

Altered Fingerprints: Detection and Localization

Elham Tabassi, Tarang Chugh, Debayan Deb, and Anil K. Jain

Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824

E-mail:{tabassie, chughtar, debdebay, jain}@cse.msu.edu

Abstract

Fingerprint alteration, also referred to as obfuscation presentation attack, is to intentionally tamper or damage the real friction ridge patterns to avoid identification by an AFIS. This paper proposes a method for detection and localization of fingerprint alterations. Our main contributions are: (i) design and train CNN models on fingerprint images and minutiae-centered local patches in the image to detect and localize regions of fingerprint alterations, and (ii) train a Generative Adversarial Network (GAN) to synthesize altered fingerprints whose characteristics are similar to true altered fingerprints. A successfully trained GAN can alleviate the limited availability of altered fingerprint images for research. A database of 4,815 altered fingerprints from 270 subjects, and an equal number of rolled fingerprint images are used to train and test our models. The proposed approach achieves a True Detection Rate (TDR) of 99.24% at a False Detection Rate (FDR) of 2%, outperforming published results. The synthetically generated altered fingerprint dataset will be open-sourced.

1. Introduction

Fingerprints have been used to identify individuals for more than a century [1]. Being one of the most reliable biometrics, it has been used by law enforcement and forensic laboratories for background checks, booking suspects, and crime scene investigations. In addition, homeland security agencies deploy Automated Fingerprint Identification Systems (AFIS) for watch list comparisons of passengers arriving at ports of entry and national registry systems for deduplication before issuing an ID. While state of the art AFIS are quite accurate and robust [2], their recognition accuracy drops when they encounter noisy fingerprint images whose friction ridges are degraded or destroyed. Intentional or unintentional destruction of friction ridge patterns, degrades the information content of a fingerprint image and therefore increases the error rate of an AFIS. Intentional fingerprint alteration, known as “altered fingerprints” (see Fig. 1), are attempted in hope of obfuscating the true identity to evade

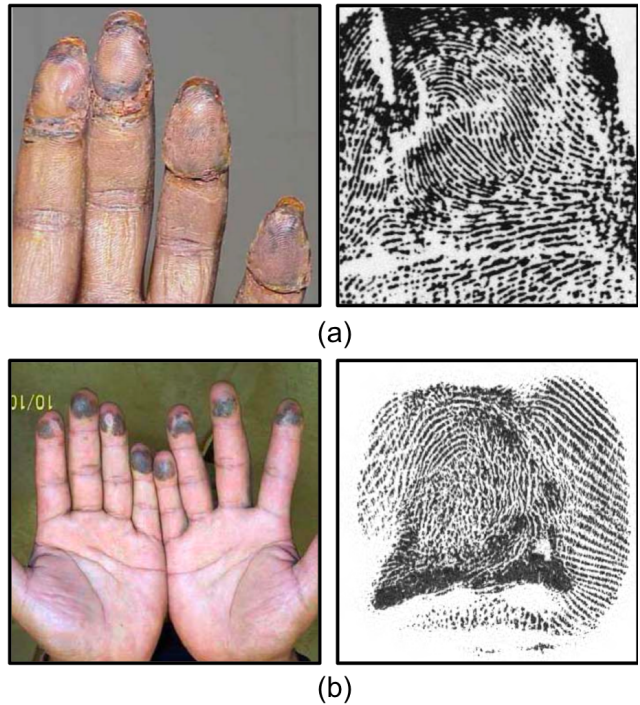


Figure 1: Example images of altered fingerprints. (a) Transplanted friction ridge skin from sole, and (b) fingers that have been bitten. Source: [4].

law enforcement and is a threat to AFIS [3].

The first recorded observation of finger tip skin transplant is by Galton who in 1896 reported his findings in a “casual” graft of ridged skin. A man had been cutting cardboard with a sharp knife and cut his skin. A piece of skin was inadvertently sliced off. This piece was immediately applied to the wound and tightly bandaged. Examination of the injury (30 years later!) showed that the slip of skin had been successfully engrafted, though replaced at right angles to its original direction, as shown by the alignment of ridges [10]. Cases of tampering with fingerprints to evade detection in criminal cases were reported as early as 1935. Cummins [10] reported 3 cases of fingerprint alterations and

Table 1: Related and previous work on altered fingerprint detection.

Source	Method	Dataset	Performance
Feng, Jain and Ross [5]	orientation field	1,976 simulated altered fingerprints	92% detection rate at false positive rate of 7%
Tiribuzi et al. [6]	minutiae density maps and orientation entropies	1000 genuine and synthetic altered fingerprints	90.4% classification accuracy
Yoon et al. [7, 4]	orientation field and minutiae distribution	4, 433 operational altered fingerprints from 270 subjects	70.2% detection rate at false positive rate of 2.1%
Ellingsgaard and Busch [8, 9]	orientation field and minutia orientation	116 altered and 180 unaltered from various sources	92.0% detection rate at false positive rate of 2.3%
Proposed Approach	input image and minutiae-based patches; CNN models	4,815 altered and 4,815 valid fingerprints from 270 subjects	99.24% detection rate at false positive rate of 2%

presented images of before and after alterations. In 2018, Business Insider reported that like many of the FBI’s most wanted criminals, Eduardo Ravelo, who was added to the FBI’s 10 Most Wanted list in October 2009, was believed to have had plastic surgery to alter his fingerprints to evade authorities [11]. In recent years, border crossing applications have been targeted by altered fingerprint attacks. In 2009, ABC news reported that Japanese officials arrested “a Chinese woman who took a particularly extreme measure to evade detection” [12]. The Chinese woman had paid a plastic surgeon to swap fingerprints from her right and left hands. Patches of skin from her thumbs and index fingers were reportedly removed and then grafted onto the ends of fingers on the opposite hand. As a result, her identity was not detected when she re-entered Japan illegally. In 2014, the FBI identified 412 records in its IAFIS which indicated deliberate fingerprint alterations [13].

