be utilized in security entry, check cashing, and other similar applications.

5. Perturbations to Other Parts of the Criminal Justice System

If a latent print system is developed there may be a significant impact on the rest of the criminal justice system--the DA, the courts, and the prison system. An effective latent print system may increase the potential number of solved crimes via fingerprints alone from 3 to 20-30 percent. Such a potential increase in the crime solution rate may prove a significant transitory load factor on the rest of the criminal justice system. The DA's office may be provided with a better case against the defendant with fingerprints proving a source of hard physical evidence. By the use of a latent print system, a suspect may be tied to several unsolved cases, thus making it more difficult for him to get off with probation or a light sentence. The system may also have a significant deterrent effect if the latent system can improve the crime solution problem, conviction rate, and stiffness of the sentencing.

VIII. UNCERTAINTIES

This report cannot answer all of the uncertainties concerning the development of an automated fingerprint processing system. However, we shall address the major uncertainties which are broken down into the following areas:

1. System utility
2. Theoretical modeling
3. Hardware availability
4. Image enhancement
5. Error and resolution requirements
6. Algorithm development and testing
7. Classification

1. System Utility

We have stated that the major benefits of an ID system would be to (1) provide a more cost-effective system than the manual system, and (2) (by providing communication links from local booking facilities to higher level systems) eliminate a criminal from escaping a want-and-warrant by utilizing a false ID. In the latent print area the utility involves the ability, for the first time, to actually process latent prints to solve crimes.

One of the unresolved questions involves the prevalence of criminals using false IDs in escaping a want-and-warrant. Estimates from law enforcement officials indicate that the percentages of criminals arrested who get away, or potentially can escape, without being held over for a want-and-warrant is on the order of a few percent. The system utility could be better estimated if police agencies were to keep statistics on these occurrences. Presently we could find no law enforcement agencies that kept such statistics. It would also be desirable to determine the frequency of occurrence that false IDs are issued at the national (passports and social security numbers), state (drivers license, etc.), and local levels as an indicator of the utility of tightening up the issuance of IDs.

2. Theoretical Modeling

It is very disturbing that virtually none of the literature on the fingerprint process deals with statistical modeling of the process. Practically all of the work in this area involves an ad hoc approach. Without a model of the process it is impossible to predict the performance of the system in terms of type I and type II statistical errors.*

In the feature matching realm, Osterburg has provided us with some data on the frequency of occurrence of minutiae in the print. The major problem in modeling feature matching systems is that while the effect on minutiae location of errors is known precisely many of the errors are not readily modeled in this realm. For instance, while the effects of noise can be modeled fairly well in terms of the intensity levels of the image, the effect on the minutiae (the creation of the false minutiae) is not easily modeled. Additionally, missing areas in the print may eliminate key minutiae which make it virtually impossible to model the process and predict performance.

Fortunately, in the image matching realm models exist for relating all of the errors (geometric, rotational, noise, missing areas, and contrast reversals) to a change in the performance of the system. The only remaining questions have to do with the statistical noise-free properties of the fingerprint itself. The fingerprint must be assumed to be homogeneous (i.e., that within any region the average intensity level is expected to remain constant, and that constant is not expected to change between regions). The major unknowns have to do with the number of independent elements in the image and the uniqueness of the pattern. Obviously, many of the image elements are correlated and, from a statistical point of view, it is necessary to determine the number of independent data elements in the image. Preliminary estimates indicate that there are approximately 1000 independent elements in a fingerprint image. Once the parameter has been determined on a larger sample, it is a

*Type I error refers to the true match from the candidate list, while type II errors refer to accepting false matches as true ones.

relatively simple task to predict performance for any level of error. The other parameter of interest to image matching or correlation systems is the uniqueness of the pattern. Two prints can indeed be fairly similar in pattern. This print similarity problem requires data and a model so that its effects on performance can be estimated. Juncosa [57] has made some progress toward this modeling task but more data are needed.

3. Hardware Availability

We have, in developing a preliminary design for an image matching system, determined the capability and availability of hardware that is required to perform the task. This hardware availability study was not exhaustive. The study should be expanded to include other pertinent hardware systems and should determine the impact of technology forecasts which could aid in the development of an automated system.

4. Image Enhancement

Image enhancement is important for both the matching process and the verification phase (via a display for use by the fingerprint expert). Image enhancement for matching is an area where a great deal of work has been performed, as witnessed by the publications list. [31-56] A major unanswered question (resolution requirements are to be discussed later) is how to display the print on a CRT so that a fingerprint technician can readily determine if it matches the print in question. Fingerprint technicians have an exhaustive task in verifying matches via fingerprint cards. The situation is exacerbated in the latent print area where a fingerprint technician may only be able to work an hour or two a day. The efficiency of a fingerprint technician may be significantly improved by providing displays. The type of data displayed and the ability to manipulate the display can be important elements of the overall fingerprint processing system. It has yet to be determined how the data should be displayed (e.g., minutiae and image comparisons) and the type of manipulation that should be performed (e.g., superposition of the two prints, rotation of the prints, etc.).

5. Error and Resolution Requirements

The print processing system must accommodate four major error sources. These are described in Appendix C. No published literature exists as to the statistical distribution of these errors. Thus to ensure proper system development it is necessary to determine the statistical error properties of latent and ID prints. In the ID area it is also necessary to determine the changes that occur in an individual's prints due to changes in the fingers over time, and due to the variation in rolling prints by different fingerprint technicians. In the latent print area the major statistical parameters to be determined are the rotational misalignment error (how well can a fingerprint technician or an automated machine program align the axis of the print relative to the axis of the stored ID print), the characteristics of print stretching, the relative size of the missing areas, and the amount of noise present.

Resolution is another question for which there has been no determination based on analysis. Resolutions used in the real world vary between 70 elements on a side (used in some classification techniques) to 750 elements (used by some of the minutiae matchers in extracting minutiae from print imagery). Obviously the resolution requirements will depend on the function being performed. A number of specific functions are of interest; included among these are: classification, minutiae extraction and matching, image matching, print error measurements, and display. It is estimated that the ball park resolution requirements for each of these functions would be:

- | | |
|-----------------------------------|--------------------------------------|
| (a) Classification | -- 70 pixels on a side |
| (b) Low resolution image matching | -- 100 pixels on a side |
| (c) Crude level minutiae matching | -- 100 pixels on a side |
| (c) Print error measurements | -- 500 pixels or higher
on a side |
| (c) Minutiae extraction | -- 500 pixels on a side |

- ```
(d) Display -- 500 pixels on a side
 (TV compatible)
(c) High resolution matching -- 500 pixels on a side
```

The above estimates are based on the following:

- (a) Fu and Moayers work.
- (b) Theorem and noting that there are roughly 40 to 50 ridges and valleys across a print in one direction.
- (c) Initial guess.
- (d) The eye having a resolution of one-third holding the print four inches away from the eye (the print being approximately one inch across), and assuming TV capability.

A research effort is required to quantify the exact resolution requirements of each of these functions.

## 6. Algorithm Development and Testing

The three properties that the algorithm should possess are the ability to accommodate errors, an ability to screen prints, and sufficient speed to meet the processing requirements. In order to be able to accommodate errors, especially rotation and stretching, it is necessary to know the distribution of the errors so that a subarea size can be chosen such that it is consistent with the expected amount of error. It will also be necessary to screen prints by establishing an absolute cutoff error. This part of the algorithm design will (1) eliminate portions of the print (latent print case) which are obviously too noisy to match, and (2) determine which prints have a reasonable chance of being matched. In order to obtain speed one would like to go to as low a print resolution as possible. It is likely that an efficient print matching system will start out with a low resolution matching stage (where coarse screening of prints occurs) and proceed to subsequently higher levels of resolution (with fewer and fewer candidate matches being carried from one stage to the next). The resolution requirements at each stage of the matching process are thus one of the parameters to be determined. To summarize, much of the algorithm development work will be dependent on the results of the error analysis and resolution requirements described earlier.

In order to test any new system it is necessary to utilize a data base against which to test the system. The size of the data base will determine confidence intervals about the point estimate of performance for the system. The standard deviation associated with this estimate of performance goes as the square root of the number of prints matched. Thus a few hundred test prints should provide an adequate basis for initially designing a system.

It is important in designing a test file (especially a latent print system) that fingerprint cards be selected for which there are (1) latent prints, (2) ID cards on the same individual taken over several years, and (3) cards on the same individual which have been rolled by fingerprint technicians with varying degrees of experience. It is also necessary when performing tests on the system to run (1) cases in which the print to be matched is in the file, and (2) cases in which the print is not in the file, in order to develop some measures of system performance relative to both type I and type II errors.

#### 7. Classification and File Structure

As pointed out previously, structuring the file by means of such characteristics as status (applicant or criminal), age, and other pertinent parameters can have a significant payoff in terms of speeding up the search time. Classification is another means of reducing the volume of prints to be searched. As pointed out in Appendix A, the Henry System (or a variant, the Galton System) commonly used in classifying ID prints manually, and the Batley system can be used under certain conditions for classifying a single latent print. Relative to classification, an automated system can have five options; these are:

1. Use no classification system
2. Retain the present manual classification system
3. Modify the present manual systems to have a more equal distribution of prints among categories
4. Develop a new classification system more suited to the needs of an automated processor
5. Development of a new classification system and the utilization of the present system

AD-A103 314

RAND CORP SANTA MONICA CA

F/G 5/11

INCREASING EFFICIENCY IN THE CRIMINAL JUSTICE SYSTEM: THE USE O--ETC(U)

SEP 80 J A RATKOVIC

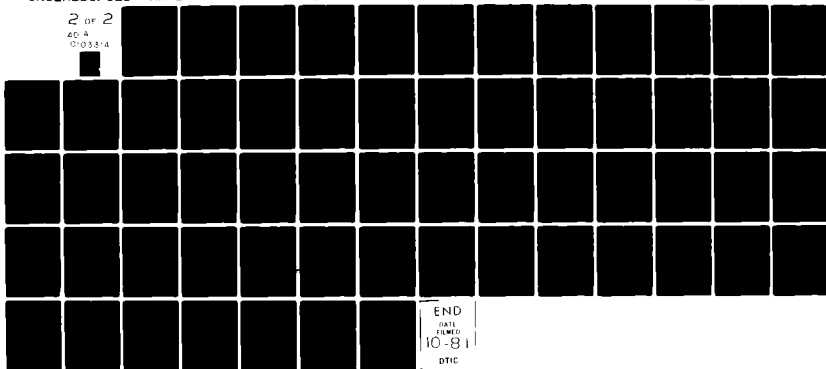
RAND/P-6546

NL

UNCLASSIFIED

2 OF 2

AD A  
O-03314



END  
DATE  
FILMED  
10-81  
DTIC

The employment of a high-speed processor and the use of other means of structuring the file (age, sex, locale, etc.) may negate to some extent the need for further structuring of the file by means of classification, especially when considering (1) the error rate (10 percent) in identifying cards is primarily due to classification, (2) the time involved in classification (five to ten minutes for a manual classification, and about a minute for automated classification), (3) the difficulty of defining a registration point (about which many of the new classification schemes hinge on), and (4) the likelihood that no classification scheme would be of any value in dealing with latent prints containing missing areas.

Retaining the present manual system in an automated system is likely just due to its established acceptance by fingerprint technicians, whereas development of a new system may meet with organizational resistance. The Henry System, as pointed out, does have the potential for a large number of classes, but in actual fact the distribution among the classes is quite uneven, with eight percent of all people falling into the largest single subgrouping (ten ulnar loops). Additional discrimination is customarily obtained by counting the number of ridges between easily locatable special points in the pattern.

This unequal distribution of prints among categories suggests modification of the present system or the development of a new system. Shelman and Hodges [49] have suggested modifying the present system to obtain a better breakdown of the classes which are heavily populated. In the 1970s a number of new classification systems have been proposed. Tou and Hankley [47] have proposed a syntactic approach to classification based on the topological representation of the pattern. Moayer and Fu [39,42,45,48] suggest a syntactic method based on the relationship between the core and delta point in the print. Kameswara Rao and Balck [37,40,46] suggest a class based on a ridge flow of the fingerprint compressions. In any event the development of any new classification system, or the use of the present system or a modification thereof, will require testing on

a large data base in order to determine the utility of these techniques. This utility will depend on the time required to classify (either manually or automatically) the experimentally determined error rate and the number of categories\* in the classification scheme.

It may be possible to utilize several of these schemes in parallel in structuring an automated filing system if these classification schemes are orthogonal to each other (which is a good possibility). In this case the entire classification network of each classification scheme may be utilized or, in order to reduce the possibility of misclassification error, only the primary classes of each scheme could be used.

#### IMPACT OF UNCERTAINTIES

The two areas which could have the greatest impact on the system design, performance, and cost are the error and resolution requirements, and algorithm development and testing.

The system design for which the performance specifications were generated assumed a nominal error in print rotational alignment of 10 deg and a nominal scale factor of 10 percent. If the error distributions on these parameters exceed this nominal value, this will require smaller subarea submaps, thus raising the number of correlation chips required to obtain the same level of performance. Doubling the nominal error characteristics would probably raise the cost of the special purpose computer by 50 to 100 percent. Considering that the special purpose computer accounts for only about 10 percent of the total investment cost the net effect on cost should not be too severe.

---

\*Many of these classification systems promise on the order of thousands of categories. For statistical significance about ten prints per category will be required. Thus, a data base consisting of tens of thousands of prints will be required for testing.

For design purposes we have assumed that the vast majority of mismatches could be screened using low- to medium-level resolution, and in subsequent stages of the matching process higher resolution could be used on a small fraction of the data base to obtain candidate matches. If this sequential screening process did not filter out a large fraction of the file as candidates at the low- to medium-resolution then, in order to obtain the desired performance specifications, the number of parallel processors would have to be raised from 5000 to 25,000 in order to accommodate higher resolution requirements. This would raise special purpose computer costs by a factor of 5 and also (due to more system complexity) raise system development cost by one or two million. The net effect would be an overall rise in investment cost of around \$5 million (similar to the case shown in Table 5.4 where investment costs doubled). At this point the discounted costs of the automated and manual systems are almost equal.

Uncertainties in algorithm development and testing could complicate the software design in order to account for some anomalies in fingerprint imagery not foreseen. The net effect would be felt in the development costs, possibly raising them from 1 to 2 million to the 2-to-5-million range.

The worst case would be incurred if all the above parameters went out of control. In this situation the total investment cost would be on the order of three times the estimated value, making the manual ID system slightly preferable to the automated system when considering the development of an ID system alone. However, if a joint development program (ID and latent) were undertaken, the automated system would still look attractive compared to the "status quo".

