FAR and FRR Analysis in Real Versus Synthetic Fingerprints

Eric Kane
Computer Science Master's Student
1855 Eggleston Drive
Findlay, OH
ejkane@bgsu.edu

Brian Sigurdson
Computer Science Master's Student
5210 Williston Rd
Northwood, OH
bsigurd@bgsu.edu

ABSTRACT

Biometric authentication is a relatively new branch of computer security in which persons are granted access to systems via some part of their anatomy as opposed to something that they remember or know, such as a password or PIN. Fingerprint identification is one of the most prevalent forms of biometric authentication today, using the fact that all people have unique fingerprints and that fingerprints stay the same throughout one's life. This paper aims to find out whether or not a given system of matching fingerprints is susceptible to falsely accepting fingerprints and conversely if the system is susceptible to falsely rejecting prints. We will use a simulation along with a previously generated dataset to complete our analysis.

CCS CONCEPTS

• **Computer Security → Biometric Authentication**

KEYWORDS

False Acceptance Rate (FAR), False Rejection Rate (FRR), Biometric authentication tools

ACM Reference format:

1 INTRODUCTION

Access to sensitive or private data is the central issue in the computer security world, and as techniques to gain and exploit security vulnerabilities get more sophisticated, techniques to keep private data safe need to improve as well. Biometric authentication is a method of providing access to an individual based on attributes inherent to their body, rather than the classic method of providing access via a piece of data that the individual knows. Technology is currently available to recognize individuals by their voice, vein patterns in their hands, iris / retina scanning, facial recognition, or even the way in which they walk. All of these technologies are being used in some capacity and are constantly being researched to test the viability of tools that can be built using these technologies. Possibly the most prevalent biometric authentication technology today is fingerprint identification. Widely used in forensic science to identify criminals, immigration to assist in background checks of immigrants / refugees, and many others, fingerprint identification has become even more widespread in its use recently, as now seemingly everyone unlocks their mobile device using the technology. Basically, users are able to hold their fingerprints on a sensor present on their mobile device and that sensor attempts to match the fingerprint given to a trusted fingerprint image in the device's database. When the fingerprint matches a trusted fingerprint, the person obtains access to the device. Now, the concept of fingerprint authentication seems simple, but the algorithms that are built to do the physical matching of the prints can be quite complex. While the matching algorithms are complex, we need to be sure that those with malicious intent are unable to exploit them and gain unwanted access to devices they are not authorized to use. In this paper, we set out to test a fingerprint recognition algorithm on a dataset containing both *real* and *synthetic* fingerprints to measure a variety of different metrics with regards to the fingerprint matching results. In particular, we aim to track the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) in order to analyze the efficacy of the matching algorithm under test. Are any of the sets of fingerprints available in our dataset able to fool the matching algorithm into thinking two incongruent fingerprints are a match, and if so, what does that say about this matching algorithm in particular as well as fingerprint identification as a whole?

2 RELATED WORKS

In this section, we discuss some works related to our own research. In [22], the authors write about their experience hosting the first Fingerprint Verification Competition, FVC2000. The competition provided a means for academic and industry practitioners to come together and evaluate different pattern matching finger print recognition algorithms. Three databases of fingerprints were obtained using state of the art scanners, and on database of synthetic prints were used in the competition.

In [23], the authors write about their experience hosting the second Fingerprint Verification Competition, FVC2002. The success of the 2000 competition attracted the attention of additional academic and industry participants, with 33 algorithms submitted in the competition. As with the 2000 competition, three databases of real fingerprints have been collected, and a forth database of synthetic fingerprints is also included.

In [24], building on the success of the 2000 and 2002 Fingerprint Verification Competitions, the authors the results of the 2004 competition, which included 67 algorithms competing on three real and one synthetic database.