Detection of altered fingerprints is of high interest to law enforcement and homeland security agencies. This paper proposes deep learning based approaches to classify input fingerprint images into two classes: valid or altered fingerprints, and to localize the regions of a fingerprint that is altered. This can be broadened to assessing the *fingerprintness* of an input image [4], such that valid fingerprints, or valid region of fingerprints, shall produce high scores and altered fingerprints, or altered portion of fingerprints shall produce low or zero scores.

The organization of the paper is as follows: Previous works are outlined in Section 2. Section 3 describes the operational valid and altered fingerprints that were used for training and testing of our network models. Models are explained in Section 4, along with our synthetic altered fingerprint generation algorithm. Results are presented in Section 5, and finally conclusions and future work are discussed in Section 6.

2. Related work

Existing approaches for detecting fingerprint alteration have primarily explored hand crafted features to distinguish between altered and valid fingerprints. Feng et al. [5]

trained an SVM to detect irregularities in ridge orientation field; evaluated their method on 1,976 simulated altered fingerprints; and reported a 92% detection rate at a false positive rate of 7%. Tiribuzi et al. [6] combined the minutiae density maps and the orientation entropies of the ridge-flow in order to identify the altered fingerprints. They reported a 90.4% classification accuracy on a dataset of 1,000 genuine and synthetic altered fingerprints. Yoon et al. [7, 4] utilized the orientation field and minutiae distribution to detect altered fingerprints. Their method was tested on a database of 4,433 altered fingerprints from 270 subjects, providing for 70.2% correctly identified altered fingerprints at a false positive rate of 2.1%. Ellingsgaard and Busch in [8, 9] discuss methods for automatically detecting altered fingerprints based on analyses of two different local characteristics of a fingerprint image: identifying irregularities in the pixel-wise orientations, and examining minutia orientations in local patches. They further suggest that alteration detection should be included into standard quality measures of fingerprints. Beyond detection of altered fingerprint, Yoon and Jain [14] investigated feasibility of a state-of-the-art commercial fingerprint matcher to link altered fingerprints to their pre-altered mates.

Table 1 summarizes previous work in altered fingerprint detection. All these methods are based on examining irregularities in orientation flow or minutia maps based on hand crafted features. Our approach differs from the previous works by using a deep learning technique to learn and evaluate salient features.

Research on altered fingerprint detection has been constrained with limited availability of data and lack of public domain altered fingerprint datasets. Furthermore, because previous works each used a different dataset, comparing their results is not feasible. To alleviate this problem, we propose a method to generate synthetic altered fingerprints.

3. Altered Fingerprint Dataset

An operational dataset of 4,815 altered fingerprints, from 635 tenprint cards of 270 subjects, acquired from law enforcement agencies is utilized in this study. The num-




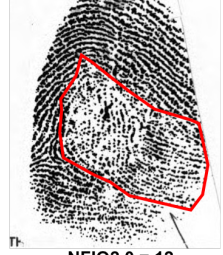
	Valid	Altered
Train	 NFIQ2.0 = 64	 NFIQ2.0 = 7
Test	 NFIQ2.0 = 76	 NFIQ2.0 = 12

Figure 2: Example of altered and valid fingerprint images used for training and testing in one of the five folds. The altered region is highlighted in red. The NFIQ 2.0 quality scores are also presented for each image; the larger NFIQ 2.0 score, the higher fingerprint quality. The NFIQ 2.0 quality scores ranges between [0, 100].

ber of tenprint cards per subject varies from 1 to 16 due to multiple encounters. However, not all 10 fingerprint images in a tenprint card may be altered. The number of altered fingerprint instances per subject varies from 1 to 137. Another operational dataset of 4, 815 rolled fingerprint images is used for valid fingerprints. Fingerprint images in both sets of altered and valid are images collected as part of law enforcement operations. All images are 8-bits gray scale. A five-fold cross-validation is employed where in each of the five folds, the training set contains 3, 852 altered and 3, 852 valid fingerprints. The testing set in each fold contains the remaining 963 altered and 963 valid fingerprints, such that the train and test sets are disjoint. Figure 2 shows sample altered and valid images used for training and testing in one of the five folds.

