

Graduate Theses, Dissertations, and Problem Reports

2021

Deep Fingerprint Matching from Contactless to Contact Fingerprints for Increased Interoperability

Alexander James Wilson West Virginia University, axwilson@mix.wvu.edu

Follow this and additional works at: https://researchrepository.wvu.edu/etd

Part of the Artificial Intelligence and Robotics Commons

Recommended Citation

Wilson, Alexander James, "Deep Fingerprint Matching from Contactless to Contact Fingerprints for Increased Interoperability" (2021). *Graduate Theses, Dissertations, and Problem Reports.* 10186. https://researchrepository.wvu.edu/etd/10186

This Thesis is protected by copyright and/or related rights. It has been brought to you by the The Research Repository @ WVU with permission from the rights-holder(s). You are free to use this Thesis in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses you must obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/ or on the work itself. This Thesis has been accepted for inclusion in WVU Graduate Theses, Dissertations, and Problem Reports collection by an authorized administrator of The Research Repository @ WVU. For more information, please contact researchrepository@mail.wvu.edu.

Deep Fingerprint Matching from Contactless to Contact Fingerprints for Increased Interoperability

Alexander Wilson

Thesis submitted to the Benjamin M. Statler College of Engineering and Mineral Resources at West Virginia University in partial fulfillment of the requirements

for the degree of

Master of Science

In

Computer Science

Nasser Nasrabadi, Ph. D., Chair Gianfranco Doretto, Ph. D. Jeremy Dawson, Ph. D. Omid Dehzangi, Ph. D. Department of LCSEE Friday, October 11, 2020

Lane Department of Computer Science and Electrical Engineering

Morgantown, West Virginia 2021

Keywords: Fingerprints, Neural Network, Fingerprint Reconstruction Copyright ©2021 Alexander Wilson

Abstract

Deep Fingerprint Matching from Contactless to Contact Fingerprints for Increased Interoperability

Alexander Wilson

Contactless fingerprint matching is a common form of biometric security today. Most smartphones and associated apps now let users opt into using this form of biometric security. However, it's difficult to match a finger-photo to a fingerprint because of perspective distortion occurring at the edges of the finger-photo, so direct matching using conventional methods will not be as accurate due to a lack of sufficient matching minutiae points. To address this issue, we propose a deep model, Perspective Distortion Rectification Model (PDRM), to estimate the fingerprint correspondence for finger-photo images in order to recover more minutiae points. Not only do we determine the feasibility of matching synthesized fingerprints from finger-photos, but we also show that matching a finger-photo to a fingerprint directly is possible by using our proposed Coupled Generative Adversarial Network (CpGAN) verifier. The results from our PDRM show that our method for creating synthetic fingerprints from finger-photos provides a more accurate matching (AUC=96.4%, EER= 8.9%) than just using the same commercial matcher to match finger-photo and fingerprints directly (AUC=92.1%, EER=15.7%). Finally, our proposed CpGAN verifier provides the best matching accuracy with AUC=98.4% and EER=6.3%.

Table of Contents

Chapter 1:	Introduction1				
Introductio	n				
Contributio	ons				
Related Wo	ork5				
Outline					
Chapter 2:	Proposed Method				
Proposed N	10 fethod				
Generative	Adversarial Network				
Perspective	Distortion Rectification Method 12				
Coupled G	enerative Adversarial Network (CpGAN) 14				
MinutiaeNo	et16				
Chapter 3:	Loss Functions				
Contrastive	2 Loss				
Adversaria	Adversarial Loss				
L2 Reconst	ruction Loss				
Total Losse	es				
Chapter 4:	Details and Experiments				
Experimen	tal Details				
Dataset					
Implementa	ation Details				
PDRM Architecture					
CpGAN	Architecture				
Minutiae	Net				
Chapter 5:	Results and Evaluation				
Evaluation.					
Chapter 6:	Conclusion and Future Work				
Conclusion					
Future Work					
References					

List of Tables

List of Figures

Figure 1: (Top Left) Contactless finger-photo. (Bottom Left) Ground truth fingerprint. (Top Right)
Synthetic fingerprint from only pix2pix module of PDRM. (Bottom Right) Synthetic fingerprint
from PDRM with only the CpGAN module
Figure 2: U-Net model architecture
Figure 3: CoarseNet model architecture
Figure 4: Perspective distortion rectification model, consisting of a pix2pix module, a CpGAN
verifier and a MinutiaeNet module
Figure 5: Coupled GAN consisting of two conditional GANs coupled together via their embedded
feature vectors
Figure 6: MinutiaeNet architecture [9] consisting of a CoarseNet and a FineNet
Figure 7: Pre-processing steps for the "WVU non-contact fingerprint dataset" dataset
Figure 8: Experiments 1–4; (a) Baseline: Fphoto vs Fprint using Commercial Matcher, AUC:
92.1%, EER: 15.7%; (b) Experiment 1: PDRM - Synthetic Fprint vs Fprint using Commercial
Matcher AUC: 96.4%, EER: 8.9%; (c) Experiment 2: PDRM w/o CpGAN+MinutiaeNet -
Synthetic Fprint vs Fprint – Commercial Matcher AUC: 65.6%, EER: 46.1%; (d) Experiment 3:
PDRM w/o MinutiaeNet - Synthetic Fprint vs Fprint - Commercial Matcher AUC: 91.7%, EER:
15.5%; (e) Experiment 4: PDRM w/o CpGAN - Synthetic Fprint vs Fprint using Commercial
Matcher AUC: 58.7%, EER: 49.7%; Experiment 5 – (a) Fphoto vs Fprint using CpGAN Matcher
AUC: 98.4%, ERR: 6.3%
Figure 9: (Left) Contactless finger-photo. (Middle) Ground truth fingerprint. (Right) Synthetic
fingerprint from PDRM
Figure 10: (Left) Contactless finger-photo. (Middle) Ground truth fingerprint. (Right) Synthetic
fingerprint from PDRM without CpGAN Verifier
Figure 11: Experiment 5 – (a) Fphoto vs Fprint using Commercial Matcher AUC: 92.1%, EER:
15.7%. (b) Fphoto vs. Fprint using CpGAN Matcher AUC: 98.4%, EER: 6.3%

List of Symbols and abbreviations

Symbol/Abbreviation	Meaning			
PDRM	Perspective Distortion Rectification module			
GAN	Generative Adversarial Network			
cGAN	Conditional Generative Adversarial Network			
CpGAN	Coupled Generative Adversarial Network			
PPI	Pixels Per Inch			

Chapter 1: Introduction

Introduction

Fingerprint matching is a common biometric modality which can be used almost anywhere for quick and easy security, from consumer products, like phones, to government facilities. The reason the use of fingerprints is so widespread is because of their fast-matching capabilities by matching only particular feature points on a fingerprint called minutiae points. These minutiae points are extracted from the ridges and valleys on a fingerprint. While only one or two minutiae points might not be unique, the combination of minutiae points contained in the entire fingerprint are. Most fingerprint matching systems use these minutiae points for matching [1],[9]. While the entire fingerprint is generally unique individual minutiae points might match up to other people minutiae points so creating a matching vector of minutiae points that has enough datapoints is directly correlated to higher security, so any fingerprint matching software wants to have the maximum number of minutiae points it can have.