Theoretical modeling and image enhancement considerations do not impact significantly in the system design other than possibly requiring a few software changes for accommodation. These issues could be considered neutral to the system design.

On the other hand, system utility, hardware availability, and classification could favorably affect the system design, performance, and cost. In the system utility arena there will be more uses found for such a system, if developed, than enumerated herein. For instance, such a system could aid government in fraud prevention (e.g., welfare cheating, medicare claims, etc.) and generate spinoffs in the private sector in such areas as check cashing aids and security entry systems.

Computer hardware costs have been steadily declining while performance, in terms of increased storage capability and processing rates, has been increasing. New technologies are on the horizon (e.g., optical and bubble memories) which could favorably impact the size, cost, and complexity of our system design.

Print classification has not been utilized in our system design. If the current Henry system were modified, or a new classification scheme were developed that proved reliable with a large number of print categories, it could reduce processing requirements by 100 to 10,000 with an enormous impact on system cost and complexity.

The remaining section of this report discusses the conclusions of this study.

## IX. CONCLUSIONS

1. As indicated by Table 5.9, automated ID systems appear to be a cost-effective means of processing prints relative to current manual methods. Their cost effectiveness can be increased even further by developing an automated system which encompasses not only the central processing bureau but also the local police agencies.

2. Automated latent print processing systems appear (based on the "scoreboard" calculations shown in Table 6.1) to have benefits (increased felony arrests, increased recovery of stolen property, increased latent print utility, reduced crime rate, and reduced investigation time) which outweigh the development, procurement, and operating costs associated with such a system. These costs can be lessened even further if a latent system is developed as an offspring of an advanced ID system. Image matching affords the opportunity for an ID system to be converted over to latent print use.

3. Since cost effectiveness alone should not be a sufficient condition for developing an automated system (i.e., there is limited utility in making a poor system less costly), it appears that automation with rapid communication links between criminal justice agencies is necessary to improve system performance. Rapid positive ID through the use of electronic links between agencies should (1) eliminate the possibility of wanted criminals escaping the system before they are correctly identified, (2) reduce the crime rate, (3) reduce police investigation time, and (4) decrease system complexity and redundancy.

4. The use of electronic fingerprint imagery (stored digitally) is the key to the development of a new generation of automated processing systems. Such imagery affords the capability to (1) rapidly communicate prints to speed the identification process, (2) develop new algorithms that improve the speed and reliability of the matching process for both ID and latent prints, and (3) rapidly and efficiently expedite the verification process via electronic displays and image processing algorithms to aid the fingerprint technicians.

5. Specialized hardware (in terms of mass storage memory devices, high-speed correlation chips, electronic displays, etc.) is currently available to develop the next generation automated ID and latent processing systems. Similar hardware and software configurations between the ID and latent print usage should cut the cost of developing a latent system presuming that the ID system is developed first.

6. Several uncertainty areas could impact the decision to develop an automated system. Specifically drastic unfavorable changes in the error and resolution requirements or algorithm development and testing areas could possibly change the preference from automated to manual ID processing unless a joint development program were considered. On the other side of the coin, uncertainties in system utility, hardware availability, and print classification are likely to favorably impact the development of an automated system.

7. Uncertainties require that research be undertaken (error and resolution requirements, print classification techniques, etc.) to resolve issues which affect system design. Finally, a nationwide demonstration program needs to be instituted (using a statistically representative data base) to test any new automated system for speed and reliability.

REFERENCES

1. Automated Latent Fingerprint Identification System, A Feasibility Study, Department of Justice, Bureau of Identification, State of California, September 1977.
2. Automated Fingerprint Identification System, A Feasibility Study, Department of Justice, Bureau of Identification, State of California, September 1977.
3. Greenwood, P. W., et al., The Rand Habitual Offender Project, A Summary of Research Findings to Date, The Rand Corporation, P-5957, March 1978.
4. Greenwood, P. W., et al., Prosecution of Adult Felony Defendants in Los Angeles County: A Policy Perspective, The Rand Corporation, R-1127-DOJ, March 1973.
5. Los Angeles Times, March 30, 1979, p. 3, col. 1.
6. Crime in the U.S., 1977, FBI Uniform Crime Reports, October 1978.
7. Sourcebook of Criminal Justice Statistics, 1977, U.S. Department of Justice, LEAA, National Criminal Justice Information and Statistics Service.
8. Criminal Justice Agencies in Region 9, October 1974, U.S. Department of Justice, LEAA, National Criminal Justice Information and Statistics Service.
9. Discussions on 5/8/79 with Bob Bronam, Records Manager, Orange County Police Department, and a local officer of the California Law Enforcement Association of Records Supervisors (CLEARS).
10. Discussions on 5/11/79 with Lt. Connie Speck, Assistant Supervisor for Records and Identification, Los Angeles Police Department.
11. Discussions on 5/5/79 with Mrs. June Price, Records and Identification Supervisor, Los Angeles County Sheriff's Department.
12. Petersilia, J., P. W. Greenwood, and M. Lavin, Criminal Careers of Habitual Offenders, The Rand Corporation, R-2133-DOJ, August 1974.
13. Finkel, W. P., "Project Datum: Detection and Apprehension Through Use of Microfilm," Proceedings of the 1st International Electronic Crime Countermeasures Conference, Edinburgh, pp. 228-233, July 1973.
14. Seven Major Crimes Excluding Assault, California Comprehensive Data System Criminal Justice Profile, Bureau of Criminal Statistics, 1975.

15. Greenwood, P. W., et al., The Criminal Investigative Process, Vol. III: Observations and Analysis, The Rand Corporation, R-1778-DOJ, October 1976.
16. Discussions with Ray Middleton, Director of the Automated Fingerprint Project, Department of Justice, Attorney General's Office, State of California, March 1979.
17. Swanger, C. W., and J. S. Jackson, "Applications of Fingerprint Identification and Security Systems," Proceedings of the 1st International Electronic Crime Countermeasures Conference, Edinburgh, pp. 190-212, July 1973.
18. Discussions with John M. Jones, Director of Automated Fingerprint Research, FBI, May 1978.
19. Statistical Abstract of the United States, U.S. Department of Commerce, Bureau of the Census, 1978.
20. "Crimes Requiring Identification Technicians," Santa Monica Police Department, Interdepartment Memo, January 1, 1979.
21. "Statistics of Crimes Responded to by Identification Personnel," Santa Monica Police Department, Interdepartment Memo, April 1979.
22. Chaiken, Jan, The Criminal Investigation Process, Vol II: Survey of Municipal and County Police Departments, The Rand Corporation, R-1777-DOJ, October 1975.
23. Greenwood, Peter, and Joan Petersilia, The Criminal Investigation Process, Vol. I: Summary and Policy Implications, The Rand Corporation, R-1776-DOJ, October 1975.
24. Discussions on 5/2/79 with FBI Agent Tom Shield, Los Angeles Office.
25. Systems Development brochure on the SCD TBM 11 Mass Storage System.
26. Goodyear Correlation Processor, reported in Aerospace Daily, January 1979.
27. Cost estimates from USC Processing Institute, June 1978.
28. Discussions with John M. Jones, Director of Automated Fingerprint Research Section, FBI, December 1977.
29. Kingston, C. R., and F. G. Madrazo, "Latent Value Study," New York Criminalistics Research Bureau, 1970.
30. Discussions in 5/77 with Ray Middleton, Director of the Automated Fingerprint Project, California Department of Justice, Bureau of Identification.

31. Wegstein, J. H., The Automated Classification and Identification of Fingerprints, National Bureau of Standards, Technical Note PB-255 189, Department of Commerce, Washington, D.C., 1974.
32. Wegstein, J. H., Manual and Automated Fingerprint Registration, National Bureau of Standards, Technical Note 730, U.S. Government Printing Office, Washington, D.C., 1972.
33. Stock, R. M., "Automatic Fingerprint Reading," Proceedings of the 1972 Carnahan Conference on Electronic Crime Countermeasures, University of Kentucky, Lexington, 1972, pp. 16-28.
34. Rameswara Rao, C. W., and K. Balck, "Finding the Core Point in a Fingerprint," IEEE Transactions on Computers (U.S.A.), C-27, No. 1, pp. 77-81, January 1978.
35. Shelman, C. B., and J. S. Jackson, "Fingerprint Classification - Theory and Applications," Proceedings of Carnahan Conference on Crime Countermeasures, pp. 131-138, 1976.
36. Liu, C. N., and G. L. Shelton, "Computer Assisted Fingerprint Encoding and Classification," IEEE Transactions on Man-Machine Systems, MMS-11, 3, 9, 1970.
37. Rameswara Rao, C. V., et al., "On Fingerprint Classification Systems," Institution of Electronics and Telecommunications Engineers Journal, Vol. 20, No. 11, pp. 550-554, 1974.
38. Malleswara Rao, T. A., "Feature Extraction for Fingerprint Classification," Pattern Recognition, Vol. 8, No. 3, pp. 181-192, 1976.
39. Moayer, B., and K. S. Fu, "A Syntactic Approach to Fingerprint Pattern Recognition," Pattern Recognition, Vol. 7, No. 1-2, pp. 1-23, 1975.
40. Rameswara Rao, C. V., "On Fingerprint Pattern Recognition," Pattern Recognition, (GB), Vol. 10, No. 1, pp. 15-18, 1978.
41. Ting, V. M., and A. P. Ho, "Fingerprint Image Enhancement System," IBM Technical Disclosure Bulletin, Vol. 16, No. 7, pp. 2688-2690, 1974.
42. Moayer, B., and K. S. Fu, "An Application of Stochastic Languages to Fingerprint Pattern Recognition," Pattern Recognition, Vol. 8, No. 3, pp. 173-179, 1976.
43. Singh, V. K., et al., "Feature Recognition and Classification in Fingerprint Patterns," Proceedings of 1977 International Conference on Crime Countermeasures - Science and Engineering, Oxford, England, Lexington, Kentucky, VIII, No. 255, pp. 241-248, July 1977.

44. Levi, G., and F. Sirovich, "Structural Descriptions of Fingerprint Images," Information Sciences, Vol. 4, No. 4, pp. 327-355, 1972.
45. Moayer, B., and K. S. Fu, "A Tree System Approach for Fingerprint Pattern Recognition," IEEE Transactions on Computers, Vol. C-25, No. 3, pp. 262-274, March 1976.
46. Rameswara Rao, C. V., and K. Balck, "Type Classification of Fingerprints - A Syntactic Approach," Third International Joint Conference on Pattern Recognition, Coronado, California, pp. 778-782, November 1976.
47. Hankley, W. J., and J. T. Tou, "Automatic Fingerprint Interpretation and Classification via Contentual Analysis and Topological Coding," Pictorial Pattern Recognition, G. C. Cheng, et al., eds., pp. 415-456, Thompson Book Company, 1968.
48. Moayer, B., and K. S. Fu, Syntactic Pattern Recognition of Fingerprints, Purdue University, W. Lafayette, Indiana, TR EE 74 36, 437, December 1974.
49. Shelman, C. B., and D. Hodges, "A Decimal Henry System," Proceedings of the 1st International Crime Countermeasures Conference, Edinburgh, pp. 213-220, July 1973.
50. Martelli, A., and V. Montevani, "Optimal Smoothing in Picture Processing: An Application to Fingerprints," IFIP Congress, Vol. I, 1971.
51. Scherlowski, L. A., "Optical Spatial Filtering and Its Application to Enhance Low Contrast Fingerprint Images," Proceedings of Photo-Optical Instrumentation Engineers, Solving Problems in Security Surveillance and Law Enforcement with Optical Instrumentation, Vol. 33, pp. 133-138, September 1972.
52. Millard, K., "An Approach to the Automatic Retrieval of Latent Fingerprints," Proceedings, 1975 Carnahan Conference on Crime Countermeasures, pp. 45-51.
53. Shelman, C. B., "The Application of List Processing Techniques to Picture Processing," Pattern Recognition (GB), Vol. 4, No. 2, pp. 201-210, 1972.
54. Hunt, L. B., "Numerical Smoothing and Filtering in N Dimensions," The Computer Journal (GB), Vol. 15, No. 11, pp. 58-65, 1972.
55. Livesay, R., "Fast Match for Fingerprints," Engineering (GB), Vol. 208, No. 5398, 1969.

56. Moore, R. T., et al., "The Graphic Pen: An Economical Semiautomatic Fingerprint Reader," Proceedings of the 1977 Carnahan Conference on Crime Countermeasures, Lexington, pp. 59-62.
57. Juncosa, M. L., The Rand Corporation, paper in progress on statistically modeling both the minutiae and image matching of fingerprints.
58. Guidelines on Evaluation of Techniques for Automated Personal Identification, Federal Information Processing Standards Publication No. 48, U.S. Department of Commerce/National Bureau of Standards, April 1977.
59. Becker, L. G., "Congressional Interest in Security and Privacy of Criminal Justice Information Systems," Proceedings of the 1975 Carnahan Conference on Crime Countermeasures, pp. 1-9.
60. Colton, I. W., and P. Meissner, "Approaches to Controlling Personal Access to Computer Terminals," Proceedings, Second Symposium on Computer Networks Trends and Applications, Gaithersburg, Maryland, June 1975.
61. Greenwood, P. W., Rand Research on Criminal Careers: Progress to Date, The Rand Corporation, N-1286-DOJ, August 1979.
62. Nicholson, W., Microeconomic Theory, Basic Principles and Extensions, Dryden Press, Hinsdale, Illinois, 1972.
63. Goeller, B. F., et al., Protecting a Estuary from Floods--A Policy Analysis of the Oosterschelde, Vol. 1, Summary Report, The Rand Corporation, R-2121/1-NETH, December 1977.
64. An Analysis of Automated and Semiautomated Systems for Encoding and Searching Latent Fingerprints, Project SEARCH, Latent Fingerprint Subcommittee of the State Identification Bureau Project Committee, Technical Memorandum No. 9, March 1974.
65. Project SEARCH, Report on Latent Fingerprint Identification Systems, Technical Memorandum No. 8, March 1974.

## Appendix A

A BRIEF DESCRIPTION OF THE CHARACTERISTICS OF FINGERPRINTS

The two most common methods of characterizing fingerprints are by (1) the features contained within the print (these are commonly referred to as minutiae), and (2) the classification of patterns contained within the print (the most commonly used classification method being the Henry system).

The most common of minutiae or features used for matching are shown in Fig. A.1, with the frequency of occurrence being given in Table A.1. Minutiae agreement between prints forms the basis of positive identification. There is no legal basis which dictates the number of minutiae which must agree between two prints for positive identification; however, the proper alignment of seven minutiae is generally considered adequate for this purpose.