4. Proposed Approach

4.1. Altered Fingerprint Detection

The goal of this study is to detect altered fingerprint images. This can be formulated as a binary classification problem with two classes; *altered* and *valid*. A more sophisticated model would be a multi-class classification that detects the type of alteration, when valid fingerprint has a type “none”. As shown in Figure 3, different types of alteration







Obliteration	Distortion	Imitation
 Scar NFIQ 2.0 = 46	 Transplantation with Z-Cut NFIQ 2.0 = 28	 Removal of portion of skin NFIQ 2.0 = 35
 Mutilation NFIQ 2.0 = 13	 Transplantation from other friction ridge, e.g. palm NFIQ 2.0 = 20	 Transplantation to match ridge pattern NFIQ 2.0 = 42

Figure 3: Types of fingerprint alterations: (i) Obliteration, such as scars, or mutilations, (ii) Distortion, *i.e.* friction ridge transplantation to distort friction ridge area, and (iii) Imitation, *i.e.* transplantation or removal of friction ridge skin while still preserving fingerprint like pattern.

procedures would result in different fingerprint degradation. Different types of alteration procedures and their effect on friction ridge pattern are discussed in [4] and [8]. Based on the changes made to friction ridge patterns, they categorized altered fingerprints into three types: *obliteration*, *distortion*, and *imitation*.

Obliteration consists of abrading, cutting, burning, applying strong chemicals, or transplanting friction ridge skin. Skin disease or side effects of drugs can also obliterate fingertips. *Distortion* comprises of cases of using plastic surgery to convert normal friction ridge pattern into unusual ridge pattern. Some portions of skin are removed from the finger and grafted back onto a different position causing an unusual pattern. *Imitation* is when surgical procedure is performed in such a way that the altered fingerprints appear as natural fingerprints, for example, by grafting skin from the other hand or a toe onto a large or perhaps the entire finger tip skin such that fingerprint ridge pattern is still preserved. While there are distinct alteration types, and despite Yoon and Jain’s [4] suggestion to develop different models for different alteration types, we propose to utilize a single model for the following two reasons: a) insufficient data for each alteration type for training deep networks, and b) manual labeling of the alteration type would be subjective because an image can suffer from more than one alteration type. We trained a Convolutional Neural Network (CNN) to classify an input fingerprint image into one of the two classes of valid or altered. Data augmentation techniques,

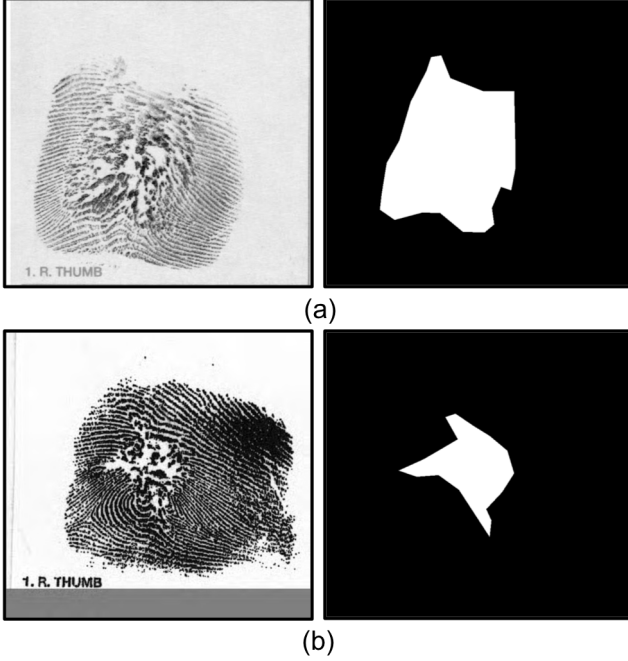


Figure 4: Examples of altered fingerprints and corresponding manually marked regions of interest (ROI) circumscribing the areas of fingerprint alterations. Local patches overlapping with manually marked ROI are labelled as altered patches, while the rest are labelled as valid. The test phase is fully automatic and does not require any manual markup.

such as mirroring, random cropping, and rotation have been employed to increase the size of the training data.

4.2. Altered Fingerprint Localization

To localize and highlight the altered regions of fingerprints, we augment our whole image based altered fingerprint detection with a patch-based approach. Our approach is as follows: First, region of interest (ROI) is manually marked for 1,182 randomly selected altered fingerprints from our database of 4,815 altered fingerprints. See Figure 4. Next, local patches of size 96×96 centered around each extracted minutia are cropped. Local patches with more than 50% overlap with the manually marked ROI are labelled as altered patches, and the remaining patches are labelled as valid. Because a majority of fingerprint alterations generate discontinuities and noisy regions in the friction ridge pattern, a much higher number of spurious minutiae are generated in altered fingerprints compared to valid fingerprints of the same size [4]. Local patches centered around minutiae have also shown to provide superior performance in fingerprint spoof detection compared to patches extracted in a raster scan manner [15]. A total of 81,969 valid and 89,979 altered patches are extracted and utilized

