On the Current State of Cross-Domain Fingerprint Recognition

Steven A. Grosz
Michigan State University
428 S Shaw Ln, East Lansing, MI 48824
groszste@msu.edu

Joshua J. Engelsma
Amazon
440 Terry Ave N, Seattle, WA 98109
jengelsm@amazon.com

Anil K. Jain
Michigan State University
428 S Shaw Ln, East Lansing, MI 48824
jain@cse.msu.edu

Abstract

Fingerprint recognition has a long history in person identification with the state-of-the-art algorithms now achieving near perfect accuracy on public benchmarks, such as the NIST Fingerprint Vendor Technology Evaluation (FpVTE) and FVC-Ongoing competition. Nowadays, researchers have turned toward mitigating edge cases in which current fingerprint recognition algorithms may still fail. One such application is in cross-domain fingerprint recognition, where a single fingerprint recognition algorithm performs universally well across a wide range of sensor types and capture scenarios. In this paper, we leverage the recently released dataset NIST SD 302 to evaluate the current state-of-the-art in cross-domain fingerprint recognition, which contains fingerprint images captured across 18 different capture devices. The aim of this paper is to i.) establish a common and challenging evaluation protocol using currently public and easy to access datasets for evaluating fingerprint recognition algorithms and ii.) provide the research community with the current baseline performance in cross-domain fingerprint recognition using state-of-the-art algorithms. We make our performance results publicly available to encourage further research on this topic: `github.com/tba`*.*

1. Introduction

Since it's scientific origins in the late 19th century, fingerprints have continued to explode into many national and civil identity applications due to their inherent uniqueness and permanence, as originally pointed out in the seminal work titled "Finger Prints" by Sir Francis Galton published in 1982 [1] and further strengthened by evidence provided in follow-up studies such as [2] and [3]. Today, many of the top performing fingerprint recognition algorithms are able to achieve near perfect accuracy in con-

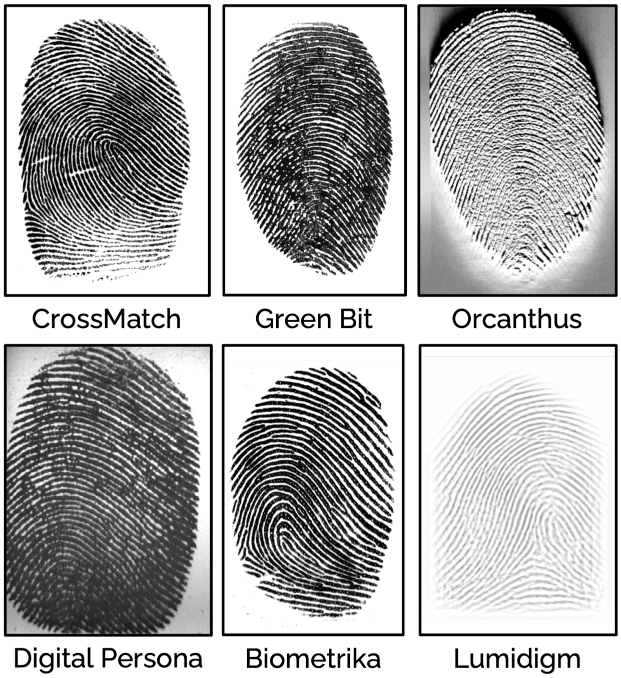

Figure 1: Example fingerprint images from various fingerprint readers: Green Bit, CrossMatch, Biometrika, Digital Persona, Orcanthus, and (f) Lumidigm. Matching fingerprint images captured across multiple different fingerprint readers is a challenging task due to starkly different visual characteristics, especially across different sensing modalities (e.g., thermal swipe, optical FTIR, etc.) but even across readers of similar type (e.g., Biometrika, CrossMatch, Digital Persona, and GreenBit; which all use FTIR imaging).

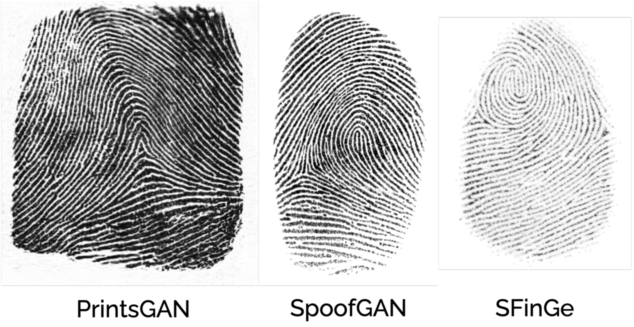

Figure 2: Example synthetic fingerprint images from PrintsGAN, SpoofGAN, and SFinGe.