Fingerprint classification, on the other hand, is not a means of securing positive identification, but is rather a shorthand method for screening prints that have some similar properties.

Thus, before fingerprints can be manually matched they are classified in order to reduce the number of prints that must be examined. The Henry system [1,4] has provided the basic means of classifying prints due to its simplicity and reliability. This system uses three basic pattern types--arches, loops, and whorls (indicated in Fig. A.2)--along with their frequency of occurrence. [1] The global features associated with these pattern features are the core and delta singularities, shown in Fig. A.3. The basic classification process determines the primary pattern type for each finger and its secondary class. An elementary Henry system allows eight classifications for a fingerprint--two loop variants, (radial and ulnar), two arch variants (plain and tented), and four whorl variants (plain, central pocket loop, double loop, and accidentals)--thus suggesting  $8 \times 10$  possible classes for the

| Name                                    | Visual Appearance | Name                                | Visual Appearance |
|-----------------------------------------|-------------------|-------------------------------------|-------------------|
| 1. Ending ridge<br>(E)                  |                   | 6. Spur (or hook)<br>(S)            |                   |
| 2. Fork (or bifurcation)<br>(F)         |                   | 7. Eye (enclosure or island)<br>(I) |                   |
| 3. Island ridge (or short ridge)<br>(I) |                   | 8. Double bifurcation<br>(Z)        |                   |
| 4. Dot (or very short ridge)<br>(D)     |                   | 9. Delta<br>(O)                     |                   |
| 5. Bridge<br>(B)                        |                   | 10. Trifurcation<br>(T)             |                   |

Fig. A.1—Nomenclature and shape of the ten individual ridge line (Galton) characteristics<sup>(2)</sup>

Table A.1  
ESTIMATES OF PROBABILITY PARAMETERS

| Parameter       | Cell Configuration        | Frequency | Estimate of Probability Parameter | Estimated Standard Deviation of Estimate |
|-----------------|---------------------------|-----------|-----------------------------------|------------------------------------------|
| P <sub>e</sub>  | Empty <sup>a</sup>        | 6,584     | 0.766                             | 0.0045                                   |
| P <sub>1</sub>  | Island (I)                | 152       | 0.0177                            | 0.0014                                   |
| P <sub>2</sub>  | Bridge (B)                | 105       | 0.0122                            | 0.0012                                   |
| P <sub>3</sub>  | Spur (S)                  | 64        | 0.00745                           | 0.00093                                  |
| P <sub>4</sub>  | Dot (D)                   | 130       | 0.0151                            | 0.0013                                   |
| P <sub>5</sub>  | Ending ridge (E)          | 715       | 0.0832                            | 0.0030                                   |
| P <sub>6</sub>  | Fork (F)                  | 328       | 0.0382                            | 0.0021                                   |
| P <sub>7</sub>  | Lake (L)                  | 55        | 0.00640                           | 0.00086                                  |
| P <sub>8</sub>  | Trifurcation (T)          | 5         | 0.000582                          | 0.00024                                  |
| P <sub>9</sub>  | Double bifurcation (Z)    | 12        | 0.00140                           | 0.00040                                  |
| P <sub>10</sub> | Delta (O)                 | 17        | 0.00198                           | 0.00048                                  |
| P <sub>11</sub> | Broken ridge (or EE)      | 119       | 0.0139                            | 0.0013                                   |
| P <sub>12</sub> | Other multiple occurrence | 305       | 0.0355                            | 0.0020                                   |
| Total           |                           | 8,591     | 1.0                               |                                          |

SOURCE: Ref. 3.

<sup>a</sup>No minutiae characteristics exist in the cell.

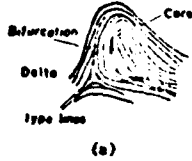
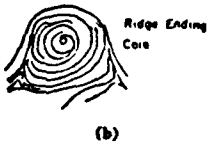
|       |                                                                                               | Frequency of<br>Occurrence<br>(percent) |
|-------|-----------------------------------------------------------------------------------------------|-----------------------------------------|
| Arch  |  <p>(a)</p>  | 5                                       |
| Whorl |  <p>(b)</p>  | 60                                      |
| Loop  |  <p>(c)</p> | 35                                      |

Fig. A.2 —Description of arch, loop, and whorl (Ref. 5)

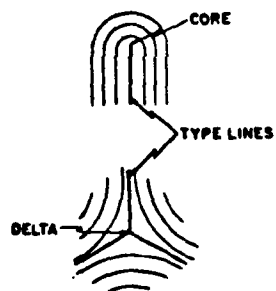


Fig. A.3—Global fingerprint features (Ref. 6)

fingerprints of ten fingers. The effective number of classes is significantly less\* as many classes do not occur; some are very rare while others are very common. This is due to (1) high correlation between adjacent fingers in pattern type, and (2) some of the fingers (pinky) almost always contain the same pattern type. There has been a push (at least in the area of automation) to develop new classification systems or modify the present system so that a more even distribution among prints over classes occurs.

The Henry system generally cannot accommodate latent prints since it is based on all ten prints being classified. The single print classification system used by most law enforcement agencies is the Batley system. [1,4] This system uses a special reticle with ruled concentric circles to measure certain properties of the print. These properties then become the basis for classification. As searching the file for latents is a tedious and time-consuming task, most police departments do not have a separate file broken down by single print classification against which to check latents. The print file kept by police agencies is almost exclusively based on the ten-print Henry classification system or some variant thereof.

---

\*The Henry system contains 1024 (2 to the 10th) primary classes based on the existence or absence of a whorl on each of a person's ten fingers.

REFERENCES--APPENDIX A

1. The Henry System, Royal Canadian Mounted Police, Ottawa, Canada  
(no date).
2. Cumins, H., and C. Midlow, Finger Prints, Palms and Soles, Research  
Publishing Co., South Berlin, Massachusetts, 1976.
3. Osterburg, J. W., et al., "The Development of a Mathematical Formula  
for the Calculation of Fingerprint Probabilities Based on Individual  
Characteristics," Journal of the American Statistical Association,  
December 1977, Vol. 72, pp. 772-778.
4. Bridges, B. C., Practical Fingerprinting, Funk and Wagnalls Company,  
New York 1963.

## Appendix B

MATCHING PROCESS

The purpose of this appendix is to describe the generic forms of fingerprint matching, which are feature matching and image correlation. Before describing these processes it is desirable to describe an overview of all phases of the matching process. Figure B.1 shows such an overview. First, descriptors (print classification, crime type, physical attributes, etc.), as indicated in the figure, are used when possible to narrow down the part of the master file that must be searched for a match. Once this part of the process is completed the prints that have been edited as potential matches are then compared to the suspect or latent print by means of feature matching or image correlation. This matching phase of the process will usually generate several candidate matches which must be checked by a fingerprint expert during the verification phase of the process. The result of this process is either a "hit" or no matches in the file.

The focus of this paper deals with the matching process; however, there have been significant efforts in the classification process which can aid the overall matching process. Presently most police departments utilize the Henry or Galton system, or some variant thereof to classify prints. There are several problems associated with utilizing a classification system. First, in the case of latent prints, the print image may not contain a sufficient amount of information for a classification to be made. Second, errors can be made in classification which can significantly reduce the chances of a successful match. Finally, and most importantly, the classification process does not contain prints uniformly distributed throughout the categories. Instead the majority of prints fall into a small portion of the total number of categories.

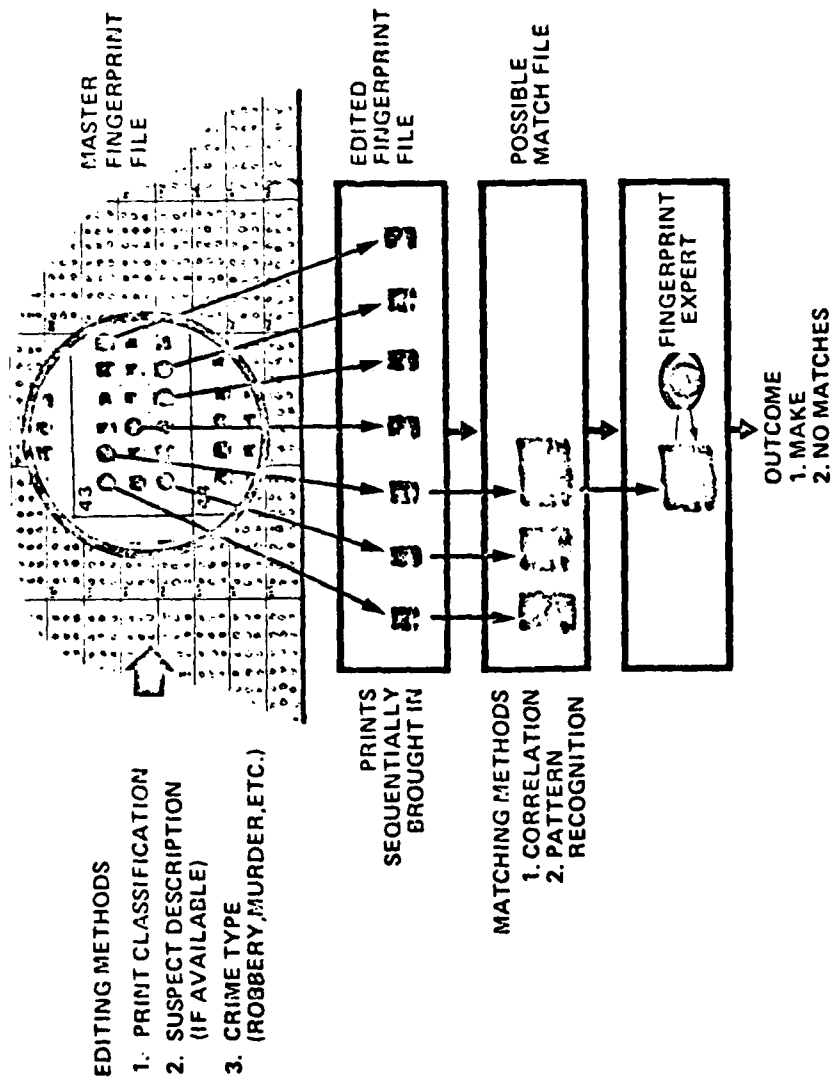


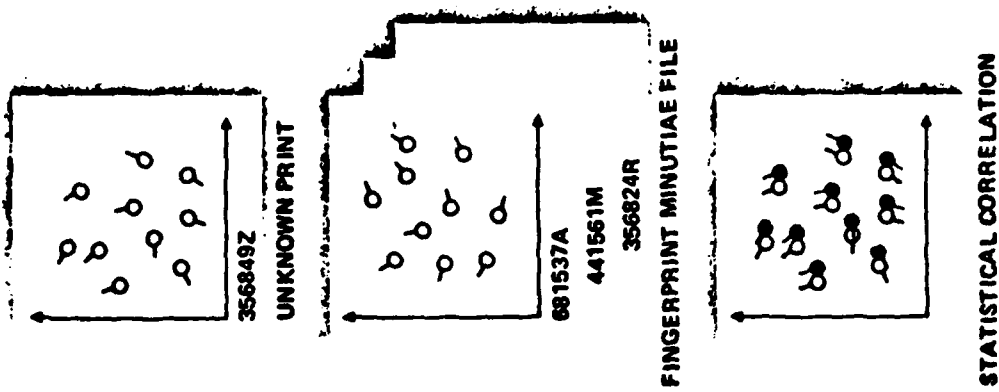
Fig. B.1—Fingerprint Matching Process

For these reasons our system design does not incorporate any reduction in print processing due to classification. However, as was discussed in Section VIII, if a classification can be developed which can overcome some of the aforementioned deficiencies it should be incorporated into the system design.

There are two basic approaches to the matching process--minutiae matching and image correlation. The matching processes for minutiae matching systems are illustrated in Figs. B.2 and B.3. In Fig. B.2 we see a representative diagram of the minutiae matching systems (see Refs. 1 through 10). As indicated in the figure, the original print is enhanced (i.e., missing areas filled in) and a ridge direction plot is obtained. The minutiae in the fingerprint are extracted and combined with the ridge flow pattern at each minutiae point. With all the prints in the master file having been reduced to their basic minutiae and ridge flow directions, it is possible to compare the file prints and the unknown print on a minutiae basis. This is generally done by means of finding the position of best alignment between the two sets of minutiae and then summing the alignment error (X-Y position) between the two fingerprints, accounting also for the ridge slope alignment. One of the problems with this approach has been trying to understand how errors (generally associated with intensity level variations in the scene) translate into geometrical errors and, ultimately, how one relates these minutiae test measures to the probability that the two prints do in fact match. Without such an analytical relationship it is impossible to decide upon a cutoff threshold on the matching measure to retain prints as candidate matches. This problem of ranking prints from best to worst without any cutoff criterion on the measure basis (with every print in the file receiving a ranking) is one of the most severe problems facing the minutiae matching approach.