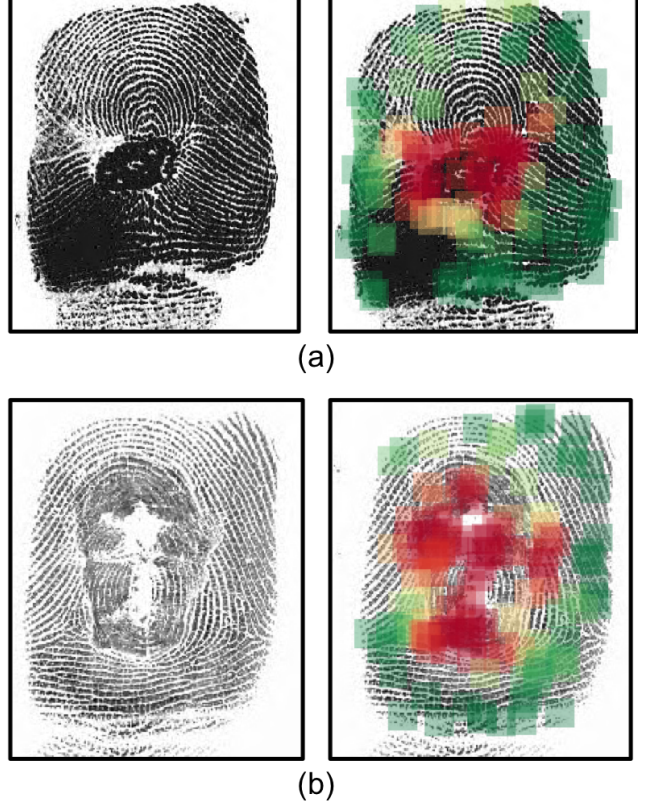


Figure 5: Examples of altered fingerprint localization by our proposed method. Local regions highlighted in red represent the altered portion of the fingerprint, whereas regions highlighted in green reflect the valid friction ridge area.

for training two different networks: Inception-v3 [16] and MobileNet-v1 [17]. Fig. 5 presents examples of altered fingerprint localization output by the proposed approach. An overview of the proposed approach to detect and localize altered fingerprints is presented in Figure 6.

4.3. Fingerprint image quality analysis

Figure 7 shows distribution of NFIQ 2.0 [18, 19] scores for the altered and valid fingerprint images used in this study. NFIQ 2.0 software reads a fingerprint image, computes a set of quality features from the image, and uses these features to predict the utility of the image as an integer score between 0 and 100. About 75% of altered fingerprints have a NFIQ 2.0 score of 40 or lower, and only 10% of images have a NFIQ 2.0 score larger than 50. The median NFIQ 2.0 score is 23 for altered fingerprints, and 48 for valid. This suggests that NFIQ 2.0 may be suited to detect altered fingerprints.

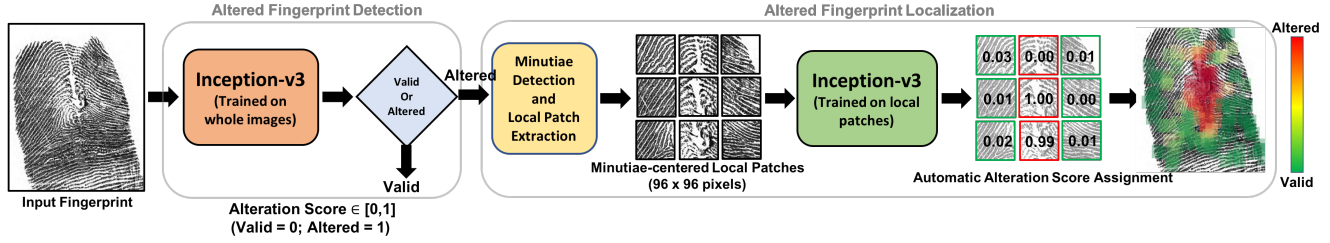


Figure 6: An overview of the proposed approach for detection and localization of altered fingerprints. We trained two convolutional neural networks (Inception-v3 and Mobilenet-v1) using full fingerprint images and local patches of images where patches are centered on minutiae locations.

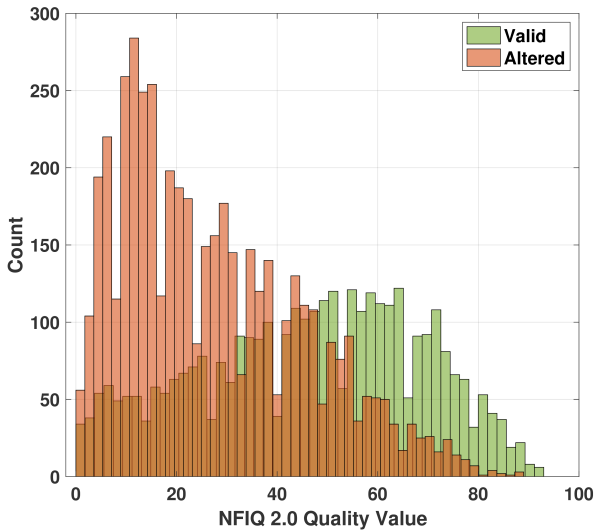


Figure 7: Histogram of NFIQ 2.0 quality scores for valid (green) and altered (red) fingerprint images. Approximately, 75% of altered fingerprint images have a NFIQ 2.0 score of 40 or lower, and only 10% of altered dataset has a NFIQ 2.0 score of larger than 50. The median NFIQ 2.0 score for altered fingerprint images is 23, while median NFIQ 2.0 score for valid fingerprint images is 48. This suggests NFIQ 2.0’s suitability for detecting altered fingerprints, particularly for cases of fingerprint obliteration.

4.4. Deep learning for detecting altered fingerprints

Using the code in [20], we were able to train MobileNet-v1 [17] and Inception-v3 [16] networks as binary classifiers (altered vs. valid fingerprints). The input is a full fingerprint image and the output is a probability (or score) of belonging to Altered or Valid class, referred to as *alteration score*. A valid fingerprint image should result in an alteration score of close to 0, whereas an altered fingerprint image should result in an alteration score of close to 1. The network hyper-parameters used to train the CNN models are presented in

Table 2: Network hyper-paramters utilized in training CNN and GAN models.