In [5], the authors were involved in hosting the 2004 Fingerprint Verification Competition (FVC2004). They write about the competition and its ability to allow them to study the theoretical and practical issues of performance verification of fingerprint verification systems. The discussion goes into more depth than the shorter papers discussed in [22],[23],[24].

Although, there is no lack of literature on fingerprint analysis, there is considerably less, when restricting the focus to the comparison of real versus synthetic fingerprints.

3 METHODOLOGY

3.1 Introduction

The basic steps of our approach were to compare the False Acceptance Rate (FAR) and False Rejection Rate (FRR) for real versus synthetic fingerprints.

When fingerprints are compared, the result is generally not a binary yes or no value, but rather a score, generally between zero and one hundred, and the researcher sets a threshold value. A score above this value is assumed to be a match, and a score below this threshold is consider to not being a match.

The researcher generally has access to some meta-data about the real and synthetic prints. This meta-data allows the researcher to determine when an indicated match or rejection is incorrect.

The FAR is the ratio of the number of false acceptances divided by the total number of comparisons. The FRR is defined in a similar manner to the FAR.

3.2 Tools and Resources

3.2.1 SourceAFIS. This open source software was used to read raw images from files and compute a similarity value. According to the SourceAFIS website, SourceAFIS "is an algorithm [for] recognizing human fingerprints." [21] The software is available in two nearly identical version, Java and .NET, and has a goal of being easy to use. The Java version required only a single jar file be added to a project, in order to access the SourceAFIS's classes.

Each image is loaded as a raw byte array, and then a template object is created, whereby specific items are extracted from the image and recorded in the template. These items are referred to as minutiae.

Below is a small portion of our code illustrating some of the pertinent activities that occur in the processing of images in order to create templates and ultimately calculate similarity values between selected images. Try blocks omitted.

Here, we read in raw bytes for our image under consideration.

```
// read in the bytes for image
  image = Files.readAllBytes(Paths.get(fd.theFile.getPath()));
```

We then need to create a template for each image that is read into the system, because templates will hold all of the pertinent information about an image in order to create a similarity value.

```
// create template
  fd.template = new FingerprintTemplate(image);
```

At this stage, we have images to compare and therefore construct a matcher object for one of our images. The object used to create the matcher object is irrelevant, as the comparison is a symmetric activity.

```
// create a matcher for the random sample item
  FingerprintMatcher matcher =
    new FingerprintMatcher(rsFDItem.template);
```

With a matcher object we can calculate a similarity score.

```
// use matcher to create score for the current random sample item
// and the currently selected image from the pool of images
  double score = matcher.match(candidate.template);
  long score = Math.round(matcher.match(candidate.template));
```

With our score, we can determine if the images are a match.

```
  boolean scored_match = (score >= threshold);
  boolean true_match =
    rsFDItem.name.equalsIgnoreCase(candidate.name);
```

When all our calculations are completed we write the resulting values to file for further analysis.

```
// write to all data file
all_data_writer.println(
     threshold + ":" +
     score + ":" +
     scored_match + ":" +
     true_match + ":" +
     rsFDItem.name + ":" +
     rsFDItem.fvc_year + ":" +
     rsFDItem.db_num + ":" +
     rsFDItem.scanner_type + ":" +
     rsFDItem.print_type + ":" +
     candidate.name + ":" +
     candidate.fvc_year + ":" +
     candidate.db_num + ":" +
     candidate.scanner_type + ":" +
     candidate.print_type
)
```

The following is a sample output record.

- 15 : 6 : false : false :
- 2000-db2-106_6.jpeg : 2000 : 2 : 2 : R
- 2004-db4-107_7.jpeg : 2004 : 4 : 4 : s

3.2.2 Fingerprint Verification Competition (FVC2000, FVC2002, FVC2004). This series of fingerprint competitions,

[25][26][27], provides a subset of the original databases used in the actual competitions. These databases were used in our analysis. Each competition has three real fingerprint databases, generated with state of the art scanners of the time, and one synthetic fingerprint database generated by SFinGe[28].