The image matching approach utilizes all the information in the print. In the optical domain, image correlation can be considered simply as taking the negative of the unknown or suspect print and overlaying it on the positive of a file print. If the prints are

# FINGERPRINT MATCHING



## FINGERPRINT READING

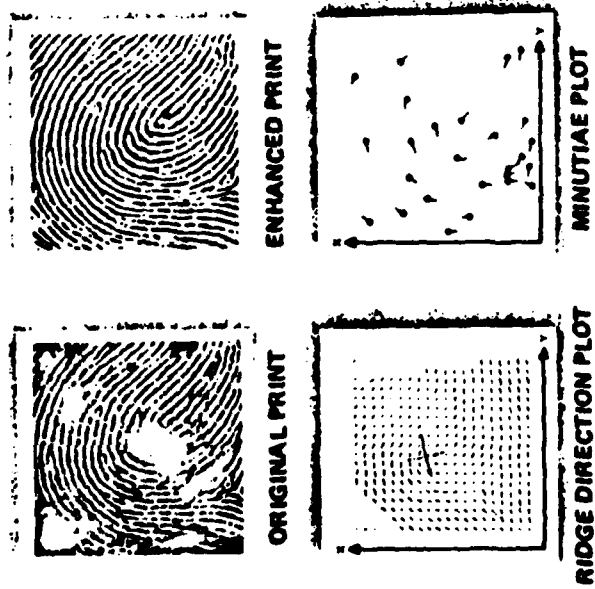


Fig. B.2—Description of a minutiae matching system (Ref. 11)

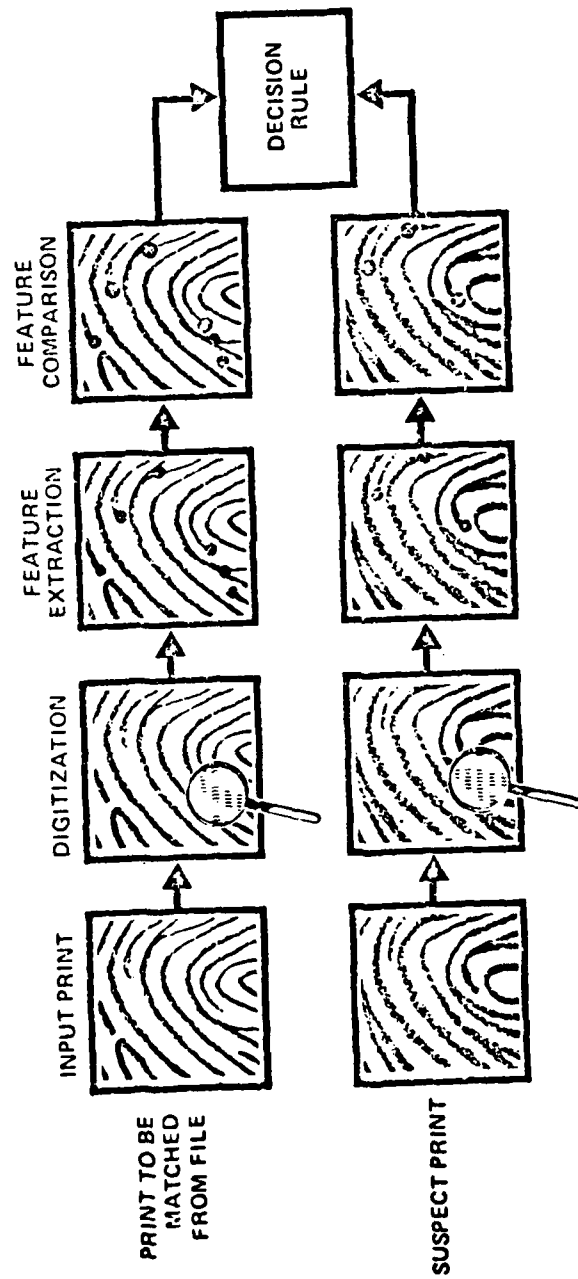


Fig. B.3—Fingerprint Matching via Pattern Recognition

without errors and indeed a match, then this overlay at the position of matching would result in zero light coming through the superimposed prints. For nonmatch prints and positions of nonmatch between two identical prints, spurious amounts of light pass through the superimposed images. This process can be replicated on a digital computer by first considering a digital representation of the image. If the print is broken into a grid network with the resolution of the grid network being such that an individual scene element or pixel is no larger than the width of a ridge or valley, then the print can be described digitally as a matrix of pixels with each pixel having a zero/one intensity level indicating the presence of a valley/ridge structure. Figure B.4A is an example of a digitized fingerprint image, while Fig.B.4B shows the pattern of this print. Having a digital representation of the fingerprint, it is now possible to perform a correlation between an unknown print and the file print. The exact resolution required for the matching process is presently unknown. Initial analysis indicates that a resolution on the order of 100 pixels per dimension is likely to be adequate ( $10^4$  total pixels for the image) for the matching process. Figure B.4A shows a digital representation of a fingerprint at this resolution. The resolution requirement is likely to be different for other functions, such as display and verification, when a significantly higher resolution may be required. (The FBI has indicated that a resolution of 750 x 750 pixels is required for minutiae extraction; however, this appears to be a little too high even for display purposes, and our initial experience indicates that standard TV resolution is probably more than adequate.) The correlation matching for this zero/one image representation is quite simple, being only a logic comparison to count up the total number of agreements between the two images. For this statistical process (as it is easier to model the effects of errors in changing the digital representation) it is possible to estimate the probability of match between any two images and thus set up a cutoff criteria for screening prints for further processing.

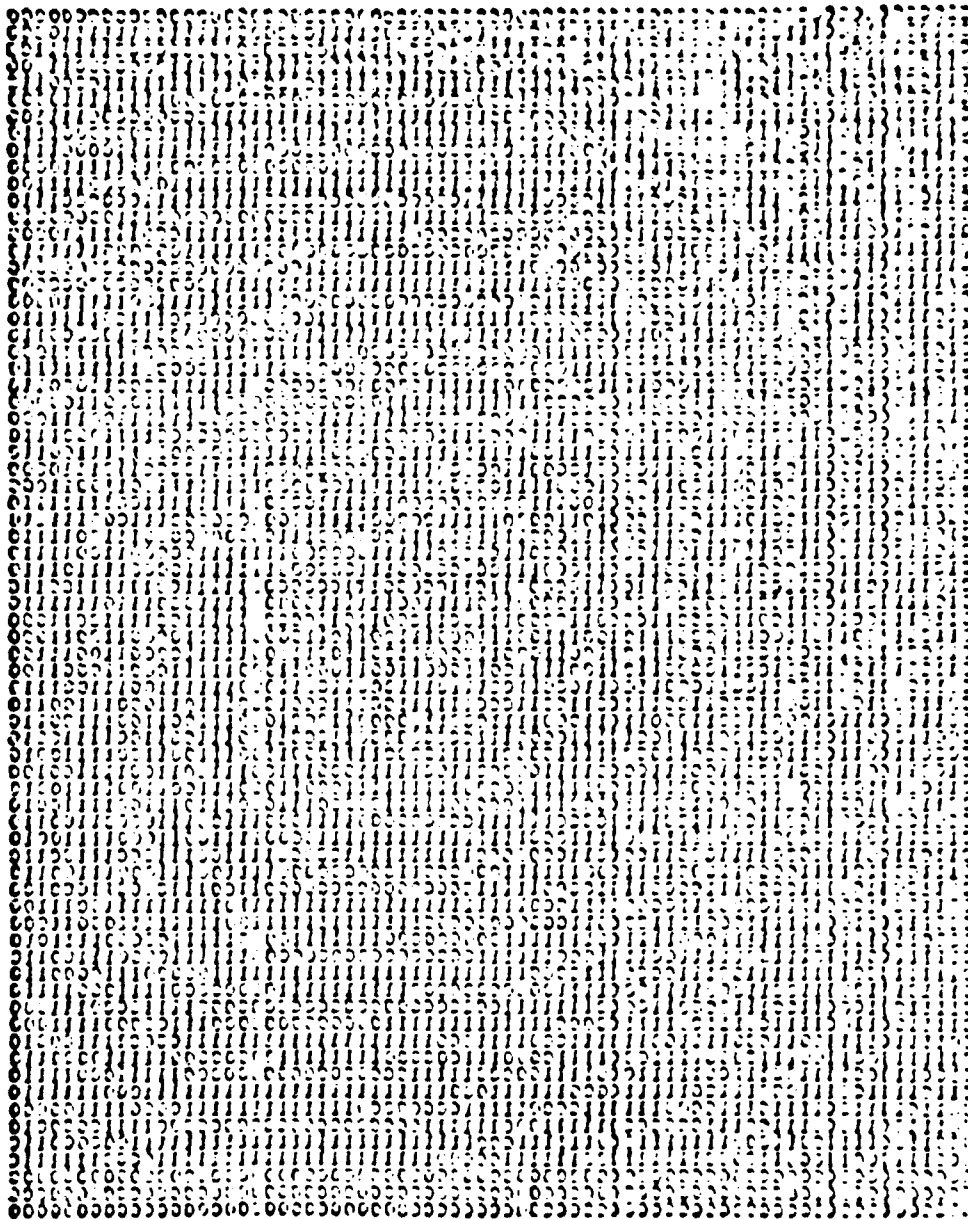


Fig. B.4A—Digital Representation of a Fingerprint Image



Fig. B.4B—Print Pattern for Digital Image

In Fig. B.5 we have an example of digital image correlation on a small area of the print in which we take the suspect print, represented as a set of ones and zeros, and the file print represented the same way. These digitized values can be represented by column vectors,  $X$  and  $Y$ , of ones and zeros and we can perform a zero-one comparison between the two images in any subarea. Here we indicate by the  $Z$ -vector whether we have a match, indicated by one, or a no-match, indicated by a zero. In a subarea correlation we sum up the equivalent number of correct matches and divide by the total number of elements compared. This forms the correlation value in a subarea or region of the print. By adding up all the subareas we can come up with a total print correlation or print score and, based on probability values, establish a threshold by which to carry a print on for further print comparison. By using a probability threshold in each subarea one can ignore noisy or missing portions of prints without eliminating the print from being a candidate match. In addition, information about where the subareas match is useful to eliminate some prints from being falsely considered as matches and to correct distortions in others.

One of the major advantages of this formulation of the problem is that computers are very good at making zero-one comparisons, that is, to decide whether a one in one register equals a one in another computer register, and this process can be carried on very rapidly and accurately, thus making it possible to employ high-speed processing techniques to solve this problem.

Up to this point we have been discussing how prints are matched in a generic sense; however, since there are errors present, all matching processes must deviate in some way from the general approach in order to accommodate these errors. In the remainder of this appendix we shall describe the various kinds of errors that enter into the print matching problem and discuss their effect on the matching process. In the following appendix we shall describe a system design which incorporates processing techniques to accommodate these errors.

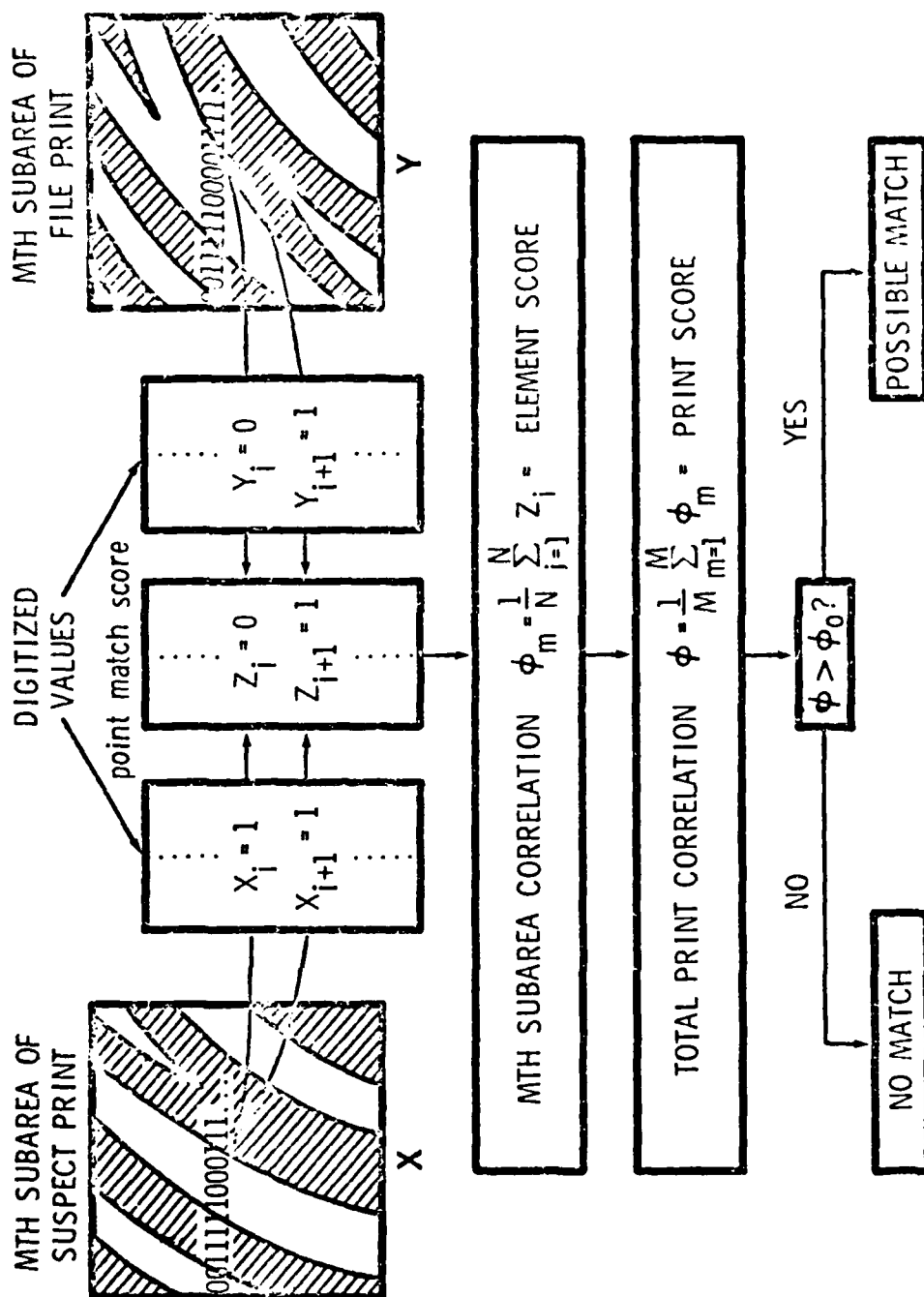


Fig. B.5—Digital Image Correlation

Figure B.6 shows the primary sources of error in print processing. Rotational misalignment results from an inability to correctly align the axis of the unknown print with that of the file print. Stretching errors occur because of uneven pressure over the surface of a fingerprint when it contacts the surface of an object. This stretching causes local distortions to exist in the print image, especially toward the outer surfaces. Missing areas and noise exist primarily in latent prints.

One of the major problems faced by a system designer is that these errors have not yet been statistically quantified. Thus, without knowledge of the statistical distribution associated with the error it is difficult to design a system to the finest detail. This is an area where data analysis is required to facilitate the design of both the minutiae matching and image matching systems.

Minutiae matching systems can be made to accommodate rotation and stretch errors quite handily, but do have significant difficulty with noise (which can cause extra features to appear) and missing areas (which can be located in a portion of the print where a key feature lies). Correlation systems, on the other hand, are fairly efficient at accommodating noise and missing areas. The biggest obstacles to designing a correlation system are overcoming the geometrical distortions of rotation and stretch. In the next appendix we shall discuss, in the system concept, methods for accommodating these types of errors.