Hyper-parameters	Inception-v3	MobileNet-v1	DC-GAN
Batch Size	32	100	64
Optimizer	RMSProp	RMSProp	Adam
Learning Rate	[0.01 - 0.0001]; exp. decay 0.94	[0.01 - 0.0001]; exp. decay 0.94	0.0002
Momentum	0.9	0.9	0.5
Iterations	25,000	25,000	1,350

Table 2.

4.5. Generating synthetic altered fingerprints

One major constraint of studies on altered fingerprint detection is the limited amount of altered fingerprint images available. This limitation is perhaps the cause of relatively few investigations on this topic. To remedy the issue of limited available data, we trained a Generative Adversarial Networks (GAN) that generates altered fingerprints. We used the DC-GAN architecture¹ proposed in [21]. See Figure 8. We utilized all of the 4,815 altered fingerprint images for training by cropping them to 512×512 pixels. The trained model outputs 256×256 synthetic altered fingerprint images². The network hyper-parameters used to train the GAN model are presented in Table 2.

Generation of synthetic altered fingerprint is a related but separate topic than detection of altered fingerprint as discussed in Section 4.4. Our motivation was to investigate ways to remedy the lack of publicly available altered fingerprint data for research.

5. Experimental Results

5.1. Altered fingerprint detection and localization

Figure 9 shows the Receiver Operating Characteristic (ROC) curves for the proposed altered fingerprint detec-

¹<https://github.com/carpedm20/DCGAN-tensorflow>

²To avoid the fast convergence of the discriminator network, the generator network is updated twice for each discriminator network update

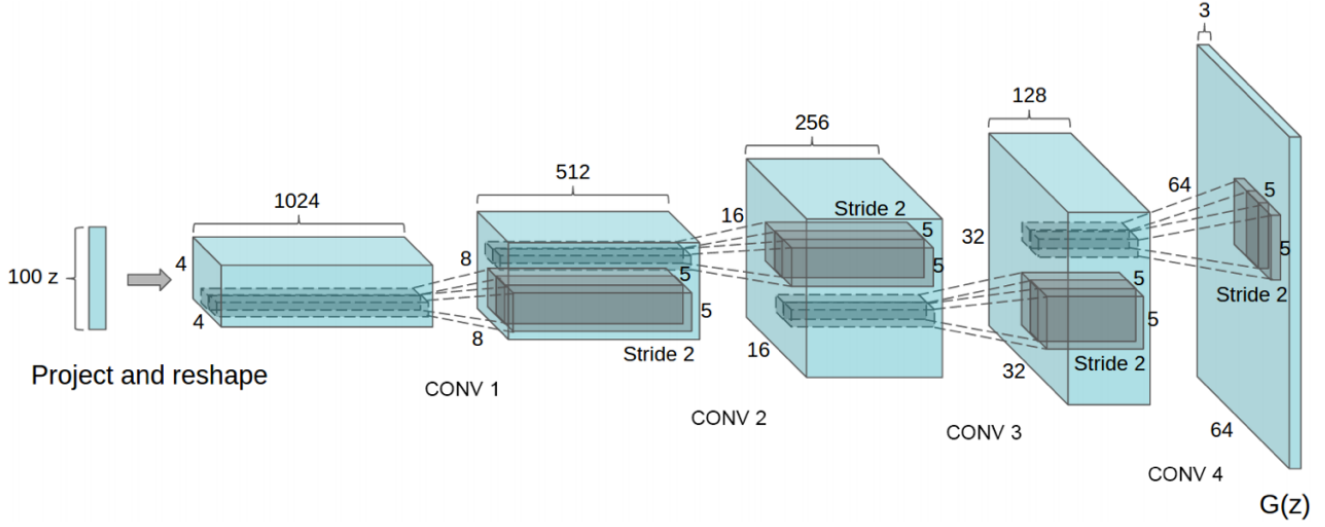


Figure 8: Architecture of DC-GAN used to generate synthetic altered fingerprint images. Source: Radford, et al. [21].

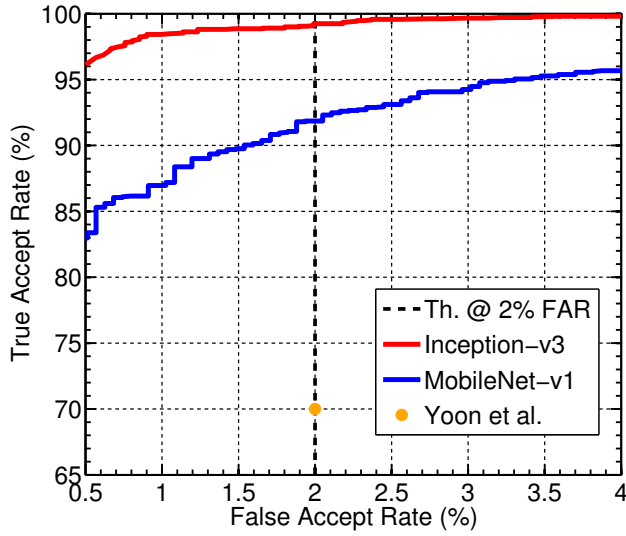


Figure 9: Performance curves for the proposed altered fingerprint detection approach utilizing Inception-v3 and MobileNet-v1 CNN models. Yoon et al. [4] (baseline) achieved a TDR of 70% @ FDR = 2% on 4,433 altered fingerprints, while the proposed approach achieves a TDR (over five folds) of $99.24\% \pm 0.58\%$ @ FDR = 2% on 4,815 altered fingerprints.

