CERIAS Tech Report 2009-39

Multi-Finger Recognition

by Dan Bowman, Mithun Vaidhyanathan, Alexander Miller
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

MUTLI-FINGER RECOGNITION

Dan Bowman, Mithun Vaidhyanathan, Alexander Miller
{ddbowman, mvaidhya, mille130}@purdue.edu
Purdue University

December 2009

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Fingerprint verification is a commonly used modality in biometric identification and as such, Biometric fingerprint verification continues to be incorporated into many facets of world-wide society it is prudent that multiple factors in the image acquisition by accepted as 'industry standards' to facilitate and ensure the information security community can seamlessly integrate technologies.

There is also a need for both better understanding how fingerprint recognition system can better match against multiple fingers without creating the potential for greater security holes.

The impetus for this paper is the better understand the how combinations of multiple fingers affect match scores against a common thresh-hold and to determine, if one exists, an optimal number and combination of fingers to match against to create the lost possibility to both false accepts and false rejects.

Keywords: Biometrics, Fingerprint, Fingerprinting, Fingerprint Recognition, Ten-Print, Multi-Finger Recognition, Biometric System Optimization

CHAPTER 1. INTRODUCTION/ MOTIVATION

As information security requirements continue to grow, there is symbiotic growth in physical forms of security. This security barrier is steadily taking form as a biometric checkpoint, and again, more specifically, fingerprint verification checkpoints.

Fingerprint recognition is the most widely used Biometric modality; securing everything from personal computers to Classified Government Information Systems, fortifying the need for more secure systems.

The objective of this study is to understand two aspects of fingerprint recognition. First, which finger on each hand provides the 'best' images, as defined by the lowest FAR, FRR, and FTE rates, and the highest quality scores and minutia counts, and secondly, what number of combined fingers provided the most efficient match. By using multiple fingers in the identification or verification process it should be possible to create more secure portals of logical or physical access.

CHAPTER 2. LITERARY REVIEW

Fingerprints are composed primarily of ridges and valleys, including minutiae points, which are points where ridges come together or separate apart (Prabhakar & Jain, n.d.). The minutiae and patterns can both be extracted from the fingerprint using developed algorithms and are used to identify each individual (Prabhakar & Jain, 2001). If the match is successful, the user is then permitted after the decision is made by the algorithm that the user is genuine to the particular system the user is trying to access. If by some reason the algorithm determines that the minutiae point template matches somebody else, that person is considered an imposter, and a false accept is made. If the user is denied when the user is indeed genuinely providing the right fingerprint, then a false reject is made by the algorithm. This is the basis for the FAR and FRR variables that can be seen on ROC (receiver operating characteristic) curves (Prabhakar & Jain, 2001). ROC curves are plots of specific FAR levels versus FRR levels, usually in fractions of a percent, that map out how each fingerprint algorithm performs for a variety of FAR and FRR values (Prabhakar & Jain, 2001). It is generally accepted that the closer the curve is towards the origin (or 0%, 0%), the better the algorithm performed.

Fingerprint technology is one of the oldest, and most tried and true, biometrics available on the market today (Prabhakar & Jain, n.d.; Rosenzweig, Kochems, & Schwartz, 2004). Due to its proven effectiveness, it has been adopted by the Department of Homeland Security (DHS) as a means to identify individuals who may be entering and exiting our country (Theofanos et al, 2008). Previously, the DHS used a two fingerprint solution, however recently they have upgraded to a 10-print scanner for added security (Theofanos et al, 2008). As was pointed out in Pankanti, Prabhakar, & Jain, “the probability that a fingerprint with 36 minutiae points will share 12 minutiae points with another arbitrarily chosen fingerprint with 36 minutiae points is 6.10 x 10^-18” (2002), therefore there is a drastic increase in security for every additional fingerprint. However, significant issues impact the implementation of such a system, such as the angle and height of the 10-print scanners to be easy to use for collecting all ten fingerprints of an individual. Counter height options could not be altered, so a solution of rotating the angle of the scanners for shorter and taller individuals was decidedly a solution temporarily, as counter height had the highest impact of performance of the measured variables (Theofanos et al, 2008).

The primary 10-print scanner currently used by the government at entry points to the United States is the L SCAN Guardian by CrossMatch (“L Scan,” 2009; “Livescan Fingerprint,” 2007). This particular fingerprint scanner was also used for the study in this experiment. It allows, as stated before, for four slap enrollments of the four fingers on the right hand, of the left hand, and finally the thumbs. It is also used in Britain at their points of entry as well, and is considered a useful asset in improving border safety (“Britain’s Borders,” 2009).