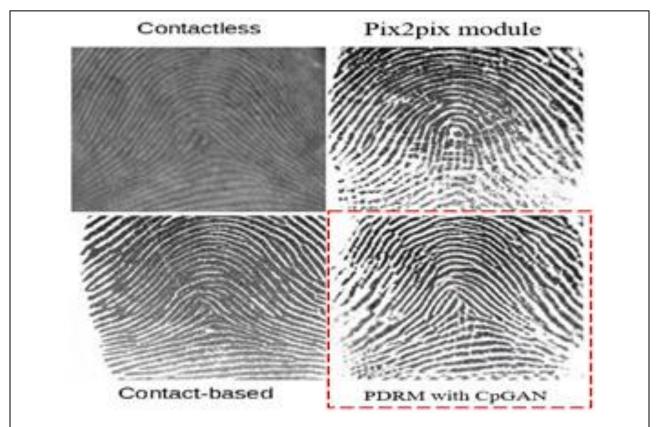


Figure 1: (Top Left) Contactless finger-photo. (Bottom Left) Ground truth fingerprint. (Top Right) Synthetic fingerprint from only pix2pix module of PDRM. (Bottom Right) Synthetic fingerprint from PDRM with only the CpGAN module.

There are a multitude of ways to collect fingerprints; these methods include using ink and paper to get a rolled fingerprint, using a contact-based capacitive or optical fingerprint reader, and capturing a close-up picture of a finger, which is referred to as a finger-photo. Any contact-based fingerprint can suffer from elastic deformation, which is when the skin compresses or stretches while applying pressure onto paper or a platen. This deformation causes displacements for the relative properties of minutiae, and consequently, alters the identification information within the captured sample. While contactless finger-photo collection lacks elastic deformation due to the inherent structure of the capturing process [6]. However, contactless data suffer from a different kind of distortion, perspective distortion caused by the 3D shape of the fingertips. With a rolled fingerprint, one can get an even view of all points on a finger from edge to edge. However, from a finger-photo, the edges of the finger are curved compared to the center of the finger. This compresses the minutiae points and makes them harder to identify and represent accurately in a fingerprint template. So, it is a tough balancing act of which method is more viable, while contact based collection doesn't have perspective distortion is does have elastic distortion and while contactless based collection has perspective distortion it does not have elastic distortion. Contactless however also has the added benefits of being hygienic and in today's age of Covid-19 this is much more valuable. Cameras are ubiquitous in modern society and having the ability to create an equivalent fingerprint without any deformations from a finger-photo allows even more accessibility to biometric security.

The main objective of this paper is to create a method that can take a finger-photo and turn it into a fingerprint by removing the perspective distortion. This allows commercial matchers to match finger-photos to an existing rolled fingerprint database. Our secondary objectives are to match legacy fingerprints to the synthetic fingerprint images generated from contactless based finger-photos and to create a pre-processing module to allow our new method to seamlessly integrate into any existing fingerprint matching system. No new technology will be widely used if it does not have compatibility with existing framework, which is why we added the secondary objectives. We want any module created from this research to also be practical. First and foremost is to create synthetic fingerprints from contactless based finger-photos however a good model will be able to accomplish both the primary and secondary objectives at the same time. We propose a Perspective Distortion Rectification Module (PDRM) to map the domain of finger-photo images to the domain of synthetic rolled fingerprints. The proposed PDRM is a careful modification of a Conditional Generative Adversarial Network (cGAN) [3] upgraded using two deep fingerprint-to-finger-photo verifiers to force the generator to preserve the identification information of samples during the mapping. Some results are shown in Fig. 1 for unrolling a finger-photo to an equivalent fingerprint. The method described in this paper can easily be incorporated as a pre-processing module into any existing commercial fingerprint matching system, allowing commercial matchers to be used without modification by enabling the finger-photo probe input to be matched directly against a rolled contact-based fingerprint gallery

One major challenege that we faced is the two different distortions between the two fingerprint collection methods, elastic deformation and perspective distortion. If elastic deformation is removed by using contactless based fingerprint capturing methods then the fingerprint image will end up having perspective distortion. Since our secondary objectives is to match synthetic fingerprints to legacy fingerprints we will end up converting perspective distortion into elastic deformation, not just removing perspective deformation all together. Another challenge is image consistency among the dataset. Contactless fingerprints are all captured on a camera and there can be small variations in light, angle, and color can all effect a model, these variances needed to be accounted for and removed if possible using computer vision techniques.

In our research we first tried to understand how existing systems deal with perspective distortion and elastic deformation in their own domain matching systems to determine if there are similarities between the two methods. We wanted to find commonalities that legacy systems used to match finger-photo to finger-photo and fingerprint to fingerprint. Finding this common ground would allow us to determine what we need to focus on when create the synthetic fingerprints. The next thing we researched was for existing methods to match finger-photos to fingerprints directly, these methods would need to account for all the pre-processing issues that were addressed in the challenges so we could have a better understanding of what our pre-processing steps should be. This would also allow us to determine the faults and challenge that these other researchers found during their own investigations as well so we could be better prepared when we start creating our model. This would also give perspective into other models and methods that can perform our primary objective to see what works and what doesn't work.