3.3 Steps Taken

After obtain the sourceAFIS software, the fingerprint databases for the 2000, 2002, and 2004 competitions were downloaded. There were a total of 80 images per database, with 240 per year, provided us with 960 total images to analyze.

Since, a fourth of the images were synthetic, we allotted one fourth of the sample images to be from the synthetic images. The images were given a unique identifier, and twenty images were selected at random, with the restriction that five of the twenty images be selected from the synthetic image pool.

The images were then each read into a Java program as raw byte arrays. Image templates were created for each images and stored in an array for easy comparison.

At this point the template for each sample image was compared to each image's template in the total image pool, and a resulting similarity score was computed. The similarity scored between the compared images, and their relevant meta-data was written to a file for analysis.

This whole process was repeated for several threshold levels between zero and 100.

4 RESULTS

During each trial run, the threshold for the score necessitated in order to achieve a "match" was increased, in increments of ten from the values 15 to 85. All in all, the 20 (15 of which are real and 5 of which are synthetic) prints that were chosen as the baseline prints for the study were compared to 959 fingerprints each for the eight trials of this experiment. This results in a relatively large data set of 19,180 data points for each threshold level and 153,440 data points in total. With these data points we are able to visualize the results to show just how important the threshold value is so that the matching algorithm is not too harsh or friendly. In Table 1 below, we can see that the False Acceptance Count (FA) and False Acceptance Rate (FAR) decrease as the threshold increases. That result is illustrated further in Figure 1. As can be seen in the table, each trial of the experiment had one False Rejection (FR) when a certain print was compared to itself and failed the match test. This single occurrence was the same print for each trial. Due to this uninteresting result of FRs, we do not illustrate that result in a figure.

Table 1: Overall False Acceptance and Rejection Rates

Threshold	FA	FR	Total	FAR	FAR	1-(FAR+FRR)
15	516	1	19180	2.6903%	0.0052%	97.3045%
25	165	1	19180	0.8603%	0.0052%	99.1345%
35	126	1	19180	0.6569%	0.0052%	99.3379%
45	116	1	19180	0.6048%	0.0052%	99.3900%
55	106	1	19180	0.5527%	0.0052%	99.4421%
65	93	1	19180	0.4849%	0.0052%	99.5099%
75	83	1	19180	0.4327%	0.0052%	99.5620%
85	77	1	19180	0.4015%	0.0052%	99.5933%
Total	**1282**	**8**	**153440**	**0.8355%**	**0.0052%**	**99.1593%**

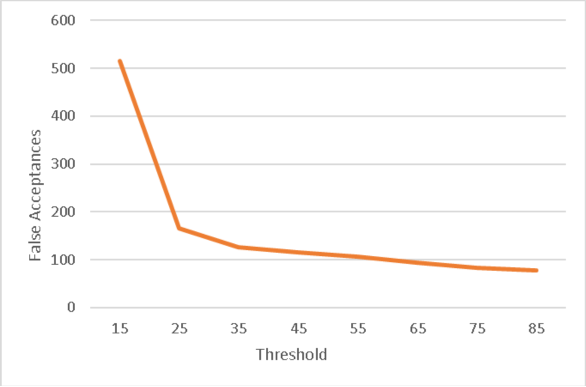

Figure 1: False Acceptances by Threshold

Another important level of detail that is present in this study is the type of fingerprints that are being compared to each other. There are four possibilities in this dimension: a real print can be compared to a real print (RR), a real print can be compared to a synthetic print (RS), a synthetic print can be compared to a real print (SR), or a synthetic print can be compared to a synthetic print (SS). The database is approximately made up of 75% real prints, so the breakdown that is illustrated in Table 2 below shows that there are more comparisons involving real prints than there are involving synthetic ones. So, for each trial, the numbers from the table stay consistent, with the 15 subject real prints being compared to every other print in the study, as well as the 5 subject synthetic prints undergoing the same comparison to every other data point. In Table 3, we take our two meaningful statistic dimensions, FA/FR occurrences and comparison types (RR, RS, SR, SS) in order to display the frequency of false outcomes with regard to the types of fingerprints that are being compared.