One noticeable disadvantage of taking a capture of all ten fingerprints versus two fingerprints is the additional processing power and bandwidth needed to process these extra fingerprints, which increases the amount of time it takes to perform matching and ultimately give a decision on the validity of the user. In fact, one study showed acquiring ten prints took an average of about 30 seconds (Theofanos et al, 2007). For large sums of people, this can indeed get burdensome, as both the right hand, left hand, and both thumbs need to be captured separately.

CHAPTER 3. DATASET AND METHODOLOGY

3.1. Dataset Description

Data was collected from 70 participants in a study conducted in 2007. Because the full image of each acquired finger was saved it was not necessary to acquire any additional fingerprint images. Three images were collected from each finger and thumb for a total of 1680 finger images and 420 thumb images. The images were collected on an L3 Cross-match Guardian 10-print system using slap fingerprint acquisition.

3.2. Research Question

Fingerprint recognition has become the most population and widely used biometric modality for identification, verification, and authorization, for both logical and physical access. Current fingerprint recognition systems utilize single fingerprint image to match against a database. While this has been an effective method for many years there is always a demand for more secure systems. If a fingerprint recognition system were to collect multiple fingerprint images and average the quality scores it would create a single score to match against a threshold while using multiple fingers, rather than the traditional single image. This study seeks to determine if there is an optimal number of fingers to match to create both a secure and efficient biometric system.

3.3. Methodology

After the dataset had been collected the images were separated into two subfolders, thumbs, and fingers and each file was named according to the following convention scheme:

1000_T_8N_LH_0001
Person Hand Finger

Figure 1 - Finger File Naming Convention

1000_T_8N_TH_00001

Person Thumb Hand

Figure 2 - Thumb File Naming Convention

The fingers were named based on an ID number given to each participant, and the hand, either ‘LH’ or ‘RH’ was added to the file name, finally, the finger code, was concatenated to the filename.

Table 1 - Finger Codes for File Names

0001	Index
0002	Middle
0003	Ring
0004	Little

The thumbs used a similar file name convention with the person identification number followed by the ‘TH’ for thumb and the hand code.

Table 2 - Thumb Hand Codes for File Names

00001	Right
00002	Left

Using the Verifinger 5.0 SDK code was written to enroll each individual finger into it’s own database, setting the stage for all of the imposter and genuine comparisons to be made. Once the images had been verified against all of the other images in the database the False Accept, False Reject, and Failure to Enroll rates were calculated.

The Aware Quality software was used to calculate Quality Scores and Minutia Counts, which allowed for each finger's statistics, were extracted and analyzed.

Individual fingers were enrolled into the VerfiFinger application to generate Imposter match scores, genuine match scores, and Failure to Enroll rate.

Code for separating aware quality scores:

Once the quality scores were generated, they were separated into files by a Java code that used the following steps:

- Read the file containing quality scores for all finger samples of all participants
- Separate the scores for each finger based on the naming convention discussed above
- Write out the quality scores that have been separated into separate files

Code for combining match scores from VeriFinger (for both genuine and imposter comparisons):

Output obtained from VeriFinger was then used to generate various combinations of fingers by a Java code that used the following steps:

- Specify the match score files of the fingers that need to be combined as command line input
- Find various combinations of the number of files entered. Each combination will be of the form 2^n-1. For example, if 2 files are entered for left index (LI) and right index (RI), we will have the 3 combinations (2^2-1) as LI, RI, and LI & RI.
    - For each combination, compute the average match score of corresponding samples for an individual. Consider the following example. If for person with ID 1000, we have score from matching sample 1and 2 of LI as 100 and score from matching sample 1 and 2 of RI as 200, the average will be computed as 150. However for the same person, if there is a score from matching sample 2 and sample 3 for RI, this score will not be averaged with score from matching sample 1 and 2 of LI. So, match scores from non-corresponding samples will not be averaged, i.e. score obtained from matching sample 1 and 2 of a finger will not be averaged with score obtained from matching sample 2 and 3 of the other finger. The same logic has been followed in all combinations across all datasets

Once the above steps are completed, write the data out to 10 separate files, each file indicating the number of fingers that have been combined. Typically, the 10^{th} file will contain match scores averaged from combining all 10 fingers; the 9^{th} file will contain match scores averaged from combining 9 fingers and so on.

CHAPTER 4. RESULTS & ANALYSIS

Table 3 identifies abbreviations used in analysis.