Contributions

The contributions of this project can be summarized as follows:

- Alexander Wilson contributions:
 - CpGAN model
 - Complete PDRM model
 - o MinutiaeNet module of PDRM
- Ali Dabouei contributions:
 - First iteration of verifier module in PDRM model
 - Pre-processing of the dataset
- Brady Williams contributions:
 - o Results from testing on commercial matcher

Related Work

With the rise of fingerprint matching, one of the main issues with capturing the fingerprint is elastic deformation. This elastic deformation can be solved in several ways, special equipment like sensors [21], [22]. However, the more affordable and practical method would be to just not have the fingerprint come into contact with the capturing device at all, having a contactless-based fingerprint capturing method. The problem with contactless based fingerprint collection thought is perspective distortion, which is the distortion along the edges of the finger-photo that increases in severity as the region of interest moves further from the finger center. Most of the current approaches to address this issue extract minutiae from both the contactless and contact-based fingerprints and match them against each other [8]. However, the number of reliable minutiae for matching is very small due to the perspective distortion. Another method is to just ignore the perspective deformation and focus only on the large cluster of minutiae points in the central core region of the finger by enhancing the image and making minutiae points pop out of their surroundings, as addressed in [8], [13]. However, the problem with this approach is that the matching system will then be ignoring vital minutiae points that could impact the overall accuracy. While this approach is fine for lower security systems that might not need a high chance of certainty in the accuracy of the match, it would be unsecure to use this in anything more advanced and secure. Another approach is to focus on localized texture patterns (i.e., ridge locations, ridge orientations, pores, etc.) from the entire contactless fingerprint and match them using those features instead, as shown in [7], [15]. In [23] they define a method that allows for not only

matching on the minutiae feature vector, but also the overall minutiae topology and their relevance to other surrounding minutiae points. This approach gives another layer of security on top of simply matching minutiae points by making the entire fingerprint another major feature as well since the location of minutiae points in relevance to other minutiae points will also be unique. Instead of just making two minutiae points vectors the entire fingerprint is taken into account, this removed the need to even reconstruct the minutiae points in the area of the image affected by perspective distortion.

A more accurate form of fingerprint matching is 3D fingerprint matching, and this does solve the problems with deformation however the new issue here in this solution is that sometimes multiple cameras are needed to properly capture the contactless fingerprint. One such paper [18] has created a sensor that can illuminate the finger and take three images of the finger from different angles to gather all necessary information to create a proper representation of the contactless fingerprint. These 3D representations can then be matched using contactless 3D fingerprint matching software like in paper [20]. However, using multiple cameras of special hardware is quite costly but one solution to this problem is addressed in [12] where they perform the same steps as a typical 3D fingerprint matching algorithm but use only one camera. They generate a new kind of 3D representation of the fingerprint from the single camera. Existing minutiae conventions are then converted to this 3D space to allow matching between their special 3D representation of the contactless fingerprint data to be matched with new 3D fingerprints collected it would require a brand-new matcher to replace existing structures.

Another way to solve the perspective distortion problem is to clear up the image in preprocessing. There are many image processing techniques that allow perspective deformation to be corrected [19] and in the paper [14] they show a pre-processing setup that allows for correcting of the contactless fingerprint image and they also create a matcher that can match contact-based fingerprints to the corrected contactless based fingerprint. Their matcher matches both the texturebased representation of the fingerprint as well as the minutiae points themselves.

There are also several other potential problems with capturing a contactless finger-photo, including nonuniform illumination, environmental conditions, and even finger orientation. These issues often reduce the effectiveness of minutiae or feature extraction algorithms which,

consequently, reduce the accuracy of fingerprint matchers [5], [10]. To compensate for distortions in the orientation maps, neural networks are used to correct the orientation of finger-photos [11]. These neural networks extract minutiae points regardless of orientation and can match contactless fingerprints. Nonuniform illumination is addressed in [7], where they apply a robust pre-processing step to finger-photo images that normalizes uneven illumination, as well extracts points of interest in the finger-photo.

Wider adoption of contactless fingerprint matching is what biometrics practitioners should be striving for, but in order to do that, according to [8], an existing model needs not only to match contactless fingerprints to contactless fingerprints, but also be able to match contactless fingerprints to a database of legacy rolled fingerprints. The method addressed in [8] says this issue with a model called the deformation correction model to correct the deformations in the contactless fingerprint to then be used to match the legacy fingerprints. However most legacy fingerprint was captured using contact-based methods meaning they might suffer from elastic deformation. A matcher that matches contactless fingerprints to legacy fingerprints will also need to account for this deformation conversion.

The takeaway from the research done here is the following. Pre-processing is a very important step, alone it is almost able to correct the perspective distortion in a contactless fingerprint if a custom matcher is used for matching these cleaned images. To cut down on cost and make contactless fingerprint matching more widely used it needs to have minimum impact on existing system, meaning no extra cameras, sensors, or brand-new matchers. Using only one image will also cut down on user error as well when collecting images, if there is only one image of the fingerprint that is being collected at a time there is only one view that needs to be corrected when it comes to orientation and illumination. A new method needs to be as un-invasive to existing infrastructure as possible and be able to match existing legacy contact-based fingerprints to contactless-based fingerprints. A neural network can be used to create a new representation of an image and match based on this new representation that will use features in the embedded domain for matching. Our method will be using all of this in different areas throughout the project.

Outline

Chapter one of this thesis was to explain the general information of the work that needed to be done. It showed the background information of the domain and scope of the thesis and defined

what terms would be used. We went over the common fingerprint collecting methods and their flaws. It shows the contributions of the team, the challenges we faced, and a general explanation of the final solution for our thesis, the PDRM model. And finally, the research to determine what would need to be done in the thesis.

Chapter two explains in more detail the final model first explained in chapter one, the PDRM model. Going over each individual module, their use, and how they were constructed. This chapter also explains the building block technologies used to make up these modules and the loss functions behind each one to be later used in chapter three. The first section explains the building blocks of all modules and the PDRM while each subsequent section of this chapter focuses on the individual module.

In chapter three we go over every loss function that we created for every module and the final PDRM. Each loss function has its own label to identify the difference between loss functions and be able to easily identify each section and how its used in the diagrams form chapter two. This chapter is used to better show how exactly each variable is being used throughout the entire process.

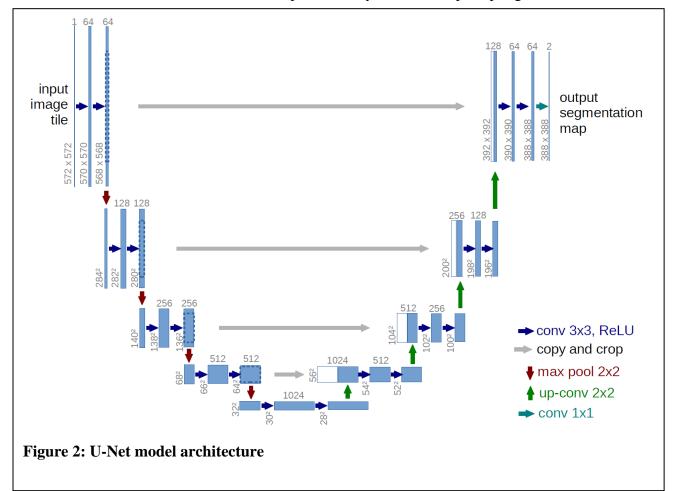
Chapter four first goes over the experiments that were performed as well as the details of how they were performed and the dataset they were performed with. The chapter also goes into exact detail of the models used to construct each individual module and the parameters used for testing. The chapter also explains how the compare the results of the experiments and what they should be compared to.