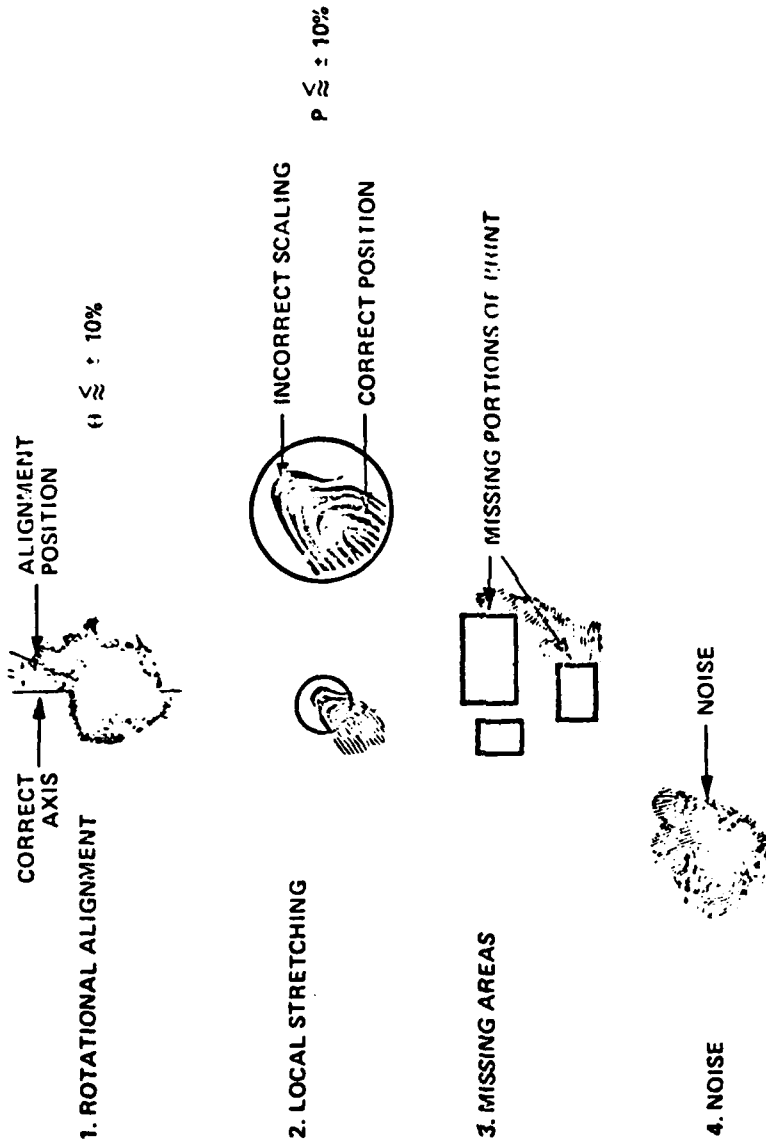


Fig. B.6—Error Sources

REFERENCES--APPENDIX B

1. Banner, C. S., and R. M. Stock, "Finder, The FBI's Approach to Automatic Fingerprint Identification," Proceedings of a Conference on the Science of Fingerprints, Home Office, London, 1974.
2. Wegstein, J. H., and J. F. Rafferty, Computer Science and Technology: The LX39 Latent Fingerprint Matches, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C., NBS Special Publication 500-36, August 1978.
3. Wegstein, J. H., Automated Fingerprint Identification, Center for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C., NBS Technical Note 538, August 1970.
4. Wegstein, J. H., The M40 Fingerprint Matcher, National Bureau of Standards Technical Note 878, U.S. Government Printing Office, Washington, D.C., 1972.
5. Swanger, C. W., and J. S. Jackson, "Application of Fingerprint Identification Technology to Criminal Identification and Security Systems," Proceedings of 1st International Electronic Crime Countermeasures Conference, Edinburgh, July 1973, pp. 190-212.
6. Riganati, J. P., et al., "Minutiae-Based Fingerprint Matching," Proceedings of 1971 IEEE Conference on Decision and Control, Miami Beach, December 1972, pp. 217-218.
7. Asai, K., et al., "Fingerprint Identification System," Proceedings of Second USA-Japan Computer Conference, Session 1-4, pp. 1-6, 1975.
8. Riganati, J. P., "An Overview of Algorithms Employed in Automated Fingerprint Processing," Proceedings of the 1977 International Conference on Crime Countermeasures - Science and Engineering, Oxford, pp. 125-131.
9. Rennick, R. J., and V. A. Vitols, "MUFTI - A Multi-Function Identification System," WESCON Technical Papers - Western Electronic Show and Convention, pp. 1-5.
10. Stock, R. M., "Present and Future Identification Needs of Law Enforcement," WESCON Technical Papers - Western Electronic Show, Vol. 19, pp. 1-13, 1975.
11. Rockwell brochure on Latent Fingerprint Identification System.

## Appendix C

DEVELOPING A FEASIBLE MATCHING SYSTEM

Matching is only one element of the overall fingerprint processing task; however, in order to have a good system one needs an efficient system to perform the matching process. The matching process should be designed to (1) accommodate errors, (2) screen prints, and (3) provide a high throughput capacity. As pointed out in the previous appendix, the major errors to be accommodated are rotation, stretching, noise, and missing areas. Correlation matching can accommodate noise and missing areas reasonably well. The problem in using image correlation with rotational misalignment, as indicated in Fig. C.1, is that as the amount of rotational misalignment increases, fewer and fewer map elements overlap each other at the correct alignment position. [5] The problem is essentially the same for stretch errors. The solution to these errors is to reduce the fingerprint images to a set of subimages. The subimage or subarea (as it is referred to in the correlation jargon) should be of a size that, at the maximum amount of error anticipated, a significant number of the pixels in the subarea overlap their counterparts in the matching image at the position of correct alignment. Figure C.1 shows how to calculate the subarea size for any given misalignment error. Stretch errors can be handled in a similar manner. This technique can also be used to improve the performance of minutiae-based systems.

The first-level solution to handling rotation and stretch errors appears to be subarea correlation, [1-3] i.e., to break the print image into a number of segments and correlate each segment separately. The problem still remains of how to piece the subimages back together and say something meaningful about the probability that any two images match. This can be done in a two-step process.

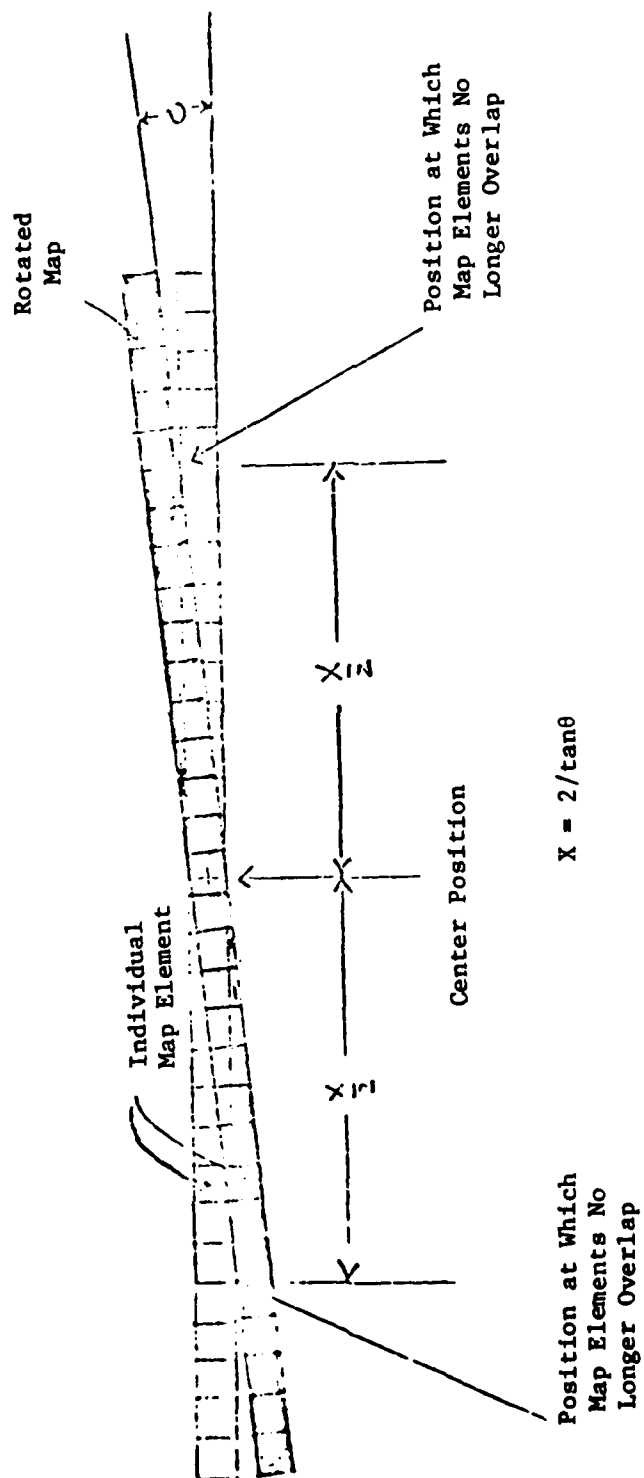
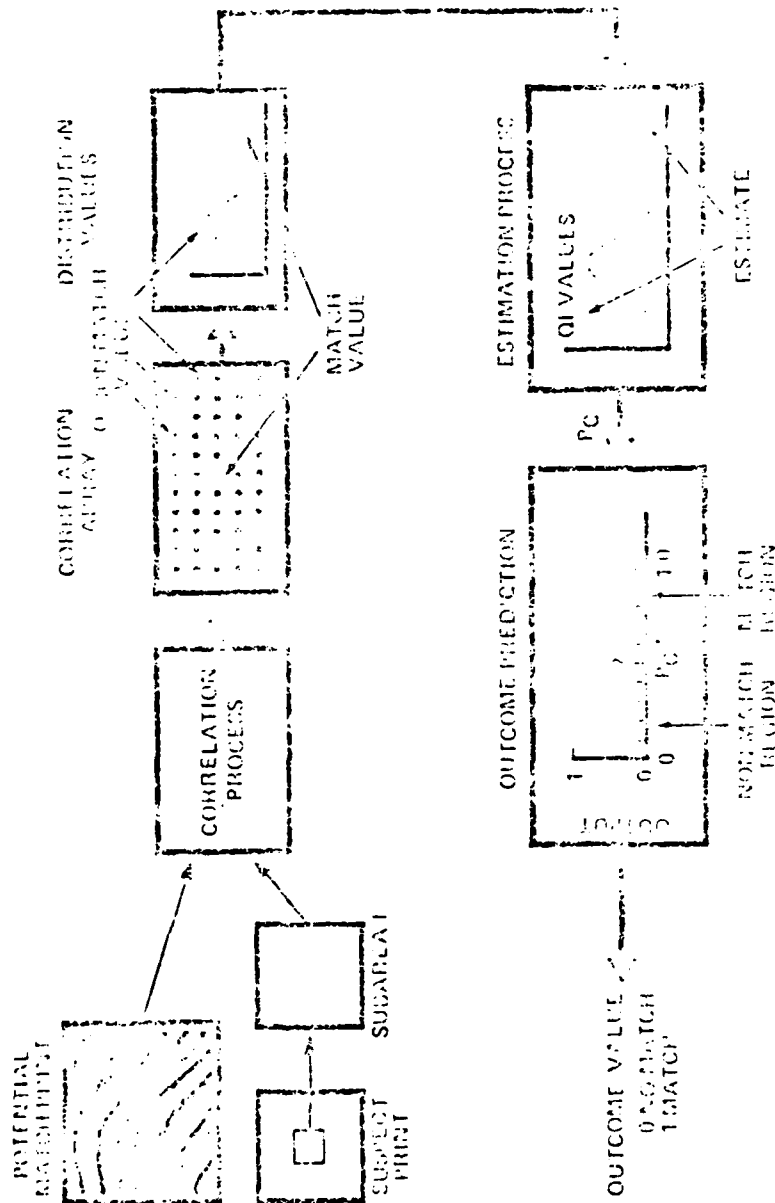


Fig. C.1—Rotational Errors Limit Map Size

First, it is possible from the outcome of the correlation process to estimate the probability of match between any two subareas. Figure C.2 shows a block diagram of the overall probability estimation process. In this figure, the output of the correlation between a subarea of the suspect print and the file print is an array of correlation data. This array is sorted statistically to separate the correlation value associated with the best candidate match position from all other nonmatch correlation values and the distribution of the nonmatch values determined. From this statistical data it is possible to analytically estimate the probability of match between the two images [4] and decide, based on the probability value, whether a match condition exists.

Having computed a probability estimate for each subarea it is possible to screen the print, as illustrated in Fig. C.3, based on the  $P_c$  estimates in each subregion and the spatial relationships between the subareas. For each subarea, information on the size of the subareas (some subareas may be larger than others and should be weighted accordingly) and the probability of match between the subarea and its counterpart in the file print should be thresholded to determine whether that probability estimate was high enough to consider a match to exist between the two subimages. The first part of the screening consists of discarding those regions which have a low  $P_c$  estimate from further consideration. In the case of a nonmatch condition between the file and suspect print, it would be expected that a large percentage of the subareas would have a nonmatch condition indicated, and that on this basis alone they could be eliminated from further processing. In the case where two prints did indeed match, there still may be some subareas which indicate nonmatch conditions due to noise or missing areas, and it is best to discard these subareas from further consideration. For those prints which have a significant percentage of subareas indicating a match condition, the spatial relationships between the subareas would be used as the next step in the print screening process. For these prints (with nonmatching subareas having already been discarded), the

Fig. C.2— $P_c$  Estimate

## AFTER SUBAREA CORRELATION COEFFICIENT ESTIMATION

| SUBAREA | NUMBER OF DATA ELEMENTS | PC                          | OUTLINE PROJECTION                         | SUBAREA MATCHED TO  |
|---------|-------------------------|-----------------------------|--------------------------------------------|---------------------|
| S1      | N1                      | PC1                         | M1                                         | (X1, Y1)            |
| S2      | N2                      | PC2                         | M2                                         | (X2, Y2)            |
| ...     | ...                     | ...                         | ...                                        | ...                 |
| Sj      | Nj                      | PCj                         | Mj                                         | (Xj, Yj)            |
| ...     | ...                     | ...                         | ...                                        | ...                 |
| SL      | NL                      | PCL                         | MCL                                        | (XL, YL)            |
| COMPUTE |                         | AVERAGE $\sum_{L=1}^L PC_L$ | $Z = \frac{\sum_{L=1}^L M_L}{Z \cdot 1 Z}$ | MAP CENTROID (X, Y) |

SUSPECT  
PRINT

## EXAMPLE:

- PC AVERAGE (QUANTITATIVE MEASURE OF OVERALL MATCH)
- PERCENT OF MATCHING ELEMENTS (Z/Z)
- SPATIAL RELATIONSHIP TO DETERMINE MATCHING COEFFICIENT

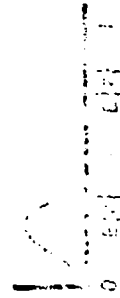


Fig. C.3—Spatial Relationships

spatial match position of each subarea will be compared to the map centroid, and those subareas which do not align themselves correctly will be discarded. Only those prints with a significant number of correctly aligned (spatially) subareas will be carried on for further processing. It is also possible at this point, from the position at which the subareas align themselves, to estimate the magnitude and nature of any geometric errors in the print and thus go back and reprocess the print, correcting for geometric distortion.