Table 2: Comparison Types per Trial

RR	RS	SR	SS	Total
10785	3600	3595	1200	19180

Table 3: FA and FR by Comparison Type

Type	RR	RS	SR	SS	Total
FA	871	44	74	293	1282
FR	8	0	0	0	8
Total	**879**	**44**	**74**	**293**	**1290**

Overall, with the 153,440 data points, there is ample data available to make meaningful conclusions about the results of the experiment. In the next section, we analyze and discuss the meaning of the obtained results, specifically what they can tell us about the security of fingerprint matching tools.

5 ANALYSIS & DISCUSSION

The basis of this study is to find out what risks are inherent to fingerprint authentication, and by extension biometric authentication as a whole. In Table 1, we see the False Acceptance Rate and False Rejection Rate as a function of the number of fingerprints that are compared and attempt to gather some meaningful information from the results. As we can see, in the table, when we set the threshold for matching at a value of 15, there are over 500 falsely accepted pairs of fingerprints as matches. This means that if a real world matching algorithm had the equivalent of a 15 threshold in their version, over 2.5% of non-matching prints could be given access to data that they are not supposed to have access to. Consequently, we can see that the number of false acceptances decreases exponentially as we increase the threshold, resulting in a FAR of less than 0.5% when the threshold is set to 85. This value still seems high, in that it means approximately 1 out of 200 people would be able to get access that they are not supposed to have. Ideally, we could set a threshold high enough to get a FAR well below 0.5% so that no access is provided to those that should not have it. Additionally, at each threshold level, there is one pair of prints that should match that do not. This print for some reason has a similarity score of zero, which leads us to believe that there is something wrong with that specific data point. All other prints have incredibly high matching scores with themselves, so it is our belief that raising the threshold will not result in a significantly higher FRR, which is a good thing. This means that increasing the threshold even more should result in a lower FAR and not negatively affect the FRR, which means we should get closer to providing the proper access to those who need it and removing access from those that should not have it.

The second set of data that we need to explore is how the real versus synthetic (faked) prints compare to one another and if one version is more likely than another to fool a matching algorithm at a given threshold level. This is illustrated in Figure 2 below.

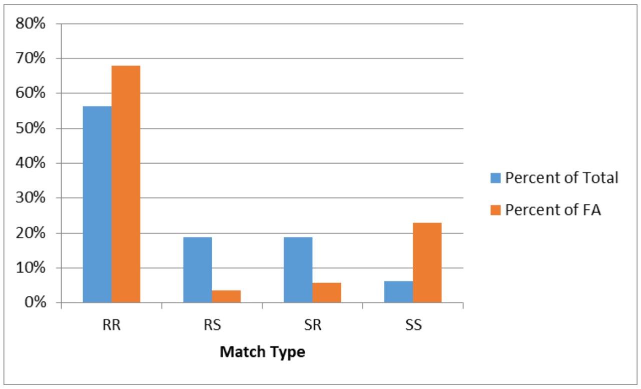

Figure 2: Percentage of Comparisons and FA by Match Type

As we can see, while there were approximately 20% each of Real-Synthetic (RS) and Synthetic-Real (SR) comparisons, that 38% total is not in line with the 9% of total FA occurrences in the study. Conversely, we can see that the comparisons where the same types of prints are being compared, whether real or synthetic, the rate of FA is much higher among that data set when compared to the percentage of the total. This is especially true when looking at Synthetic-Synthetic (SS) comparisons. This result leads us to believe that the greatest risk to the matching algorithm should not be a real world risk, as there will not be individuals using synthetic prints in order to gain access to their data, so it will be harder to spoof a real print. This is a good result for the security of fingerprint authentication.