Chapter five and six shows the results of the experiments. Most experiments are shown on a single graph, Fig. 8 and the actual synthetic fingerprints of the tests are shown together so you may see the qualitative results rather than just the quantitative graph results. We go over the experiments and explain what we believe they mean according to our research and what the overall conclusion of this thesis was. And finally, the future work that could be done to improve the thesis.

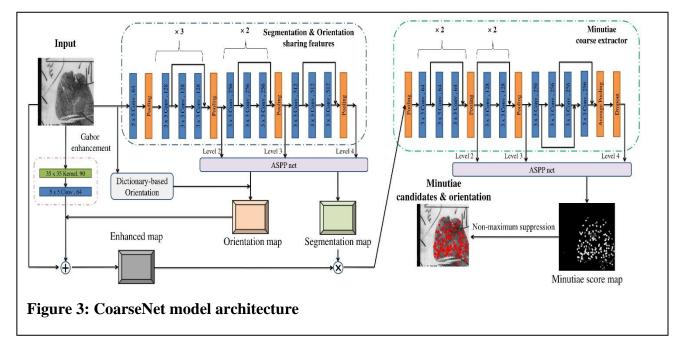
Chapter 2: Proposed Method

Proposed Method

The overall goal for the method presented here is to estimate an equivalent synthetic contact-based fingerprint from a contactless finger-photo. This would allow for any existing fingerprint matching system to use our model with minimal modifications. However, when converting a contactless finger-photo to a rolled fingerprint, the main issue is the perspective distortion. To take this issue into account, first the dataset is pre-processed to correct for illumination inconsistencies and orientation inconsistencies between the ground truth and the contactless finger-photo images, then we focused on using a Generative Adversarial Network (GAN) [4] to convert the domain of finger-photo images to another domain of synthetic rolled fingerprints, specifically using the pix2pix model [3]. The generators of GAN networks in all modules uses a U-NET architecture [1] as shown in Fig. 2. The U-NET architecture is a U-shaped convolutional network where typically an image is inserted, it is boiled down into a embedded domain feature vector used an encoder and then it is reconstruction through convolution and concatenation with its residuals from previous layers called upsampling with the decoder.



Specifically, our model uses a U-NET 256 model since the input size of the image is 256x256. Every discriminator is a simple convolution layers directly inputted into 4 fully connected layers and an output layer to determine if the image is fake or real. The MinutiaeNet module however does not have a GAN and its model is called a CoarseNet which is created using a few ResNet based models to generate some minutiae maps. These ResNet models specifically are residual based models where the residuals are brought forward in the layers as shown in Fig. 3. The ResNet residual networks generate multiple maps when combined and processed again create the minutiae score map that we need.



Generative Adversarial Network

A GAN model consists of two differentiable modules, a generator G, and a discriminator D. The generator maps some noise variable z from a prior noise distribution, $p_z(z)$, to a data space with distribution p_{data} . While the discriminator determines if an input is either a real data, y, or the output of the GAN, G(z), using a classification scheme. During the training, the generator and the discriminator are constantly working against each other in a minimax game, where the generator is trying to fool the discriminator into thinking generated (synthetic) data is the same as the real data, while at the same time, the discriminator is trying to discriminate between the generated (synthetic) and real data. The loss function for the GAN model is:

$$L(D,G) = E_{y \sim P_{data}(y)} [\log(D(y))] + E_{z \sim P_{z}(z)} [\log(1 - D(G(z)))].$$
(1)

To find the proper solutions for the generator and the discriminator, we perform a twoplayer minimax game as shown by the following optimization:

$$\min_{G} \max_{D} L(D,G) = \min_{G} \max_{D} E_{y \sim P_{data}(y)} [\log D(y)] + E_{z \sim P_{z}(z)} \left[\log \left(1 - D(G(z)) \right) \right].$$
(2)

This method is simply using a noise variable for the input to the generator. Another model called a conditional GAN [3] allows for the input sample to be added as a condition to the input of the generator and the discriminator. We will be using this version of the GAN model throughout the paper. To this aim, cGAN makes the following conditional changes to the algorithm:

$$L_{c}(D,G) = E_{y \sim P_{data}(y)} \left[\log(D(y|x)) \right] + E_{z \sim P_{z}(z)} \left[\log(1 - D(G(z|x))) \right],$$
(3)

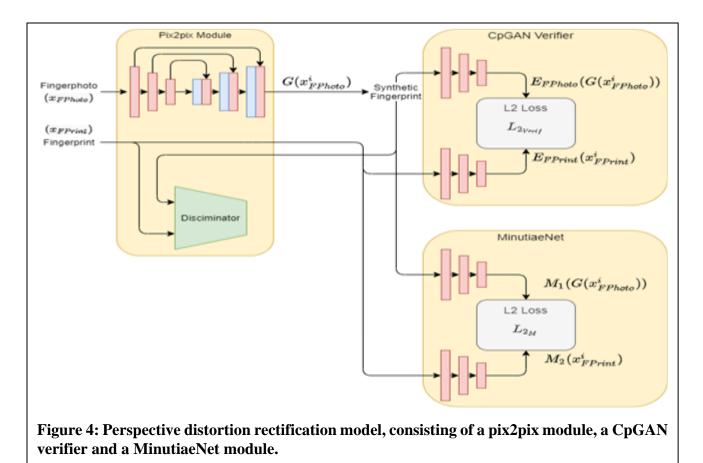
and, to optimize this function for a two-player minimax game, we employ the following objective:

$$\min_{G} \max_{D} L_{c}(D, G, y, x) = \min_{G} \max_{D} E_{y \sim P_{data}(y)} [\log D(y|x)] + E_{z \sim P_{z}(z)} \left[\log \left(1 - D(G(z|x)) \right) \right].$$
(4)

Since the GAN now allows specific conditions rather than random noise, we can now specify an input to the GAN and always get the same output from that specific input.

Perspective Distortion Rectification Method

Our perspective distortion rectification model is an implementation of the conditional generative model (cGAN) called pix2pix [3] with two added verifiers to force the generator to focus on the more important aspects of the fingerprint, as shown in Fig. 4. One verifier, called the Coupled-GAN (CpGAN) verifier [16], focuses on extracting the embedded domain features for matching, while the other verifier, called MinutiaeNet [9], identifies the minutiae points for matching.