trolled, organized competitions and performance evaluations, such as the NIST Fingerprint Vendor Technology Evaluation (FpVTE) and FVC-Ongoing competitions. As fingerprint recognition systems have continued to improve over the last century, researchers have turned to more challenging applications and capture scenarios to make fingerprint technology applicable to a wider array of use cases. Of these, cross-sensor fingerprint recognition is one of particular interest to practitioners of fingerprint recognition technology because it relieves the need to develop algorithms specific to every new type of fingerprint sensor that is developed or even perpetual upgrades to existing systems, which may render previous algorithms useless due to changes in captured image characteristics. Indeed, even subtle differences among fingerprint readers of the same type (e.g., frustrated total internal reflection (FTIR) optical readers, as is the case with GreenBit, Digital Persona, Biometrika, and CrossMatch) make cross-sensor fingerprint matching a difficult problem, let alone matching across sensing technology (e.g., optical FTIR vs. thermal swipe sensors like Orcanthus). For a visual comparison, example fingerprint images capture on six different fingerprint readers of varying types (optical FTIR, thermal swipe, and multi-spectral optical) are shown in Figure 1.

However, advancements in cross-sensor interoperability in fingerprint recognition has been limited due to growing concerns surrounding the privacy and use of biometric data. In fact, many previously public fingerprint datasets and benchmarks have been rescinded, limiting the ease of training and evaluating fingerprint algorithms. NIST SD14 and NIST SD27 are just two examples of fingerprint datasets which are no longer publicly available. This has motivated many researchers to develop synthetic fingerprint alternatives, such as PrintsGAN, SpoofGAN, and the classic SFinGe method to generate large-scale datasets to keep progress moving forward on developing more advanced fingerprint recognition algorithms. However, the utility of such synthetic generation methods is still limited and the domain gap to real fingerprint images remains quite large. Fortunately, NIST has recently released the NIST SD 302 database, which contains fingerprint images from 200 volunteers across 18 fingerprint capture devices. With this new database, it is now possible to evaluate cross-sensor fingerprint interoperability using fingerprint data that is currently publicly available and easily accessible to researchers developing new fingerprint recognition technologies. Still, there is not many alternative fingerprint datasets to choose from to develop and test new algorithms and the existing databases, such as LivDet and FVC, are not accessible to many institutions with more stringent Internal Review Board (IRB) data protection requirements. Therefore, in this work we establish a five-fold cross validation benchmark using the NIST SD 302 algorithm in hopes that it gives researchers the opportunity to train and test their algorithms on a cross-sensor fingerprint database which should be freely accessible to many institutions.

Concisely, our contributions for this report are as follows:

- Establish a common and challenging evaluation protocol using currently public and easy to access datasets for evaluating fingerprint recognition algorithms.
- Provide the research community with the current baseline performance in cross-sensor fingerprint recognition using state-of-the-art algorithms.

1.1. Datasets

The paucity of publicly available, large-scale fingerprint recognition datasets is a major limiting factor to development of next generation fingerprint recognition algorithms. However, recent advancements in synthetic data generation have now led to large-scale public releases of synthetic fingerprints, such as [4], [4], and [4] shown in Figure 2, which can successfully augment existing, real fingerprint datasets to achieve higher levels of accuracy. Therefore, in this work, we leverage the recently released PrintsGAN dataset in combination with a subset of NIST SD 302 for training and evaluate our trained algorithms on the remaining test partitions of NIST SD 302. Furthermore, there are many state-of-the-art fingerprint recognition algorithms in the literature, which have been previously trained on large, private databases of fingerprints which are not accessible to the public; as such, in order to best reflect the current state of the art in cross-sensor fingerprint recognition, we take two of these top performing algorithms, DeepPrint and a commercial system Verifinger v12.3 and evaluate/finetune these pretrained models on NIST SD 302 and report the state-of-the-art numbers.

The datasets used in this paper are summarized in Table 1, including statistics on the number of fingers, number

Table 1: Datasets used in this study.

Dataset	Type	Number of Fingers	Avg. Number of Impressions	Total Number of Images	Number of Train/Val/Test Fingers
PrintsGAN	Synthetic Rolled	34,985	15	539K	28,344 / 3,142 / 3,499
NIST SD 302	Plain and Rolled	2,000	12	25K	2,000 / 200 / 200
MSP	Rolled	37,420	12	448K	37,420 / 0 / 0

of impressions per finger, total number of fingerprint images, and number of fingers including in train, test, and validation splits of the data. Of these three datasets, PrintsGAN and NIST SD 302 are publicly available and we use these two datasets as the main datasets for training and evaluation of the state-of-the-art algorithms. However, we included the MSP dataset since the SOTA algorithm, DeepPrint, was originally proposed and trained on this large-scale, private dataset; therefore, we included results when using the MSP dataset for pretraining and subsequent finetuning on NIST SD 302.