tion approach (Inception-v3 and MobileNet-v1) compared with state-of-the-art [4]. The red curve shows the accuracy of the Inception-v3 implementation and the blue curve shows the accuracy of the MobileNet-v1 implementa-

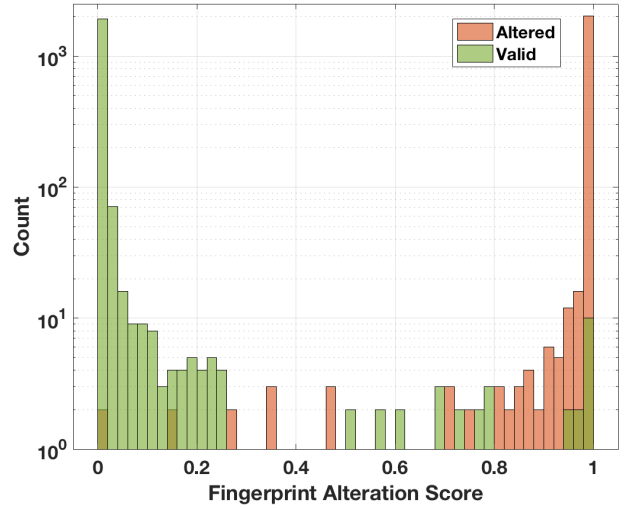


Figure 10: Alteration score histograms for valid and altered fingerprints obtained by the proposed approach using the best performing Inception-v3 model. The small overlap between the valid and altered score distributions is an indication of high discrimination power of the model. Note that the Y-axis is presented in log scale.

tion. Inception-v3 outperforms MobileNet-v1 architecture ($\sim 99\%$ to $\sim 92\%$), while the computational requirement³ for MobileNet-v1 (6 ms) is almost 10 times lower compared to time required by the Inception-v3 architecture (50 ms).

³We utilized NVIDIA GTX 1080 Ti GPU to run our implementation of Inception-v3 and MobileNet-V1 based altered fingerprint detection.





		Output	
		Valid	Altered
Ground Truth	Valid	 <p>Alteration Score: 0.0 (a)</p>	 <p>Alteration Score: 0.78 (b)</p>
	Altered	 <p>Alteration Score: 0.31 (c)</p>	 <p>Alteration Score: 0.98 (d)</p>

Figure 11: Example classifications and their alteration scores output by the proposed approach. (a) and (d) present correctly classified images, while (b) and (c) present incorrect classifications. (b) a valid fingerprint that receives a high alteration score primarily due to the noisy region on the right. (c) contains a small region of alteration which is similar to the noise present in valid fingerprints.

The superior performance of Inception-v3 over Mobilenet-v1 network can be attributed to (i) deeper convolutional network providing higher discrimination power, and (ii) larger input image size; 299×299 for Inception-v3, compared to 224×224 for Mobilenet-v1. Both network models show better detection performance than Yoon and Jain [4] which had a true detection rate of only 70.2% at a false positive rate of 2%. Figure 10 shows the histograms of scores produced by our Inception-v3 model for valid and altered fingerprint images. The very small overlap of the two distributions is an indication of the high accuracy of our model. We further investigated the images that were incorrectly labeled by our model according to the ground truth labels given at the time of training. Our visual inspection of these images suggests that some of images labeled as valid, look like altered fingerprints. This might be either due to intentional alteration or cases of poor quality where fingerprint characteristics are degraded because of age or occupation (bricklayers, for example, are known to have poor quality fingerprints because their skin is severely damaged). On the other hand, some of the images labeled as altered, have a relatively small portion of the image as altered and most parts of

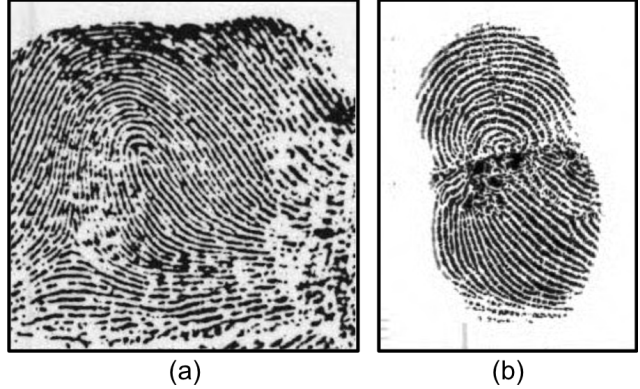


Figure 12: Example images with possible groundtruth labeling error. (a) Incorrectly labeled as altered, and (b) incorrectly labelled as valid. The Inception-v3 model outputs an alteration score of 0.20 and 0.97 for (a) and (b), respectively, indicating (a) as valid and (b) as altered.

the image look valid. If our model classifies these so called altered fingerprints as valid fingerprint images, it may not be far from truth. Example images of correct and incorrect classification by the Inception-v3 model are shown in Figure 11 along with the scores generated by our model. Examples of incorrect groundtruth label are shown in Figure 12.