The MinutiaeNet and CpGAN verifiers are both deep modules that are trained separately from the pix2pix module and are added to the pix2pix module with frozen weights. These modules are only used to validate the results of the pix2pix module and help the generator to preserve the ID information. They work similarly to the discriminator of a typical GAN model by being a checker to determine how accurate the synthetic image is compared to the ground truth. While a normal discriminator can just tell if an image is fake or not the CpGAN verifier module and the MinutiaeNet module can be used to determine how close the synthetic fingerprints are to being real fingerprints. The training of each of these modules are explained in the next two sections. The CpGAN verifier used in this model is a modified form of the CpGAN presented in [17]. The modification made to CpGAN are as follows: the weights of the finger-photo module in CpGAN are replaced with the weights of the fingerprint module, the decoders and the discriminators of both modules are removed, and the contrastive loss is replaced with an L_2 reconstruction loss. The objective of the CpGAN was to identify some embedded domain features that can be used for matching between contactless fingerprints and contact-based fingerprints and once the CpGAN has been trained to identify these features we only need the weights of the fingerprint module

because we need a model to identify these embedded domain features and treat synthetic fingerprints and ground truth fingerprints the same. The MinutiaeNet module is two MinutiaeNet generators, called M_1 and M_2 , with an L_2 reconstruction loss between the results of both MinutiaeNet generators. The MinutiaeNet's objective is to simply identify the minutiae points of a fingerprint, if two MinutiaeNets both test the synthetic fingerprints and the ground truth fingerprints and get the same results between the two then the minutiae points on the synthetic fingerprint is passable for real matching.

Our PDRM module requires these two verifiers so that they can improve and validate the quality of the generated synthetic fingerprint from contactless finger-photos. The CpGAN verifier is designed to detect low-dimensional embedded features that can be used by a contrastive loss [2] to create a common embedded feature vector for matching finger-photo and fingerprint pairs. The CpGAN verifier will then allow the PDRM to locate these low-dimensional embedded features and match their quality. The MinutiaeNet verifier is added to allow the PDRM to identify minutiae points in the synthetic fingerprints, because these minutiae points are the most important features that represent the information within fingerprints and are being widely used by the existing fingerprint matching systems. If our model is to be used commercially and be unintrusive these features are the most important features that need to be replicated to convert contactless fingerprints to contact-based fingerprints to allow any matcher that uses minutiae points for matching to use this model seamlessly.

Coupled Generative Adversarial Network (CpGAN)

The CpGAN model consists of two conditional GAN models [3] referred to as the fingerphoto module and the fingerprint module, as shown in Fig. 5. The finger-photo module is dedicated to reconstructing the finger-photo images, and the fingerprint module is dedicated to reconstructing the fingerprint images. The generators of both modules use the U-Net architecture [1] to allow for finger-photo and fingerprint matching using the generated low-dimensional embedded feature vectors constructed by utilizing a contrastive loss, the adversarial loss of each module, and the L_2 reconstruction loss.

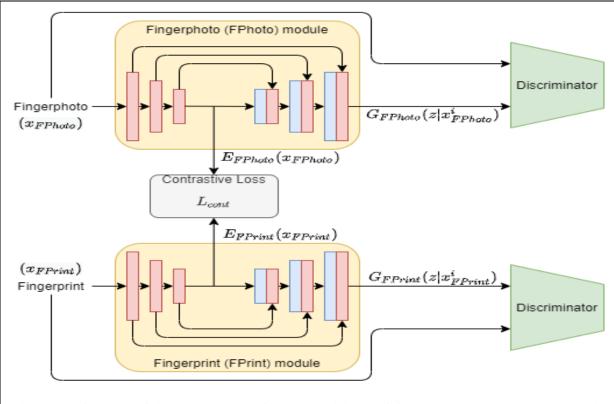


Figure 5: Coupled GAN consisting of two conditional GANs coupled together via their embedded feature vectors.

The main goal of the CpGAN is to match finger-photos and fingerprints using the embedded domain feature vectors. This is accomplished by training the generators to identify these features for both finger-photos and fingerprints, so when this CpGAN is turned into a verifier and added to the PDRM module, it can identify these features and allow the PDRM to create a better synthetic fingerprint by focusing on these embedded domain features.

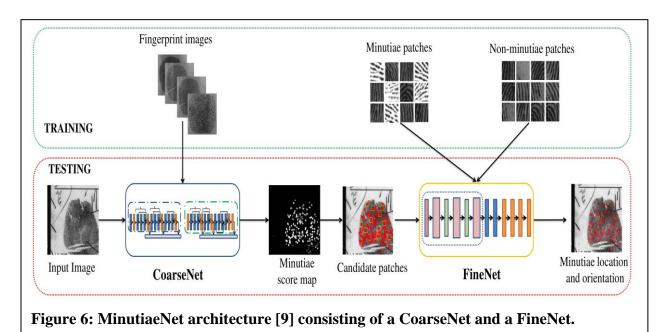
A U-Net architecture is used as our generator in the main model for its unique mapping capacity. This structure condenses an image into its contextual information in a subspace which we then use for matching a finger-photo against a fingerprint. The feature maps of each layer are also passed forward to the up-sampling layers which allow for the high-dimensional features to be combined with the up-sampled features to allow the generator to reconstruct the images.

Even though the finger-photo and fingerprint images of the same person are in different domains, the low-dimensional embedded feature vectors should be the same, meaning that the CpGAN should be able to gradually identify similarities between both domains. The features that we seek to identify are domain invariant and exist across both domains. By focusing on these features, the PDRM can identify them early in the synthesis process, as well as keep these features throughout.

Contrastive loss is used in the CpGAn to determine the difference between the embedded domain of each module using imposter pairs and genuine pairs. The L_2 reconstruction loss is used to make sure that each module is reconstructing each image at the end of the U-Net architecture. The adversarial loss is used to also emphasize the GAN create realistic recreations of the input images of each module. If the input images between the modules are genuine pairs or imposter pairs there is no difference to the adversarial loss or the L_2 reconstruction loss, they perform the same way every pair, only the contrastive loss will change.

MinutiaeNet

To further force the generator to preserve the ID information during the mapping, we employ a second-deep model to constrain the generation process. The MinutiaeNet module [9] is a differentiable feature extractor for minutiae points in fingerprints and finger-photos. MinutiaeNet uses two separate networks called the CoarseNet and FineNet as seen in Fig. 6. The CoarseNet creates a minutiae score map along with other information that is all passed into the FineNet, which further refines the score map to identify precise minutiae points. However, the PDRM method only uses the CoarseNet and score map results. Our method uses the already existing model created in [9], so no training is directly done for the MinutiaeNet.