Table 3 - Finger Abbreviations

Abbreviation	**Meaning**
LI	Left Index
LM	Left Middle
LR	Left Ring
LP	Left Little
LTH	Left Thumb
RI	Right Index
RM	Right Middle
RR	Right Ring
RP	Right Little
RTH	Right Thumb

Tables 4 and 5 contain error rates generated by the VeriFinger application. The data shows that the thumbs, on both hands, consistently produced better images, by means of a lower Failure to Enroll (FTE) rate on both hands. The next lowest FTE rates were the Left Index and Left Middle, and on the right hand, the ring finger, and the index finger. The pinky finger on both hands produced the highest FTE rates.

Table 4 - Error Rates for Left Hand

	Left Index	Left Middle	Left Ring	Left Little	Left Thumb
Genuine	360	360	342	274	412
Imposter	34050	34050	31520	22076	42644
False Rejects	0	0	0	0	0
False Accepts	16	0	0	0	2
Samples	210	210	210	210	210
Images	186	186	179	150	208
FRR	0.0000%	0.0000%	0.0000%	0.0000%	0.0000%
FAR	0.0524%	0.0000%	0.0000%	0.0000%	0.0048%
FTE	11.4286%	11.4286%	14.7619%	28.5714%	0.9524%

Table 5 - Error Rates for Right Hand

	Right Index	Right Middle	Right Ring	Right Little	Right Thumb
Genuine	342	340	360	322	406
Imposter	32600	31522	34050	28070	41824
False Rejects	0	0	2	0	0
False Accepts	0	0	2	2	0
Samples	210	210	210	210	210
Images	182	179	186	169	206
FRR	0.0000%	0.0000%	0.5556%	0.0000%	0.0000%
FAR	0.0000%	0.0000%	0.0000%	0.0087%	0.0000%
FTE	13.3333%	14.7619%	11.4286%	19.5238%	1.9048%

Similarly, table 6 shows the quality score data from all of the fingers. Again, the data shows that the Thumbs of each hand produce the highest quality images while the little fingers produce the lowest quality images.

Table 6 – Aware Quality Score for All Fingers

LEFT		Average	STDEV
	Index	76.03333333	16.77671642
	Middle	75.87142857	17.04869589
	Ring	72.30952381	20.2695804
	Little	65.91904762	21.90864283
	Thumb	80.52380952	10.3314406

RIGHT		Average	STDEV
	Index	74.01435407	16.40780726
	Middle	73.92344498	18.11113861
	Ring	71.85167464	17.53107158
	Little	66.51196172	21.62955378
	Thumb	79.63809524	12.59993454

The match scores obtained from VeriFinger for genuine and imposter comparisons have been algorithmically sorted into various combinations. For both genuine and imposter combinations, considering 10 fingers, we have $2^{10} – 1$ i.e. 1023 combinations of fingers. For each finger combination, the match scores of the individual fingers have been averaged. Data from the combinations was arranged such that 10 genuine and 10 imposter dataset were created each containing combinations of fingers from 1 to 10 combined. Table 7 shows statistics for the combinations of genuine comparisons.

Table 7 - Average and Standard Deviation values for combination of genuine comparisons

# of fingers combined	Average	Standard Deviation
1	974.5043	445.5297
2	888.8786	369.2724
3	863.0459	340.0868
4	850.435	324.5132
5	843.3552	314.8001
6	839.0959	280.1016
7	836.4102	303.3207
8	834.6341	299.6477
9	833.3267	296.7829
10	832.1131	294.7645

Table 7 shows the average match score of a combination of fingers decreases as more fingers are combined. The standard deviation about the mean, in contrast to the averages, decreases as the number of combined fingers increases. It is important to note that all the match score averages are well above the threshold of 47, hence false rejects have a low statistically probability of occurring. It was also observed that among the combinations that gave the highest combined scores the most prevalent fingers observed are the thumbs, index fingers and middle fingers, of both hands.

When each imposter match file is considered individually, there are 20 cases where the match score is above the threshold value of 47. However as we begin combining files, none of the combined match scores (for file combinations combining 2 files to 10 files) go beyond the threshold of 47. Table 8 shows that even the maximum values observed in the datasets reduce as the number of fingers combined increase. This data provides stable ground match against multiple fingers, given that the chances of a false accept or false reject reduce significantly as more fingers are matched against.