At this point it is possible to design a matching system that can accommodate print errors and screen prints based on probability of match as opposed to the ranking procedures used in present minutiae matching systems. It is shown in Section IV that hardware can economically support a high capacity throughput system. Thus far we have only looked at the first level of the matching process. It may be necessary, if there are still a large number of candidate matches remaining at this point, to do further screening. Figure C.4 shows a block diagram of the overall process. The first phase of the matching process consists of using the subarea correlation and estimation procedure described above to create a first-level candidate file. This process would probably involve using low-resolution imagery (on the order of  $100 \times 100$  pixels per image) to perform the initial screening. The philosophy of the next stage is to go for high reliability by possibly including the minutiae matching in conjunction with the image matching. Presumably, at this point in the matching process, the first stage of the matching process has screened out most of the file so there is time and processing available to do significant processing of the remaining candidates to ensure high reliability. The second stage of the process would then consist of locating features that match up between the two prints, and cross-checking to ensure that in areas where the minutiae agreed the imagery was in agreement. Finally, after this stage is complete, it is still necessary to perform manual verification of the final candidate file.

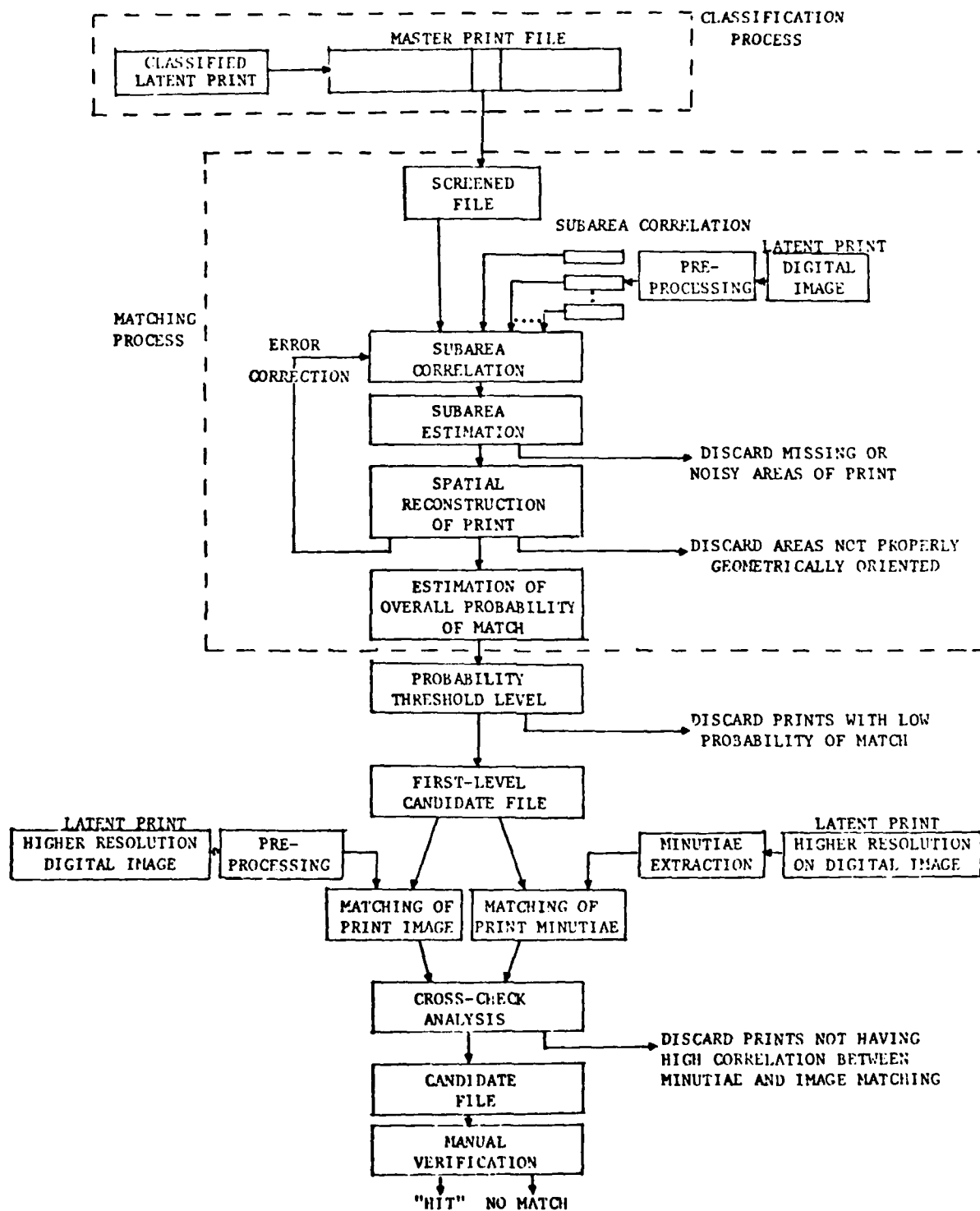


Fig. C.4—Overall Block Diagram of Fingerprint Matching System

The aforementioned design of the matching system attempts to (1) correct for the major deficiencies of the current semiautomated systems, (2) accommodate print errors, and (3) screen prints. As this process has not been attempted on actual fingerprint imagery, it is worthwhile, in Appendix E, to look at the technical feasibility of the concept by examining related work in the field of military map matching.

REFERENCES--APPENDIX C

1. Ullman, J. R., "Subset Methods for Recognizing Distorted Patterns," IEEE Trans., Systems, Man, and Cybernetics (USA), Vol. SMC-7, No. 3, pp. 180-191, March 1977.
2. Smith, F. W., et al., Optimal Spatial Filters, Systems Control, Inc., Palo Alto, September 1978.
3. Gerson, G., et al., Image Sensor Measurements Program, Volume 1, Multiple Subarea Bi-Level Correlation Scene Matching System, Hughes Research Laboratories, Malibu, California, Contract No. F-30602-77-C-0049, June 1979.
4. Ratkovic, J. A., et al., Estimation Techniques and Other Work on Image Correlation, The Rand Corporation, R-2211-AF, September 1977.
5. Bailey, H. H., et al., Image Correlation: Simulation and Analysis, The Rand Corporation, R-2057/1-PR, November 1976.

## Appendix D

PRINT IMAGERY VERSUS PRINT MINUTIAE

Putting aside for the time being the issue of matching capability, there are a number of other functions related to print processing which require print imagery. Let us step back for the moment and take an overview of the entire process. Figure D.1 shows a schematic representation of the process where the master station might be considered to be run by the state law enforcement agency with each local police agency inputting into the state system via a remote terminal. Here we have eliminated the print processing task of the local agency. If one can obtain a rapid enough turnaround time from the master station (say, on the order of two hours or less), there is little need for each police department to keep its own filing system. The schematic block diagram shown here would digitize the print at a remote station and, having displayed the fingerprint to ascertain the print quality, would transmit the digital image to the master station for an identification, wants-and-warrants, or latent print check. At the master station a file management computer would control the process and identify the portion of the master print file to be searched (if classification techniques, physical descriptors, or, in the case of latents, suspect descriptors are used to pare down the file). The known print would then be checked against the edited file via a special purpose matching processor and candidate matches electronically displayed on a cathode ray tube (CRT). A fingerprint expert would then perform a verification to determine if any of the candidates did in fact match the known print in question. With a positive outcome determined on the ID file the management computer would check the wants-and-warrants file for the ID print. This would be a file check by number rather than another print image matching task. Having completed this process, the file management computer would

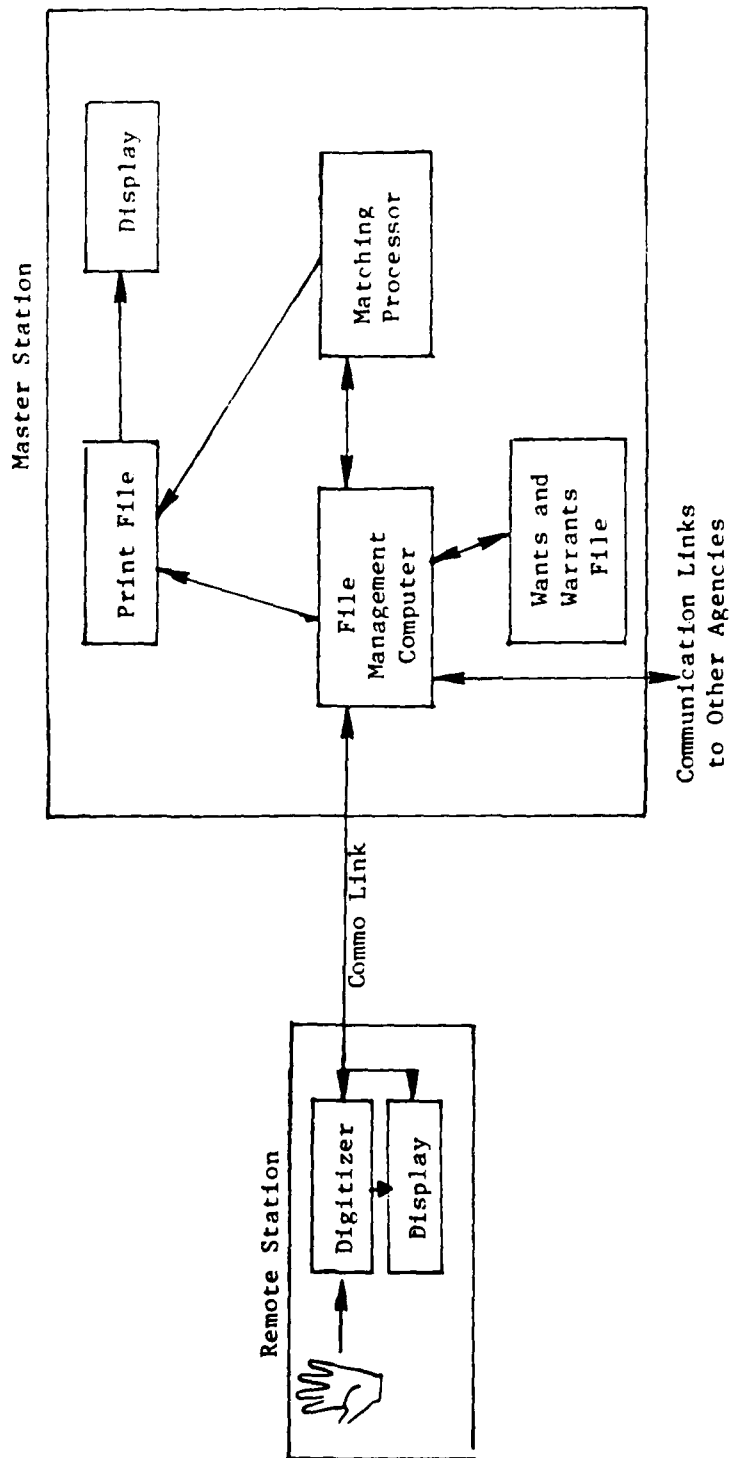


Fig. D.1—Schematic Overview of Print Processing System

communicate the information back to the local police agency and to other appropriate law enforcement agencies. If an ID was not made on the print it would be passed up the line to a higher level agency such as the FBI or some regional system composed of a number of states for further ID checks.

This system would save on manpower by reducing the personnel requirements at the record and identification bureaus of the local police agencies. The acquisition cost of this type of system is compared to the potential cost savings in reduced manpower requirements in a cost-benefit analysis contained in two sections of this report. For some of the benefits it will be difficult to assign monetary values. Included among these benefits would be faster ID and wants-and-warrants check, potential for latent print processing, and improved efficiency in print verification through the utilization of displays. No matter how much additional manpower is added to the present systems for performing the ID and wants-and-warrants checks it is not likely to improve the elapsed processing time that it takes to make a check at the ID level because much of the delays are incurred in the slow communication system (generally mail). In order to make significant gains in elapsed processing time to the state level, new hardware is needed to rapidly move the print imagery from the local policy agency to the state agency and back again. By having a rapid ID turnaround it is possible to identify felons (e.g., forgers) who are not likely to return for the arraignment hearing and take appropriate steps to see that the bail is set at a sufficiently high enough level. It is also possible once a rapid ID has been made to have a better chance of catching criminals (especially those who know how to beat the system) who have outstanding wants-and-warrants before they can escape on bail (in California potentially 4000 wanted felons per year can bail out before they are identified). [3] Additionally, an automated system, appropriately designed, would afford the capability to perform latent print processing where initial surveys indicate that in 20 to 40 percent of all crime scenes investigated [6] latents are left behind by which the suspect can be

identified. Studies indicate that less than 20 percent of all latents lifted are actually processed. [5] Finally, there is a significant fatigue factor encountered by the fingerprint experts in optically comparing fingerprints. Discussions with police personnel indicate that the fatigue factor involved in searching latents may reduce the actual work time to an hour or two a day. [4] There are techniques which can be built into a computer display such as print superposition, print enlargement, etc., to aid the fingerprint technician in this task. Thus, a computer-assisted display system would reduce this fatigue factor and increase the efficiency of this work force. [1,2]

Having discussed these system considerations, let us examine the strengths and weaknesses of the feature matching and correlation matching systems in meeting these goals.