The MinutiaeNet verifier is two CoarseNets combined, as shown in Fig. 2. The only output we utilize from the CoarseNet is the score map, which is used alongside an L_2 reconstruction loss function to determine the similarities of the minutiae points of the ground truth fingerprint and the synthetic fingerprint from the finger-photo created by the cGAN module.

This module is added to allow the PDRM to focus on recreating the most important part of the fingerprint when synthesizing the fingerprint from its finger-photo, i.e., the minutiae points. Since most common fingerprint matching systems use these features for matching, and we want our PDRM module to be able to be attached to any existing fingerprint matching system to simply improve its matching performance when presented with finger-phot probes, the minutiae points are important features that need to be recreated properly.

One minor change we performed to get the MinutiaeNet to properly work and be differentiable in the PDRM model was that the entire dataset was processed through the MinutiaeNet and the results were then taken and stored as a new dataset, this new dataset was then used to train another neural network, a ResNet-18 network [24] that was differentiable with the rest of the PDRM model, to recreate the MinutiaeNet results when the fingerprint images were fed into it.

Chapter 3: Loss Functions

Contrastive Loss

This loss function is a distance-based loss function that decreases the distance between the representations of genuine pairs (finger-photos and fingerprints of the same identities) in an embedded subspace while also increasing the distance between the representations of imposter pairs (finger-photos and fingerprints of different identities). The contrastive loss function (L_{cont}) is defined as:

$$L_{cont}(E_{FPhoto}(x_{FPhoto}^{i}), E_{FPrint}(x_{FPrint}^{j}), Y) = (1 - Y)\left(\frac{1}{2}\right)(D_{z})^{2} + (Y)\left(\frac{1}{2}\right)((0, m - D_{z}))^{2}, (5)$$

where x_{FPhoto}^{i} is the i-th finger-photo image and x_{FPrint}^{j} is the j-th fingerprint image. The variable Y is a binary label to determine if the finger-photo and fingerprint are genuine or imposter pairs. The value of Y will be 0 if the two images are from the same ID and Y will be equal to 1 if the two images form an imposter pair. The term E_{FPhoto} is the encoder of the finger-photo module of the CpGAN, while E_{FPrint} is the encoder of the fingerprint module of the CpGAN. The parameter m is the margin that is used to determine how close we want genuine pairs to cluster and how far away at minimum we want the imposter pairs to be apart in the embedding domain. The distance D_z is defined as the following:

$$D_{z} = \left| \left| E_{FPhoto} \left(x_{FPhoto}^{i} \right) - E_{FPrint} \left(x_{FPrint}^{j} \right) \right| \right|_{2}^{2}.$$
(6)

Adversarial Loss

The proposed method uses three adversarial losses to get to the final module. First, we explain the adversarial loss for CpGAN and then describe the adversarial loss for the main pix2pix module.

First the CpGAN adversarial losses. The term G_{FPhoto} is the generator for the finger-photo module, and G_{FPrint} is the generator for the fingerprint module. The variable D_{FPhoto} is the discriminator for the finger-photo module, and D_{FPrint} is the discriminator for the fingerprint module. The term y_{FPhoto}^{i} is a real finger-photo image, and y_{FPrint}^{j} is a real fingerprint image. Using the notations in Eq. (4), the adversarial loss function FPhoto GAN is given as:

$$L_{FPhoto} = \min_{G} \max_{D} L_{c} \left(D_{FPhoto}, G_{FPhoto}, y_{FPhoto}^{i}, x_{FPhoto}^{i} \right), \tag{7}$$

and similarly, the loss for FPrint GAN is given as,

$$L_{FPrint} = \min_{G} \max_{D} L_c(D_{FPrint}, G_{FPrint}, y_{FPrint}^j, x_{FPrint}^j).$$
(8)

The total loss function is the combination of these two losses together, given as:

$$L_{GAN_{CPGAN}} = L_{FPhoto} + L_{LFprint} \,. \tag{9}$$

Now the pix2pix module has a very similar objective function except that it only has one GAN loss, so there is only one generator G and one discriminator D. The loss is denoted as:

$$L_{GAN} = \min_{G} \max_{D} L_c(D, G, x^i_{FPrint}, x^i_{FPhoto}).$$
⁽¹⁰⁾

This loss is meant to force the generator of the attached GAN model to create better synthetic images to fool the discriminator in a constant back and forth game between the discriminator and the generator. Without a loss like this the GAN won't have much incentive to create realistic synthetic images.

L2 Reconstruction Loss

 L_2 reconstruction loss is used in every GAN model and it is used in place of contrastive loss when adding the CpGAN verifier into the pix2pix model.

The CpGAN reconstruction loss is used to tell the GAN that it must recreate the output of the GAN to look like the input of the GAN based on the Euclidean distance between the input and reconstructed output images. Both the finger-photo and fingerprint GAN modules have a reconstruction loss. The reconstruction loss for the finger-photo module $(L_{2_{FPhoto}})$ and the fingerprint module $(L_{2_{FPhoto}})$ are as follows:

$$L_{2_{FPhoto}} = \left| \left| G_{FPhoto} \left(z \left| x_{FPhoto}^{i} \right) - x_{FPhoto}^{i} \right| \right|_{2}^{2},$$
(11)

$$L_{2_{FPrint}} = \left| \left| G_{FPrint} \left(z | x_{FPrint}^{j} \right) - x_{FPrint}^{j} \right| \right|_{2}^{2}, \tag{12}$$

where z is a random noise vector.

The total L_2 reconstruction loss for CpGAN is now defined as:

$$L_{2_{CPGAN}} = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} \left(L_{2_{FPhoto}} + L_{2_{FPrint}} \right), \tag{13}$$

where N is the number of training samples.

Then the next instance of L_2 reconstruction loss is pix2pix where the results of the cGAN generator (synthetic fingerprint) with the ground truth fingerprint are compared. The L_2 reconstruction loss for this model is as follows:

$$L_{2_{pix2pix}} = \sum_{i=1}^{N} (G(z|x_{FPhoto}^{i}) - x_{FPrint}^{i})^{2}.$$
 (14)

Contrastive loss cannot be used for the CpGAN verifier when it's implemented into the perspective distortion rectification module. L_2 reconstruction loss is used in place of contrastive loss, and it is defined by the following equation:

$$L_{2_{Verif}} = \left| \left| E_{FPhoto} \left(x_{FPhoto}^{i} \right) - E_{FPrint} \left(x_{FPrint}^{j} \right) \right| \right|_{2}^{2}.$$
(15)

The final instance of L_2 reconstruction loss is used when the MinutiaeNet module is added to process the output of the pix2pix model and we need to find the Euclidean distance between the minutiae heatmaps of the ground truth fingerprint and the synthetic fingerprint. Let M_1 represent the MinutiaeNet for the synthetic fingerprint, and M_2 be the MinutiaeNet for the ground truth fingerprint. The MinutiaeNet L_2 reconstruction loss is as follows:

$$L_{2_{M}} = \sum_{i=1}^{N} \binom{M_{1}(G(z|x_{FPhoto}^{i})) - }{M_{2}(x_{FPrint}^{i})}^{2}.$$
 (16)

This loss is used two different ways, one way it will force the GAN model to have the input and output images look similar as done in the pix2pix module, and the CpGAN before being converted to a verifier. Essentially making the conditional and the output of the model be the same. The more weight put into this the higher the similarities between the input and the output images. The other way is simply finding the Euclidian distance between two feature spaces in the MinutiaeNet module and the CpGAN module.