6 THREATS TO VALIDITY

As with any study, there are inconsistencies in the study as well as risks that may be mitigating factors to the applicability of the study. First and foremost, the fact that the tools available in the study were free versions immediately brings up the point that there are other versions of tooling out there that may have allowed for better matching algorithms or other aspects of the study to be improved. A second threat would be the sample size that was tested. As there were a limited number of prints available in the databases that were being used during the experiment and resources were restricted, disallowing us to obtain giant datasets. The fact that there were only 20 subject fingerprints used in the study is a constraint that we had to deal with, as the computing power and resources available did not make it feasible to generate a huge matrix of comparisons that could have led to a more precise result. A final threat to validity is that the thresholds used in this study may or may not have been up to the standards used in modern day, production matching algorithms. While these shortcomings of the study, due to time and budget, could be a threat to the overall validity of the study, it does not tarnish the result of clearly stating that the threshold must be set at a proper value in matching so as to minimize both the FAR and FRR.

7 FUTURE WORK

As this study was undergone with a limited scope as well as a limited budget of time and money, there are many expansions that this study could use to make it an even better study. Simply sticking with the fingerprint matching piece of the biometric authentication space, in the future we would like to obtain multiple real production services or tools to run this same experiment on. Another good addition would be to include real human subjects, as many as possible so that we could be sure that the study was being tested in a real world scenario. Data sets were a huge issue in this study, so in the future if we were able to obtain much larger stockpiles of fingerprints and computing time, we could generate larger result sets that would give us a much stronger result.

In addition to the fingerprint matching algorithm part of the biometric authentication space, we believe that this study, or some variant of the study could be done with other branches of biometric authentication technology. The study could be done with Retina/Iris Scanning, Vocal Recognition, Vein Pattern Matching, etc. and the results of those future experiments could be compared to findings about fingerprint matching that would allow us to draw widespread conclusions about the efficacy of each technology. This could shape what types of security these technologies provide and in what real world scenarios they could potentially be used in. We truly believe that the expansibility of this study is something that should be explored in more detail in the future.

8 CONCLUSION

To conclude, we took a large database of real and synthetic prints and were able to compare 153000 pairs of prints in order to gather some meaningful results. Showing that increasing the threshold likely will not affect the FRR negatively while drastically reducing the FAR is a great result for the matching algorithms to be able to work properly. We also believe that this study can be used and expanded upon both in the fingerprint authentication world, but in biometric authentication as a whole.

ACKNOWLEDGMENTS

We would like to acknowledge SourceAFIS and the open source software we were able to use to complete this study.

REFERENCES

[1] Technovelgy.com where science meets fiction. Retrieved from http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=11

[2] Precise Biometrics AB, (2014). Understanding Biometric Performance Evaluation. Retrieved from https://precisebiometrics.com/wp-content/uploads/2014/11/White-Paper-Understanding-Biometric-Performance-Evaluation-QR.pdf

[3] Unar, J.A, Woo Chaw Seng, Almas Abbasi (2014). A review of biometric technology along with trends and prospects. Pattern Recognition, 47 (2014), 2673-2688

[4] A. K. Jain, J. Feng and K. Nandakumar, "Fingerprint Matching",IEEE Computer, Vol. 43, No. 2, pp. 36-44, February, 2010.

[5] R. Cappelli, D. Maio, D. Maltoni, J. Wayman, A. Jain, "Performance Evaluation of Fingerprint Verification Systems", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 28, No. 1, pp. 3-18, January, 2006.

[6] R. Cappelli, A. Erol, D. Maio and D. Maltoni, "Synthetic Fingerprint-image Generation", in proceedings 15th International Conference on Pattern Recognition (ICPR2000) , Barcelona, vol.3, pp.475-478, September 2000.