As indicated in Fig. D.2, feature matching really requires two different files, a master file which contains only the minutiae and a master file of print cards. This master computer file by itself is not useful for the verification process in that the fingerprint expert must independently validate the fingerprint match via imagery. A second file of images is therefore required. There may be, and generally are, significant delays in retrieving images. As indicated previously, there is also a problem with the manner in which the candidates for matches are created. They are a result of a ranking process (with all prints in the file being ranked from best to worst). The fingerprint expert does not have adequate match probability information to know when to cut off this candidate production process. For example, the LAPD, using a minutiae-based system, attempted to match the alleged latent fingerprint of a famous case against a file consisting of 35,000 candidates. This matching process was performed in stages with a fraction at a time of the prints being digitized and run against the latent. Because the system measure was a ranking process with no cutoff probabilities, the total number of candidates enumerated was 12,000. [7] Another major system deficiency with this system is that there is no display

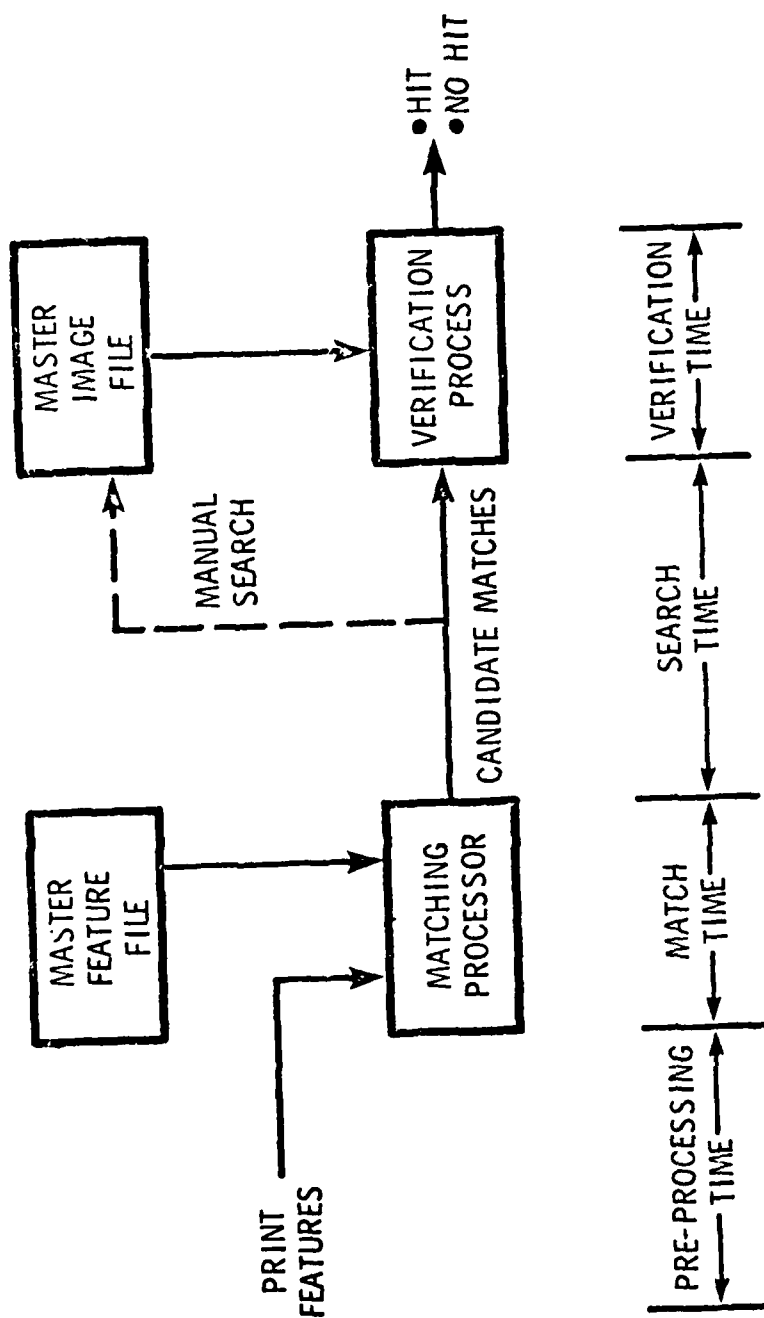


Fig. D.2—Interfaces for Feature Matching

directly compatible with the matching process. Thus, a separate hardware system is required for converting the print to a zero-one format so that telecommunications of the print would be possible.

In Fig. D.3 we have a block diagram of the digital correlation system. As seen in this figure, there would be only one match fingerprint file required, and this file would do everything from providing imagery for display to providing fingerprint imagery for communications. Digital imagery would be stored in a zero-one format for this file. This format expedites the communications problem as the prints can be sent to other agencies or to a video display electronically without any further conversion. It is extremely important to have rapid communication of prints among law enforcement agencies so that criminals can be identified before they can post bail and be gone forever out of reach. This system provides communication of the candidate prints directly to video display. There are a number of features which can be performed by the computer to enhance the display process, making the matching task simple for the fingerprint technician. For instance, the prints may be blown up, superimposed automatically, or the minutiae within the print identified. To summarize, image matching systems have the capability of solving the entire problem of not only matching fingerprints but communicating them to other agencies efficiently, storing them, and providing the means for aiding humans in the verification process by enhancing imagery in the display process. Additionally, if need be, there exist algorithms for extracting the minutiae from the digital print imagery so that an image matching system would also afford the capability of performing feature matching and minutiae identification.

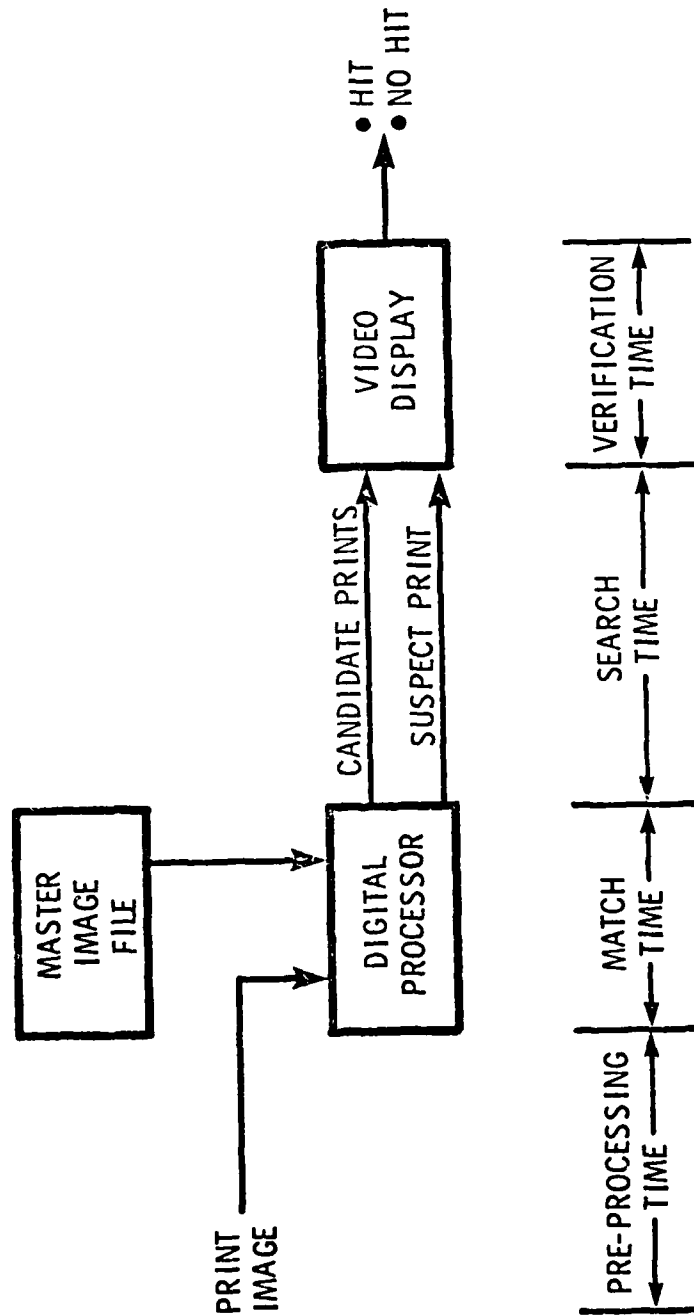


Fig. D.3—Interfaces for Digital Image Matching

REFERENCES--APPENDIX D

1. Griffith, M. L., and J. P. Rigonati, "Interactive Audio-Graphics for Speech and Image Characterization," Proceedings of the Conference on Computer Graphics, Pattern Recognition and Data Structure, pp. 163-169, May 1975.
2. Moore, R. T., et al., "The Graphic Pen: An Economical Semiautomatic Fingerprint Reader," Proceedings of the 1977 Carnahan Conference on Crime Countermeasures, Lexington, Ky., pp. 59-62.
3. Discussion on 4/16/79 with Ray Middleton, Head of Automated Fingerprint Research Project, California Department of Justice, Bureau of Identification.
4. Discussions on 2/8/79 with Lt. Jack Carter, Scientific Investigation Division, Los Angeles Police Department.
5. "Automated Latent Fingerprint Identification System, A Feasibility Study," California Department of Justice, Bureau of Identification, September 1977.
6. Greenwood, P. W., et al., The Criminal Investigation Process, Vol. III: Observations and Analysis, The Rand Corporation, R-1778-DOJ, October 1976.
7. Discussion on 2/8/79 with Capt. John Sparkenbach, Head of Technical Services Division, Los Angeles Police Department.

## Appendix E

RELEVANT MILITARY EXPERIENCE

Much of the image correlation work discussed previously has evolved from the military map-watching work shown in Table E.1. As indicated from this table, this work has been going on from the early 1950s when radar-guided weapons, which used map-watching techniques, were built and fielded. [9] Basically, these weapons employ a reference map which is stored onboard the weapon system. A sensor flying over a target area then forms images of the terrain. These images are then compared to a reference map which is stored onboard to determine the position of match between a sensor image and the reference map. Once the position of match has been determined, the alignment position is then used to update steering commands for the missile. In the early 1960s the Terrain Contour Matching System was invented which is really an altitude contour match of the ground below with a contour stored in the weapon system. The system is currently called TERCOM and is the foundation for present cruise missile developments. [19,20]

There are several significant events of noteworthy interest. First, it should be noted that map-watching systems using correlation have been around for over twenty-five years and have exhibited fairly high reliability on noisy and distorted imagery. Second, most of the early correlation systems used optical processing, and originally some research was done on fingerprint matching using optical correlation techniques. [1-6] These optical correlation schemes for print matching have had limited success with failures primarily due to inability of the system to handle geometric distortion. This is because optical systems are forced to compare the entire imagery at once and are thus unable to break the image into smaller segments where geometric distortion can be handled locally by such techniques as subarea correlation. This fact has been recognized in military applications, and there has been a definite move away from optical systems towards digital systems where it is possible to accommodate

Table E.1

## DOD MAP MATCHING WORK

---

|             |                                                                                             |
|-------------|---------------------------------------------------------------------------------------------|
| Early 1950s | -- Development of radar map matching for Regulus and Mace cruise missiles.                  |
| 1955        | -- Mace fielded in Germany.                                                                 |
| 1958        | -- Exploratory development of ICBM radar terminal guidance.                                 |
| Early 1960s | -- Terrain matching systems developed.                                                      |
| 1969        | -- Development of radar optical correlator for Pershing missile.                            |
| 1974        | -- ALCM and SLCM programs developed with a correlation (TERCOM) matching system.            |
| 1976        | -- ARPA advanced map matcher program employing feature and correlation matching algorithms. |
| 1977        | -- Goodyear advanced development work to build high-speed correlator for Harpoon            |
|             | -- Pershing switches to digital correlation system to aid flexibility.                      |
| 1985        | -- ALCM and SLCM scheduled to be fielded.                                                   |

---

errors in the software programming as compared to having to build specialized hardware to handle these errors. Third, the Defense Advanced Research Projects Agency (DARPA) has sponsored a research program which has utilized both feature matching and image correlation techniques on real-world imagery. Several important conclusions can be reached from this research imagery. The feature matching techniques were generally able to match between 50 to 60 percent of the imagery which contained significant amounts of noise and geometric distortion.

Table E.2 is indicative of the type of results generally obtained by pattern matchers in working with noisy images. Although this report shows significant improvement with the new algorithm, these improvements are generally short-lived, i.e., when the new algorithm is applied to a new scene results comparable to the old algorithm are generally obtained. One of the criticisms of feature matching algorithms is that they tend to be scene dependent. This criticism is probably not significant for the ID problem where (1) noise and distortion are not as severe as they are in the image matching problem, and (2) scene features (ridges or valleys) are consistent throughout all imagery. In the latent print case, however, noise, distortion, and missing areas may pose a severe restriction on the ability of feature matching algorithms to match prints.

Table E.2

RESULTS OF FEATURE MATCHING ALGORITHM WITH NOISY  
DISTORTED (2.5 deg) IMAGE

|                                                | Common Set of Matches            |                             | All Matches                 |
|------------------------------------------------|----------------------------------|-----------------------------|-----------------------------|
|                                                | Old Algorithm<br>(February 1978) | New Algorithm<br>(May 1978) | New Algorithm<br>(May 1978) |
| Reliability                                    | 55 percent                       | 95 percent                  | 95 percent                  |
| Accuracy<br>(normalized to<br>3 mr resolution) | 61 pixels                        | 5.3 pixels                  | 5.8 pixels                  |

Source: Ref. 11.

Based on discussions with users of print matching systems which employ minutiae matching techniques, it appears they are having approximately the same order of magnitude of success in locating latents in the file (i.e., 50 to 60 percent of the time the system actually finds the match when the ID card print is in the file). This indicates that noisy imagery is probably equivalent in terms of matching difficulty to that of latent prints. The results of this program have indicated that the simple correlation systems have done significantly better (a factor of 30 to 40 percent improvement) in matching noisy and distorted imagery than the feature matching approach.

Typical results from other image correlation programs (see Refs. 12-17, 21, 22) also indicate a high probability of success using this technique. Table E.3 shows reported flight test results using a radiometric sensor. It can be seen, even with noise and some distortions present (typical latent print problem), the results indicate a higher success rate than humans can achieve (90 percent) in the ID process where noise and distortions are not very severe.

Table E.3

## CORRELATION SUCCESS RATES (RADIOMETRIC DATA)

| Region                                                     | Number of<br>Valid Trials | Number of<br>Successes | Success Rate<br>(percent) |
|------------------------------------------------------------|---------------------------|------------------------|---------------------------|
| California                                                 | 73                        | 70                     | 96                        |
| New York                                                   | 127                       | 108                    | 85                        |
| Eglin AFB                                                  | 10                        | 10                     | 100                       |
| Green River                                                | 2                         | 2                      | 100                       |
| Total                                                      | 212                       | 190                    | 90                        |
| Total with recommended<br>remedial or preventive<br>action | 212                       | 205                    | 97                        |

Source: Reference 10

Table E.4 shows some simulation results (with all system noises modeled) for a typical TERCOM system. As seen here, false fix probabilities are less than 2 or 3 percent. Actual flight test results for TERCOM systems and other imaging systems which are operational in advanced development are classified.