Table 8 - Average and Standard Deviation values for combinations of imposter comparisons

# of fingers combined	Average	Standard Deviation
1	7.77845640671727	7.203831946
2	7.77845640671727	5.511497011
3	7.77845640672860	4.817027891
4	7.77845640671727	4.429146661
5	7.77845640672048	4.179173415
6	7.77845640674135	4.003863696
7	7.77845640671631	3.873788268
8	7.77845640671727	3.773290658
9	7.77845640671701	3.693238499
10	7.77845640671731	3.627959939

Tables 7 and 8 show that as the number of combined fingers reach the upper limit for genuine comparisons there is a significant increase in the probability of error, meaning that, there is a greater chance for imposter verification. Because of this it is critical to find the balance point where there is less chance for imposter verification and the greatest chance for genuine verification.

For example, statistics for genuine matches are optimal when there is only 1 finger and seem best for imposter matches when all 10 fingers are combined. As such, the ideal trade-off would be when between 4 and 7 fingers are combined.

Based on the above discussions, we can construct the tables 9 and 10. These tables contain the top four most desirable and least desirable combinations possible in combinations of fingers from one to ten. The data also takes into account various parameters such as: aware quality scores, Failure Accept Rate (FAR), False Reject Rate (FRR), and Failure to Enroll rate (FTE).

Table 9 - Most Desirable combination of fingers

n	FAR	FRR	Four Best Combinations
1	0	0	• [LTH], [RTH], [LI], [RI]
2	0	0	• [LI,LTH], [LI,RTH], [RI,LTH], [RI,RTH]
3	0	0	• [LI,RTH,LTH],[LM,RTH,LTH], [RI,RTH,LTH], [RM,RTH,LTH]
4	0	0	• [LI,RI,RTH,LTH], [LI,LM,RTH,LTH]. [LM,RI,RTH,LTH], • [LM,RM,RTH,LTH]
5	0	0	• LI,LM,RI,RTH,LTH], [LI,LM,RM,RTH,LTH], • [LI,RI,RM,RTH,LTH], [LM,RI,RM,RTH,LTH]
6	0	0	• LI,LM,RI,RM,RTH,LTH],[LI,LM,RI,LR,RTH,LTH], • [LI,LM,RI,RR,RTH,LTH], [LI,RM,RI,LR,RTH,LTH]
7	0	0	• [LI,LM,LR,RI,RM,RTH,LTH],[LI,LM,RI,RM,RR,RTH,LTH] • [LI,LM,LR,RI,RR,RTH,LTH], [LI,LR,RI,RM,RR,RTH,LTH]
8	0	0	• LI,LM,LR,RI,RM,RR,RTH,LTH], [LI,LM,RI,RM,RR,RP,RTH,LTH], • [LI,LM,LR,RI,RM,RP,RTH,LTH],[LI,LM,LP,RI,RM,RR,RTH,LTH]
9	0	0	• [LI,LM,LR,RI,RM,RR,RP,RTH,LTH], [LI,LM,LR,LP,RI,RM,RR,RTH,LTH], [LI,LM,LR,LP,RI,RM,RP,RTH,LTH], [LI,LM,LP,RI,RM,RR,RP,RTH,LTH]
10	0	0	• [LI,LM,LR,LP,RI,RM,RR,RP,RTH,LTH]

Table 10 - Least desirable combinations of fingers

Group Size	FRR (at FAR=0)	Combination
1	0.005556	RR
2	• 0.015789 • 0.016129 • 0.016216 • 0.016575	• RI,RR • RM,RR • RR,RP • LP,RR
3	• 0.015707 • 0.015789 • 0.016043 • 0.016216	• RM,RR,RP • LP,RI,RR • LP,RM,RR • LP,RR,RP
4	• 0.015464 • 0.015625 • 0.015625 • 0.015707	• RI,RM,RR,RP • LP,RI,RM,RR • LP,RI,RR,RP • LP,RM,RR,RP
5	• 0.005076 • 0.005076 • 0.005102 • 0.015464	• LR,LP,RI,RM,RR • LR,LP,RI,RR,RP • LR,LP,RM,RR,RP • LP,RI,RM,RR,RP
6	• 0.005025 • 0.004926 • 0.004926 • 0.004926	• LR,LP,RI,RM,RR,RP • LM,LP,RI,RR,RP,RTH • LM,LR,LP,RI,RP,RTH • LR,LP,RI,RR,RP,RTH
7	• 0.004926 • 0.004926 • 0.004926 • 0.004926	• LI,LM,LR,LP,RR,RP,RTH • LI,LM,LR,RI,RR,RP,RTH • LI,LR,LP,RI,RR,RP,RTH • LM,LR,LP,RI,RR,RP,RTH
8	• 0.004950 • 0.004854 • 0.004926	• LI,LM,LR,LP,RI,RM,RR,RP • LI,LM,LR,LP,RM,RR,RP,LTH • LI,LM,LR,LP,RI,RR,RP,RTH

When analyzing data shown in table 10, the combinations of both nine and ten fingers produced zero false accepts or false rejects and were subsequently omitted from the table.