[7] R. Cappelli, "SFinGe: an Approach to Synthetic Fingerprint Generation", in proceedings International Workshop on Biometric Technologies (BT2004), Calgary, Canada, pp.147-154, June 2004. Invited paper.

[8] R. Cappelli, D. Maio and D. Maltoni, "Synthetic Fingerprint-Database Generation", in proceedings 16th International Conference on Pattern Recognition (ICPR2002) , Québec City, vol.3, pp.744-747, August 2002.

[9] Q. Zhao, A. K. Jain, N. G. Paulter and M. Taylor, "Fingerprint Image Synthesis based on Statistical Feature Models", BTAS, Washington, D.C., Sept. 23-26, 2012.

[10] Andrea F. Abate, Michele Nappi, Daniel Riccio, Gabriele Sabatino, 2D and 3D face recognition: A survey. Pattern Recognition Letters, 28 (2007), 1885-1906

[11] Zetter, Kim (2012-07-25). "Reverse-Engineered Irises Look So Real, They Fool Eye-Scanners". Wired Magazine. 25 July 2012. Retrieved from https://www.wired.com/2012/07/reverse-engineering-iris-scans/

[12] Sudeep Sarkar, Zongyi Liu. Gait Recognition. Pg. 503-506. Henk C.A. van Tilborg & Sushil Jajodia (eds.), Encyclopedia of Cryptography and Security, ISBN 9781441959065. © Springer Science+Business Media, LLC

[13] 2016-7-26. Black Hat: Iris scanners 'can be tricked' by hackers. Retrieved from http://www.bbc.com/news/technology-18997580

[14] https://en.wikipedia.org/wiki/Iris_recognition

[15] M. Lourde and D. Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, pp.852-855, October 2010. http://www.ijcee.org/papers/239-E576.pdf

[16] S. Crisam, "A Novel Perspective on Hand Vein Patterns for Biometric Recognition: Problems, Challenges, and Implementations". Biometric Security and Privacy, Signal Processing for Security Technologies pp.21-49, 2017.

[17] M. Szczepanik and I. Joswiak "Biometric Security Systems for Mobile Devices based on Fingerprint Recognition Algorithm", The Second International Conference on Advanced Communications and Computation, Wroclaw, Poland, pp.62-67, 2012.

[18] D. Thakkar, "Importance of Biometric Fingerprinting", https://www.bayometric.com/importance-of-biometric-fingerprinting-technology/

[19] O. Henniger, D. Scheuermann, and T. Kniess, "On security evaluation of fingerprint recognition systems", Fraunhofer Institute for Secure Information Technology, Germany. https://www.nist.gov/sites/default/files/documents/2016/11/30/henniger2_olaf_ibpc_paper.pdf

[20] R. Subban and D. Mankame, "A Study of Biometric Approach Using Fingerprint Recognition" in Lecture Notes on Software Engineering vol.1, no. 2 pp.209-213, May 2013. http://www.lnse.org/papers/47-IE0038.pdf

[21] sourceAFIS (Version 2.0) [Software]. Available from https://sourceafis.machinezoo.com/

[22] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: Fingerprint Verification Competition", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 3, pp. 402 - 411, 2002.

[23] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, "FVC2002: Second Fingerprint Verification Competition", Proc. International Conference on Pattern Recognition, pp. 811-814, Quebec City, August 11-15, 2002.

[24] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, "FVC2004: Third Fingerprint Verification Competition", Proc. International Conference on Biometric Authentication (ICBA), pp. 1-7, Hong Kong, July 2004.

[25] FVC2000 fingerprint competition databases available from http://bias.csr.unibo.it/fvc2000/

[26] FVC2002 fingerprint competition databases available from http://bias.csr.unibo.it/fvc2002/

[27] FVC2004 fingerprint competition databases available from http://bias.csr.unibo.it/fvc2004/

[28] The synthetic fingerprint generator, developed by the University of Bologna, can be found here http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=12&pathSubj=111%7C%7C12&Req=&