1.2. Authentication Results

Due to the limited size of the NIST SD 302 dataset, we created five separate cross-validation splits of the dataset to more accurately report the performance of the algorithms in terms of average performance and associated standard deviation across the splits. We will also make the exact partition known to the public for easy comparison with future studies. For the authentication experiments, we computed genuine and imposter matches on the NIST SD 302 dataset and report the true accept rate (TAR) at a fixed False Accept Rate (FAR) of 0.01%, as well as the full Receiver Operating Characteristic (ROC) curve for the first test split of NIST SD 302. In particular, genuine scores are computed on the test partition via pairwise comparisons between all of the impressions of the same finger and imposter scores are computed by matching each fingerprint image of one finger to all other impressions of every other finger. Since the exact number of impressions per finger varies for each cross-validation split, the number of genuine and imposter comparison will vary between splits; however, for reference, $15,143$ genuine and $3,229,735$ imposter matches were computed for the test set of the first split of NIST SD 302.

The authentication results are shown in Table 2 as well as in the ROC plot in Figure 3. Verifinger's proprietary algorithm performs the best with a TAR of 96.71 @ FAR=0.1% across the five cross-validation test splits, followed by Verifinger's ISO matcher which achieved a TAR of 95.09%. DeepPrint pretrained on the large-scale MSP database and finetuned on NIST SD 302 achieved a TAR of 90.60% compared to the same model pretrained on PrintsGAN, which only achieved a TAR of 82.11%. Thus, it seems that the large-scale, private database makes a big difference in the performance of DeepPrint. This result motivates further research in improving synthetic fingerprint generators to synthesis better, more realistic fingerprint images to further reduce the domain gap to real fingerprints.

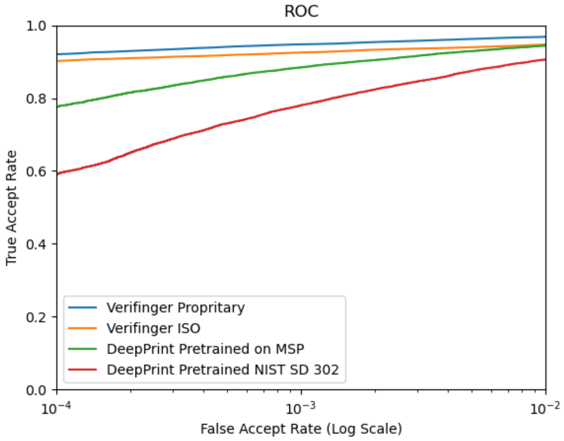

Figure 3: ROC.

1.3. Identification Results

For closed-set identification, we report the Rank-1 search performance for all the models. We again compute the performance across all five splits of NIST SD 302 and report the average and standard deviation in Table 2. In this case, Verifinger performs impressively well compared to DeepPrint, with the proprietary algorithm achieving rank 1 search accuracy of 99.80%. Furthermore, DeepPrint initially trained on MSP outperforms DeepPrint pretrained on PrintsGAN (99.34% to 91.62%).

2. Conclusion

In this technical report, we established a common benchmark for cross-sensor interoperability for fingerprint recognition using the recently release NIST SD 302 dataset which contains fingerprint images across 18 different fingerprint readers for 200 (2,000 unique finger) volunteer subjects. We

Table 2: Authentication and closed-Set identification performance on NIST SD 302.

Model	Train Dataset	Number of Parameters	Inference Speed (Nvidia Tesla V100-SXM2=16GB)	TAR (%) @ 0.1% FAR	Rank 1(%)
Verifinger proprietary matcher	N/A	N/A	640ms[1]	96.71 ± 1.16	99.80 ± 0.27
Verifinger ISO matcher	N/A	N/A	640ms[1]	95.09 ± 1.59	99.80 ± 0.27
DeepPrint	Pretrained on MSP, finetuned on NIST SD 302	76.93M	40.4ms	90.60 ± 1.72	94.34 ± 1.13
DeepPrint	Pretrained on PrintsGAN, finetuned on NIST SD 302	76.93M	40.4ms	82.11 ± 2.96	90.45 ± 1.13

[1] 600ms for template extraction and 40ms for matching on at least an Intel Core 7-8xxx family processor.

also released authentication and identification (both closed-set and open-set) performance results using four state-of-the-art fingerprint recognition algorithms (DeepPrint pretrained on MSP and finetuned on N2N, DeepPrint pretained on PrintsGAN and finetuned on N2N, Verifinger ISO Minutiae Matcher, and Verifinger Proprietary Fingerprint Matcher).

References

[1] F. Galton, *Finger prints*. Macmillan and Company, 1892.

[2] S. Yoon and A. K. Jain, “Longitudinal study of fingerprint recognition,” *Proceedings of the National Academy of Sciences*, vol. 112, no. 28, pp. 8555–8560, 2015.

[3] S. Pankanti, S. Prabhakar, and A. K. Jain, “On the individuality of fingerprints,” *IEEE Transactions on pattern analysis and machine intelligence*, vol. 24, no. 8, pp. 1010–1025, 2002.

[4] J. J. Engelsma, S. A. Grosz, and A. K. Jain, “Printsgan: Synthetic fingerprint generator,” *arXiv preprint arXiv:2201.03674*, 2022.