Based on data contained in tables 9 and 10, the performance parameters of the combined datasets can be observed. The data shows that combinations of multiple fingers do lower the FAR of match. Analyzing the finger combinations of imposter matches shows that very few false accept errors occurred and only when a single finger was used to match against. Also, the data shows that the FRR reduce gradually as the number of fingers combined increase.

While calculating FRR, 95 combinations produced non-zero FRRs. Of these, the most observed fingers in all combinations included the ring and little finger of both hands. The thumb, index finger and middle finger of both hands performed comparatively better and these results added weight to an earlier suggestion that these three fingers must be taken into account while forming finger combinations.

CHAPTER 5. CONCLUSIONS

From the results, we can conclude that the optimal number of fingers to combine into a multi-finger system is between four and six fingers. This can be attributed to the fact that while considering both genuine and imposter matches, combining fingers cause a decrease in the mean match scores, standard deviation and the FRR. From table 9, it can be seen that FRR gradually reduces as the number of fingers combined increase, a trend which certainly makes a statement to combine two or more fingers as opposed to using just one finger. The point to note here, though, is that this study was carried out at a threshold of 47. This value may be high or low depending upon the application using the biometrics. Combining more fingers at a higher threshold can lead to increased false rejects; because we observed in table 6 that the combined genuine match scores reduce when more fingers are combined. Conversely, lesser number of fingers at a lower threshold means risking more false accepts as combined imposter match scores are lower when fewer fingers are combined. These concerns add weight to the fact that out of ten fingers, the ideal number should be approximately at the center of the range 1-10. Thus, as proposed, choosing among 4, 5 or 6 fingers for combining would be an ideal approach.

In these combinations the base set of fingers should include, in order from most significant to least significant, the Left Thumb, Right Thumb, Left Index, Right Index, Left Middle, and Right Middle. This is because these six fingers keep recurring in most of the best combinations. They are also not as common as the ring and the little fingers in the list of the worst combinations. They have superior quality score compared to the ring and the little finger and perform better in terms of FAR, FRR and FTE.

Future Work:
One area that this study did not focus upon was the demographics of the population. A future work might want to study the effect of age, gender, occupation etc. on the number and the nature of the finger combinations. Involving more number of participants or collecting more number of samples per participant would further corroborate or refute the results obtained in this study. Combining the study of force pressure on fingerprint images with this study can give rise to newer dimensions of research. Also, this study can serve as a platform to further analyze the various finger combinations to study their time requirements and performance that would help in eliminating infeasible combinations and in acknowledging the good ones.

BIBLIOGRAPHY.

Livescan Fingerprint Collection with Silicone Membranes. (2007). Retrieved from http://www.infosecurityproductsguide.com/technology/2007/CrossMatchTechnologiesIM.html.

Britain's Borders Strengthened Using Biometric Technology. (2009). *Crossmatch Technologies Case Study.* Retrieved from www.crossmatch.com/products/pdf/Case_Study_UKBAIG.pdf.

L Scan Guardian Compact, Rapid Capture, Dual Use Criminal and Applicant Livescan and Fingerprint Enrollment System. (2009). Retrieved from http://www.crossmatch.com/L_SCAN_Guardian.html.

Pankanti, S., Prabhakar, S., & Jain, A. K. (2002). On the individuality of fingerprints. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1010–1025.

Prabhakar, S. & Jain, A. (2001). Decision-level Fusion in Fingerprint Verification. *Pattern Recognition, 35(2002), 861-874.*

Prabhakar, S. & Jain, A. (n.d.). Biometrics: Fingerprint. Retrieved December 2, 2009, from http://biometrics.cse.msu.edu/fingerprint.html.

Rosenzweig, P., Kochems, A., & Schwartz, A. (2004). Biometric Technologies: Security, Legal, and Policy Implications. *Legal Memorandum, 12, 1-10.*

Theofanos, M., et. al. (2007). Usability Testing of Ten-Print Fingerprint Capture. *NISTIR, 7403, 1-56.*

Theofanos, M., Stanton, B., Sheppard, C., Micheals, R., Zhang, N., Wydler, J., et al. (2008). Usability Testing of Height and Angles of Ten-Print Fingerprint Capture. *NISTIR, 7504, 1-40.*