It does appear that image correlation techniques can accommodate noise, distortion, and missing areas with test results confirming this fact. The limited amount of data in applying optical matching to the fingerprint problem indicates that the major reason for failure was the distortion and registration problem. It is generally believed that "subarea correlation" [7] (breaking the print into smaller images such that the size of the subarea is relatively invariant to the amount of distortion expected) or "spatial windowing" [8] (shaping the areas to be correlated by the degree of expected distortion, i.e., bigger subareas for the portions of print, such as the center, which expect less distortion) techniques can accommodate these errors and achieve results in the fingerprint realm at least as good if not better than those achieved in military applications (fingerprint imagery is more homogeneous than ordinary imagery, and the correlation systems should actually perform better in dealing with a homogeneous scene). It is also anticipated that these systems should perform better than minutiae-based systems (as test results indicate) and should perform at least as well as humans can achieve on "clean" ID prints.

Finally, there have been a number of hardware and software developments which have grown out of these programs and can be transferred to the fingerprint matching problem. Included among these developments are (1) concepts such as subarea correlation, spatial windowing (a technique also designed to accommodate geometric distortions), and probability estimation, [23] and (2) hardware items such as correlation chips and parallel processing to speed up the matching process.

Table E.4

## SIMULATION RESULTS FOR TERCOM SYSTEM USING EURASIAN DATA

| Run                                                          | $P_{ff}^{*1}$ | Notes                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1A                                                           | 0.006 (1)     | 1977 simulation. Test strip intensities solely determined with bilinear interpolation. No velocity or off-diagonal position errors. Reference scene coverage determined from $\pm 3.3\sigma$ along and cross-track test strip overlap. Noise added to each point zero mean, $\sigma_n = 20'$ . |
| 1B                                                           | 0.024 (1)     | Same as 1A with noise added zero mean, $\sigma_n = 30'$ .                                                                                                                                                                                                                                      |
| 2A                                                           | 0.004 (1)     | 1973 simulation described in Section 4.1 with covariance scale factor of 1.                                                                                                                                                                                                                    |
| 2B                                                           | 0.011 (1)     | Same as 2A but $\sigma_n$ determined from total test strip $\sigma_T$ .                                                                                                                                                                                                                        |
| 2C                                                           | 0.017 (1)     | Same as 2A with covariance scale factor of 100.                                                                                                                                                                                                                                                |
| 2D                                                           | 0.032 (1)     | Same as 2C but $\sigma_n$ determined from total test strip $\sigma_T$ .                                                                                                                                                                                                                        |
| 2E                                                           | 0.011 (3)     | Same as 2C but only $\text{Lat}^2$ and $\text{Long}^2$ covariance terms used.                                                                                                                                                                                                                  |
| 2F                                                           | 0.032 (4)     | Same as 2E but $\sigma_n$ determined from total test strip $\sigma_T$ .                                                                                                                                                                                                                        |
| 2G                                                           | 0.011 (4)     | Same as 2C but only $\text{Lat}^2$ , $\text{Lat} \cdot \text{Long}$ and $\text{Long}^2$ covariance terms used.                                                                                                                                                                                 |
| 2H                                                           | 0.024 (4)     | Same as 2G but $\sigma_n$ determined from total test strip $\sigma_T$ .                                                                                                                                                                                                                        |
| *1 Probability of false fix (average of runs in parenthesis) |               |                                                                                                                                                                                                                                                                                                |

Source: Reference 18.

# REFERENCES--APPENDIX E

## Optical Fingerprint Matching

1. Mangasajan, G. R., et al., "Matched Filtering on the Basis of Thick Holograms for Fingerprint Identification," Optics Communications (Netherlands), Vol. 22, No. 2, 169-727, 1977.
2. Tsuruta, T., et al., "Pattern Comparison by Interference Fringe Scanning," Applied Optics, Vol. 13, No. 5, 1089-92, May 1974.
3. Barlai, P., "Incoherent-Optical Correlation with a Hologram; and Examples for the Identification of Fingerprints," Nachrichtentech., A. NTZ (Germany), Vol. 25, No. 10, 474-5, March 1972.
4. Weinberger, et al., "Finident: Correlation of Fingerprint Transparencies by Means of Interference Processing," May 1976.
5. West, C., and D. Wild, "Fingerprint-Based Person Verification System," IBM Technical Disclosure Bulletin, Vol. 17, No. 12, May 1975.
6. McMahon, D. H., et al., "A Hybrid Optical Computer Processing Technique for Fingerprint Identification," IEEE Transactions on Computers, Vol. C-24, No. 4, pp. 358-369, April 1975.
7. Gerson, G, et al., Image Sensor Measurements Program: Vol. I, Multiple Subarea Bi-Level Correlation Scene Matching System, Hughes Research Laboratories, Malibu, CA, Contract No. F-30602-77-C-0049, June 1979.
8. Smith, F. W., et al., Optimal Spatial Filters, Systems Control Inc., Palo Alto, CA, DARPA Contract #DAAK 40-77-C-0113, September 1978.
9. Thomas, J., et al., Cruise Missiles: An Examination of Development Decisions and Management, Naval Postgraduate School, Monterey, California, March 1978.

## Military Map Matching Work

10. Sagawa, S. S., Radiometric Area Correlation Guidance Captive Flight Test Program, Phase 5 - Executive Summary, Air Force Armament Laboratory, Air Force Systems Command, Report AFAL-TR-78-102, Eglin Air Force Base, Florida, September 1978.
11. Kim, R. H., Pattern Matcher Development Study, Sponsored by Defense Advanced Research Projects Agency Report (DoD), ARPA Order #3208, June 1978, Contract DAAK 40-77-C-0017.

12. Bailey, H. H., et al., Cruise Missile Guidance: Discussion of Scene Characteristics and Processing Techniques, sponsored by DARPA, Contract MDA903-78-C-0281, unpublished working paper, February 1979.
13. Wessely, H.W., Image Correlation: Part II, Simulation and Analysis, The Rand Corporation, R-2057/2-PR, November 1976.
14. Bailey, H. H., et al., Image Correlation: Part I, Simulation and Analysis, The Rand Corporation, R-2057/1-PR, November 1976.
15. Reich, A., et al., High Accuracy Cruise Missile Terminal Guidance System, Grumman Aerospace Corporation, Bethpage, NY, sponsored by DARPA, Contract DAAK-40-77-C-0089, December 1978.
16. Johnson, M. W., ALCM Navigation Mechanization Trade Study, Vol. II, The Boeing Company, Document No. D232-10343-2, March 1975.
17. Kuglin, C. D., Performance of the Phase Correlator in Image Guidance Applications, Lockheed Missile and Space Co., Inc., Palo Alto, Report LMSC-D53148, December 1976.
18. Conrow, E. H., and J. A. Naylor, TERCOM Reference Scene Screening and Evaluation Techniques, Internal Report, General Dynamics Convair Division, San Diego, December 1978.
19. Terrain Contour Matching (TERCOM) Primer, Directorate for Systems Engineering, Aeronautical Systems Division, Air Force Systems Command, Wright-Patterson Air Force Base, Ohio, Report ASD-TR-77-61, August 1977.
20. Hinricks, P. R., "Advanced Terrain Correlation Techniques," IEEE Plans, pp. 89-96, 1976.
21. Goodyear Correlation Processor, Reported in Aerospace Daily, January 1979.
22. Merchant, J., Address Modification, Image Technology Program, Vol. I, "Overview and Theory", sponsored by DARPA, Contract No. DAAK-40-78-C-0144, April 1978.
23. Ratkovic, J. A., Estimation Techniques and Other Work on Image Correlation, The Rand Corporation, R-2211-AF, September 1977.

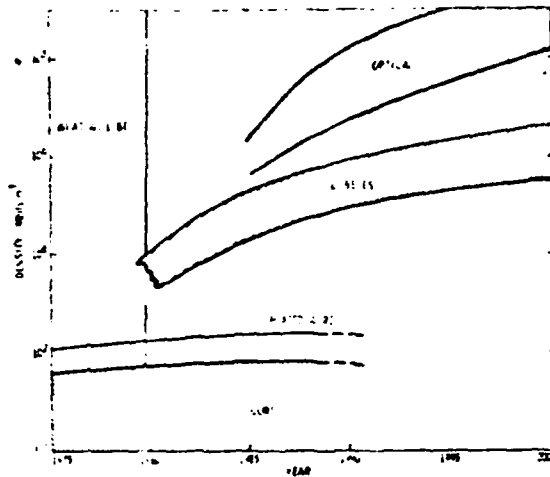
Appendix F

PROJECTIONS ON FUTURE COMPUTER SYSTEMS

Projections on future computer systems--

- o Storage capacities
- o Access rates
- o Storage costs

are taken from NASA-SP-387.



#### DISCUSSION

The forecasts represent the likely spread (what will be) for different device options. The optical and bubble forecasts assume increasing commercial drive - that is, bubbles are not supplanted by CCDs, or optical by superconductors.

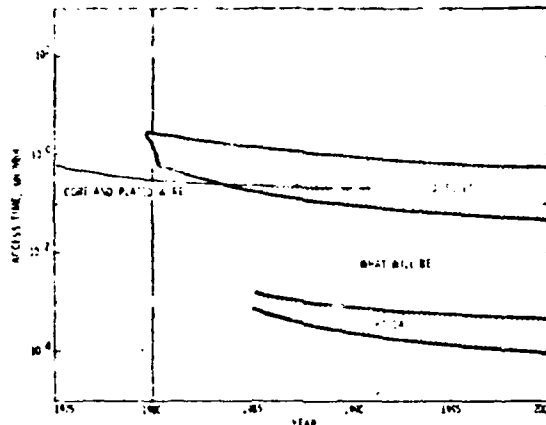
Magnetic cores will decrease in size by 1980 to outer diameters of 10 mils and inner diameters of 6 mils. Practical fabrication limitations will probably prevent further decrease in size after that time. The densities shown include system overhead of drivers, sensors, and power supplies.

Plated wire will also undergo only minor change, decreasing to a size of about 2 mils. The density shown includes system overhead.

Bubble memories are undergoing rapid development. Bit densities on single chips will compete with semiconductor memories using similar lithography and will approach  $10^9$  bits/cm<sup>2</sup> by the mid 80s. The overall system density shown includes the system overhead.

Optical memories using laser read/write techniques are still in the research stage of this time. Such memories will probably not be available before 1985 but potentially offer extremely high capacities. A practical system would involve a minimum of  $10^{11}$  bits of storage.

Fig. F.1—Future System Storage Capacities



#### DISCUSSION

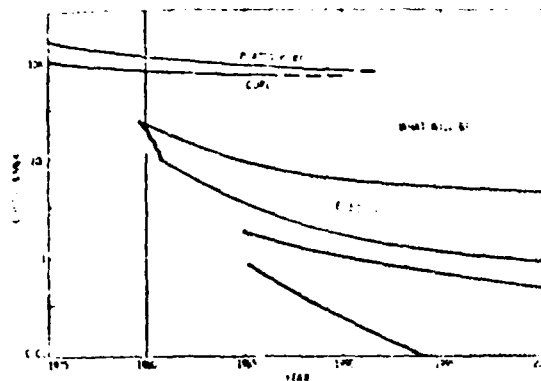
The forecasts are "what will be" for a range of device options, under the assumption that these technologies are driven commercially and survive competition with other technologies.

Read/write times in core and plated wire arrays are of the same magnitude. They are a function of delay times in word drivers, sense amplifiers, and propagation of signals in the array and are not limited by magnetic switching in the elements. Only a small improvement is anticipated by better drive circuitry and IC sensors, and closer spacing within the memory array.

Magnetic bubbles operate as shift registers with shift rates by 1975 on the order of megabits per second. These speeds and their high density make them suitable to fill the memory hierarchy gap existing between cores and disc files. The bubble circuits will probably be shift register loops on the order of 1K bits with access to any one bit in the loop of 1 millisecc. No radical improvement in bubble shift rates can be expected beyond this value. However, use of parallel system organization using the above forecasted performance can lead to much shorter access times per megabit than are shown.

Optical systems permit very short access times per megabit because of their organization into large blocks. Since each block may contain a megabit and the access time to a block is on the order of milliseconds, the access time per megabit is very low. As for the case of bubbles and semiconductors, parallel organization can provide still much shorter access times.

Fig. F.2—Future System Access Rates



### DISCUSSION

The forecasts are "what will be" for a range of device options, under the assumption that these technologies are driven commercially and survive competition with other technologies.

Plated wire and magnetic cores are matured technologies that will undergo little reduction in cost.

Bubble memories are competing with semiconductor CCD memories to replace disc files. This competition and economic motivation will drive the cost down and will make bubble memories cheaper than disc files by the mid-80s.

Optical memories using laser read/write techniques are considered for extremely high-capacity systems ( $10^{11}$  to  $10^{15}$  bits of storage). If a practical technology does emerge (after 1985), we can anticipate the cost of such a system in the millions of dollars, which still represents a very low cost in terms of dollars per megabit of memory.

Fig. F.3—Future System Storage Costs

Appendix G

SURVEY QUESTIONNAIRE

Name:

Police Department Representing:

Telephone:

Address:

Size:

ID PROCESS

Do you have a master print file:

If so, how many prints does it contain?

Size of ID department:

Total staff directly involved in fingerprint identification:

Booking:

Technical Classification:

Technical search:

ID department annual budget?

If a fully automated system were developed, would there be any reduction in your ID personnel?

----NO ----YES

If so, what cuts in personnel would likely occur?

Technical classifiers:

Technical search:

How many people would be freed to perform other tasks?

What percent of the time do you receive word back from the

Bureau of Identification that a person in custody has lied about his identity?

Of those who have lied about their identity, what fraction of the times do you have wants-and-warrants outstanding?

Of those who (1) have lied about their identity, and (2) have wants-and-warrants outstanding, how often does it occur that they remain in custody when word is received back from the Bureau of Identification?

LATENT PRINT PROCESS

Does your department have a latent print section? ---No ---Yes

If so, what is the size of the staff?

If not, do you use some other law enforcement agency to perform this task for you? Which?

What is the size of latent print budget?

Does your department perform any cold searches?

If so, how many full-time employees are involved in this process?

What percentage of the following crimes does your department roll out to collect physical data including fingerprints?

Burglary

Rape

Homicide

Robbery

Grand Theft Auto

Theft from Auto

Assault

What is the percentage of latent prints taken that are actually used?

What is the percentage of latent prints identified via any process (e.g., informants, matching MO, etc.)?

What is the percentage of latents identified via cold search?

Under what conditions will you institute a cold search?

Quality of the print

Seriousness of the crime

What is the value attached to latents as courtroom evidence?

How often are latents the principal evidence in court?