Total Losses

The total loss for the CpGAN is defined as the following function:

$$L_{Total_{CpGAN}} = \lambda_1 L_{cont} (E_{FPhoto} (x_{FPhoto}^i), E_{FPrint} (x_{FPrint}^j), Y) + \lambda_2 L_{GAN_{CpGAN}} + \lambda_3 L_{2_{CpGAN}},$$
(17)

where λ_1 , λ_2 , and λ_3 are the hyperparameters to control the effect of each loss function.

The total loss for the PDRM module is defined by the following equation:

$$L_{Total_{PDRM}} = \alpha_1 L_{GAN} + \alpha_2 L_{2_{pix2pix}} + \alpha_3 L_{2_{Verif}} + \alpha_4 L_{2_M},$$
(18)

where $\alpha_1, \alpha_2, \alpha_3$, and α_4 are the hyperparameters.

Chapter 4:

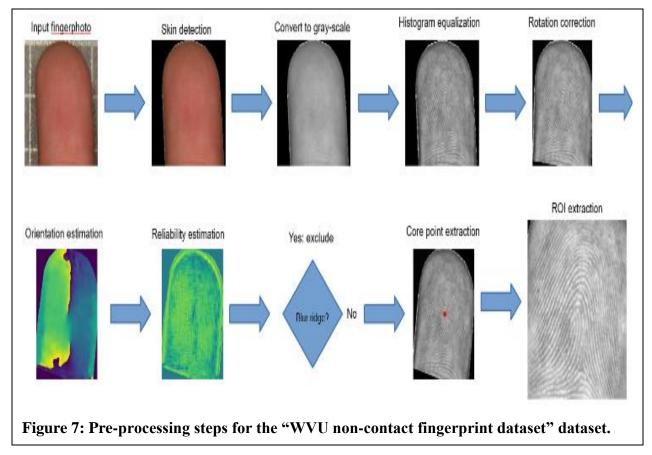
Details and Experiments

Experimental Details

For each experiment, the performance of the models is measured by using a Receiver Operating Characteristics (ROC) curve to show the overall accuracy of each model in matching finger-photos against fingerprints. In all experiments, the baseline is how well the commercial matcher can match directly the regular contactless finger-photo (Fphoto) and the fingerprint images (Fprint). If a model performs worse than this baseline, then it is no longer worth considering because this would mean the commercial matcher already outperforms our proposed models without any intervention. Both the CpGAN and PDRM models use the Adam optimizer with a learning rate of 0.0002, a batch size of 1, and both are trained for 200 epochs. The MinutiaeNet uses an Adam optimizer with a learning rate of 0.005, a batch size of 2, and is trained for 1000 epochs.

Dataset

The dataset used in this paper is the Non-Contact Fingerprint Dataset, which is a set of 970 subjects using four legacy fingerprint devices and three contactless fingerprint devices. The contactless dataset consists of 512x512 images with a resolution of 500 ppi. The contact-based



dataset consists of 800x750 sized images with a resolution of 500 ppi. The contactless prints need to be preprocessed so any insignificant differences between the contactless and contact fingerprints like orientation, color, and size, can be removed to allow easier generation for the GAN models by having them not worry about these variables and instead focus on the important variables like minutiae points and the embedded domain features. To make sure that both the fingerprints and the finger-photo are similar, pre-processing steps are applied to both images, as shown in Fig. 7. The steps are as follows: segment the skin from the background, then convert the image to grayscale, perform histogram equalization, and finally rotation correction. These steps are performed on both the fingerprints and the finger-photos, but because of the image capturing process used in the data collection, some of the ridges of the minutiae points are quite blurry. Because of this, after the first pre-processing step, any image that does not meet expectations are thrown out. The second pre-processing step is only applied to the finger-photos, which is orientation estimation and reliability estimation. In reliability estimation if the edges of these finger-photo images are not well defined they are excluded from the dataset, else the algorithm moves on to core point extract and ROI extraction. The output size for all images are normalized to 256x256 pixels.

Implementation Details

PDRM Architecture

The proposed PDRM model consists of the MinutiaeNet module, pix2pix module, and CpGAN module. The CpGAN module is the two encoders from the CpGAN model, as described in the next section connected by a L_2 reconstruction loss at the output of the encoders. The MinutiaeNet module consists of two CoarseNet models [9] connected by a L_2 reconstruction loss at the output of the CoarseNet models. The finer details of the MinutiaeNet are described in Sec. 5.2.3. The pix2pix module is a cGAN model described in [3] with a U-NET generator. The total loss function for the PDRM model is given by Eq. (18). The hyperparameters for the loss function (18) are shown in table 1. When modules are removed the hyperparameters that control that module is set to 0. The hyperparameter α_1 controls the adversarial loss of the pix2pix module. The hyperparameter α_3 controls the L_2 reconstruction loss of the CpGAN verifier. The hyperparameter α_4 controls the L_2 reconstruction loss of the MinutiaeNet module.

HYPERPARAMETER	α1	α2	α3	α4	AUC	EER
EXPERIMENT 1	1	1	1	10	96.4%	8.9%
EXPERIMENT 2	1	1	0	0	65.6%	46.1%
EXPERIMENT 3	1	1	1	0	91.7%	15.5%
EXPERIMENT 4	1	1	0	10	58.7%	49.7%

Table 1: Experiment 1-4 Hyperparameters for total loss functions.