To evaluate the localization of fingerprint alterations, a two-fold cross validation is performed. Two Inception-v3 networks are trained using 81,969 valid and 89,979 altered patches, achieving an average EER of 8.5%.

5.2. Generating synthetic altered fingerprints

A total of 4,060 synthetic altered fingerprint images are generated using the GAN model discussed in Section 4.5. Figure 13 presents example images of synthetically generated altered fingerprints, compared with operational fingerprint images. The distribution of NFIQ 2.0 quality scores for synthetically generated altered, operational altered, and valid fingerprint images are shown in Figure 14. The NFIQ 2.0 score distribution of synthetically generated altered fingerprints have large overlap with the distribution of operational altered fingerprints. The mean NFIQ 2.0 quality score for synthetic altered, altered, and valid fingerprint images are 11, 27, and 46, respectively. The low NFIQ 2.0 quality scores for synthetic altered fingerprint images can be attributed to the noisy friction ridge structure mimicked by the GAN, as well as the low resolution of the GAN output. As the training dataset is limited, a lower resolution for synthetic altered fingerprints is selected to avoid over-fitting. The synthetic altered fingerprint images are 256×256 pixels, while the operational altered fingerprint images are 750×800 pixels. This generator is our first at-

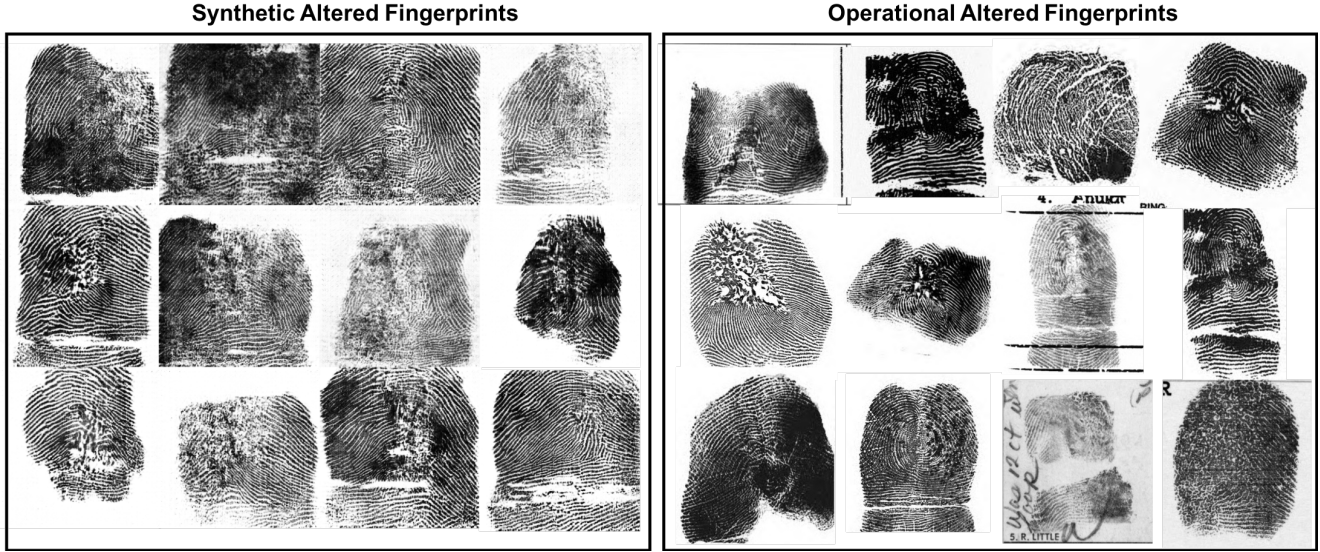


Figure 13: Example images of synthetic altered fingerprint images generated by the proposed GAN, compared to the operational altered fingerprint images.

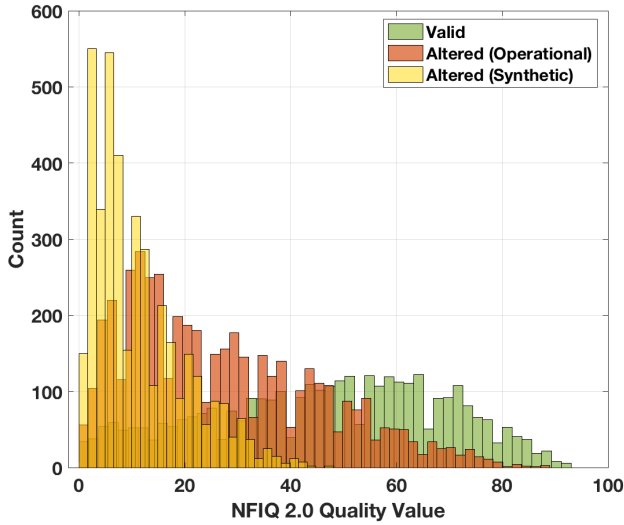


Figure 14: NFIQ 2.0 quality score distributions for 4,060 synthetically generated altered (yellow), 4,815 altered (red), and 4,815 valid fingerprint images (green). The mean NFIQ 2.0 quality scores for synthetic altered, operational altered, and operational valid fingerprint images are 11, 27, and 46, respectively.

tempt at solving the limited availability of altered fingerprint datasets, and requires further refining to match the characteristics between generated and true altered fingerprints, which we will pursue as a future work.

6. Conclusions and Future work

A robust and accurate method for altered fingerprint detection is critical to ensure the security of widely deployed AFIS in a variety of government and commercial applications. In this study, we have trained a CNN model using operational datasets of 4,815 altered and 4,815 valid fingerprint images for altered fingerprint detection. Additionally, we trained another model using minutia-centered local patches to automatically localize the regions of fingerprint alterations. Our altered fingerprint detection model achieves a True Detection Rate (TDR) of 99.24% @ False Detection Rate (FDR) of 1%, compared to the previous state-of-the-art result of TDR = 70% at FDR = 2% which used a smaller operational dataset. Finally, we trained a GAN, using the operational altered fingerprint database, to generate synthetic altered fingerprint images with similar characteristics as that of operational database. The synthetically generated altered fingerprint database will be open-sourced to alleviate the limited availability of altered fingerprint database and encourage further research on this topic.

In future, we plan to perform an analysis of pre- and post-altered fingerprint images of the same finger to benchmark the effect of alteration on recognition accuracy. We will also refine the GAN network to improve the characteristics of synthetic altered fingerprints, control the type of alteration, and use fingerprint comparison scores to assess the goodness of fit for our proposed synthetic altered fingerprint generation model.

References

- [1] A. K. Jain, K. Nandakumar, and A. Ross, "50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2016. [1](#)
- [2] C. Watson, G. Fiumara, E. Tabassi, S. L. Chang, P. Flanagan, and W. Salamon, "Fingerprint Vendor Technology Evaluation," 2015. NIST Interagency Report 8034. [1](#)
- [3] "Altered Fingerprints: A Challenge to Law Enforcement Identification Efforts," 2015. www.crime-scene-investigator.net/altered-fingerprints.html. [1](#)
- [4] S. Yoon, J. Feng, and A. K. Jain, "Altered fingerprints: Analysis and detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 34, no. 3, pp. 451–464, 2012. [1](#), [2](#), [3](#), [4](#), [6](#), [7](#)
- [5] J. Feng, A. K. Jain, and A. Ross, "Detecting Altered Fingerprints," in *20th International Conference on Pattern Recognition*, pp. 1622–1625, Aug 2010. [2](#)
- [6] M. Tiribuzi, M. Pastorelli, P. Valigi, and E. Ricci, "A multiple kernel learning framework for detecting altered fingerprints," in *21st International Conference on Pattern Recognition (ICPR)*, pp. 3402–3405, 2012. [2](#)
- [7] S. Yoon and A. K. Jain, "Is there a fingerprint pattern in the image?," in *International Conference on Biometrics (ICB)*, pp. 1–8, 2013. [2](#)
- [8] J. Ellingsgaard and C. Busch, "Altered Fingerprint Detection," *Handbook of Biometrics for Forensic Science*, pp. 85–123, 2017. [2](#), [3](#)
- [9] J. Ellingsgaard, C. Sousedik, and C. Busch, "Detecting fingerprint alterations by orientation field and minutiae orientation analysis," in *2nd International Workshop on Biometrics and Forensics*, pp. 1–6, March 2014. [2](#)
- [10] H. Cummins, "Attempts to alter and obliterate finger-prints," *Journal of Criminal Law and Criminology*, vol. 25, no. 12, 1935. [1](#)
- [11] "These are the fugitives on the fbi's 10 most wanted list," 2018. <http://www.businessinsider.com/fbi-10-most-wanted-criminals-list-2017-11>. [2](#)
- [12] "Surgically Altered Fingerprints Help Woman Evade Immigration," 2009. abcnews.go.com/Technology/GadgetGuide/surgically-altered-fingerprints-woman-evade-immigration/story?id=9302505. [2](#)
- [13] "Fbi warns about altered fingerprints," 2015. www.forensicmag.com/article/2015/05/fbi-warns-about-altered-fingerprints. [2](#)
- [14] S. Yoon, Q. Zhao, and A. K. Jain, "On Matching Altered Fingerprints," *International Conference on Biometrics (ICB)*, pp. 222–229, 05 2012. [2](#)
- [15] T. Chugh, K. Cao, and A. K. Jain, "Fingerprint Spoof Buster: Use of Minutiae-centered Patches," *IEEE Transactions on Information Forensics and Security*, 2018. [4](#)
- [16] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2818–2826, 2016. [4](#), [5](#)
- [17] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications," 2017. arxiv.org/abs/1704.04861. [4](#), [5](#)
- [18] E. Tabassi, "NIST Fingerprint Image Quality, NFIQ 2.0," 2016. <https://www.nist.gov/services-resources/software/development-nfiq-20>. [4](#)
- [19] "Information Technology – Biometric Sample Quality – Part 4: Finger Image Data," 2017. <https://www.iso.org/standard/62791.html>. [4](#)
- [20] "Tensorflow Slim (TF-Slim) Library." <https://github.com/tensorflow/models/tree/master/research/slim>. [5](#)
- [21] A. Radford, L. Metz, and S. Chintala, "Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks," *CoRR*, vol. abs/1511.06434, 2015. [5](#), [6](#)