CpGAN Architecture

As described previously the CpGAN model consists of two cGAN modules called the finger-photo and fingerprint modules. Each module is composed of a generator and a discriminator, and each generator is composed of an encoder and a decoder. The encoder will encode the input image down into an embedded domain feature vector of size 1x256 while the decoder takes that embedded domain feature vector and turns it back into the input image. The generator's architecture is the classical U-NET [1], and the two modules are connected by a contrastive loss that compares the embedded domain feature vectors of the outputs of the encoders of both modules' generators. Since this model uses a contrastive loss, an equal number of imposter pairs and genuine pairs need to be created. We create one imposter pair for every genuine pair, which is 3,335 of each pair. The total loss function for this model is given by Eq. (17). The hyperparameters for Experiment 5 (see Fig. 11) are: $\lambda_1 = 1$, $\lambda_2 = 0.001$ and $\lambda_3 = 1$.

MinutiaeNet

The MinutiaeNet module is taken directly from [9], where an already trained CoarseNet model is used to detect minutiae points and creating a minutiae point score map as shown in Fig. 6. Our MinutiaeNet module takes those weights from the pre-existing CoarseNet model, copied into another Resnet-18 [24] model that mimicked the CoarseNet model, and then applied that mimic model into the two generators in the MinutiaeNet module. The details of the Minutiae module can be found in [9].

Chapter 5: Results and Evaluation

Evaluation

Fig. 8 shows the results for Experiment 1. These results indicate that the accuracy of the matched synthesized fingerprints from finger-photos generated by the PDRM model is 4.3% higher than the accuracy of matching the finger-photos to the fingerprints directly using the commercial matcher. This shows that the full PDRM model can accurately synthesize the

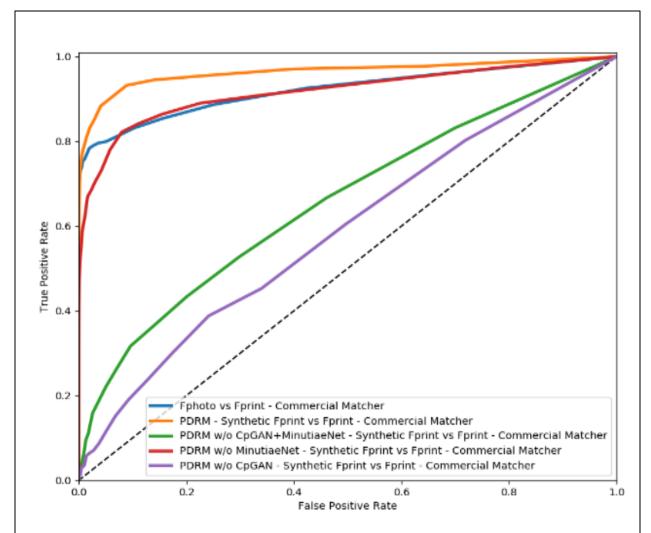


Figure 8: Experiments 1– 4; (a) Baseline: Fphoto vs Fprint using Commercial Matcher, AUC: 92.1%, EER: 15.7%; (b) Experiment 1: PDRM - Synthetic Fprint vs Fprint using Commercial Matcher AUC: 96.4%, EER: 8.9%; (c) Experiment 2: PDRM w/o CpGAN+MinutiaeNet - Synthetic Fprint vs Fprint – Commercial Matcher AUC: 65.6%, EER: 46.1%; (d) Experiment 3: PDRM w/o MinutiaeNet - Synthetic Fprint vs Fprint – Commercial Matcher AUC: 91.7%, EER: 15.5%; (e) Experiment 4: PDRM w/o CpGAN - Synthetic Fprint vs Fprint using Commercial Matcher AUC: 58.7%, EER: 49.7%; Experiment 5 – (a) Fphoto vs Fprint using CpGAN Matcher AUC: 98.4%, ERR: 6.3%.

important points of a fingerprint from a contactless finger-photo. This PDRM is also unintrusive to any existing fingerprint matching system, allowing it to be seamlessly added to any commercial matcher. Since the PDRM model is proven to work the next step is to perform an ablation study on the PDRM by removing the CpGAN module and the MinutiaeNet module to determine which of these modules are worthwhile or if they all play an important part in creating synthetic fingerprints.

In experiment 2, we removed both the CpGAN and MinutiaeNet modules from the PDRM model to see how well a simple cGAN model could synthesize the fingerprints from the contactless finger-photos. When the pix2pix synthesized fingerprints were passed through the commercial matcher, its performance was worse than the baseline commercial matcher when matching the finger-photos to the fingerprints directly, as shown in Fig. 8. The accuracy was in fact scientifically worse than performing nothing at all and just letting the commercial matcher match the contactless fingerprints and the contact-based fingerprints directly. This shows that the extra CpGAN and MinutiaeNet modules significantly improve the quality of the synthesized fingerprint images and that either both of them or one of them is the reason for the PDRMs success. As shown in Fig. 9 the quality of the synthetic fingerprint using the full PDRM module has some deformations at the top edge of the image, but the import minutiae points are very close to the ground truth.

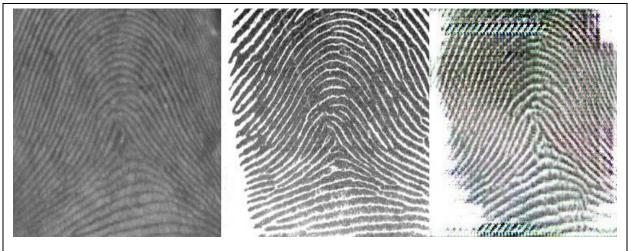


Figure 9: (Left) Contactless finger-photo. (Middle) Ground truth fingerprint. (Right) Synthetic fingerprint from PDRM.

In Experiment 3, as shown in Fig. 8, we remove only the MinutiaeNet module from the PDRM. These results show that, when solely using the CpGAN module in the PDRM model, it

can generate convincing synthetic fingerprints using only the embedded domain features gathered in the CpGAN training as a verifier for the quality of the synthetic fingerprints, even though the accuracy is 0.4% less than the baseline by. As you can see form Fig. 1 the results of the PDRM with just the CpGAN module are quite realistic. They form good fingerprints however some of the minutiae points are not being properly converted. They do not quite match up with the minutiae points of the ground truth, the image more closely resembled the contactless fingerprint rather than the ground truth.

In Experiment 4, as shown in Fig. 8, we removed the MinutiaeNet from the PDRM. These results are very poor, and the accuracy of the modified PDRM is less than the PDRM with just the pix2pix module. In Fig. 10 you can see that the unlike experiment 3 the synthetic fingerprint created from the PDRM without the CpGAN verifier more closely resembles the ground truth however it's very fuzzy, especially around the center where more of the important minutiae points are located. Just focusing on creating good minutiae points does not seem to be an adequate approach when trying to create synthetic fingerprints; more details are important in these matchers than what was originally thought including visibility and clarity. Also, these central minutiae points features play a much larger role than previously thought when it comes to matching.

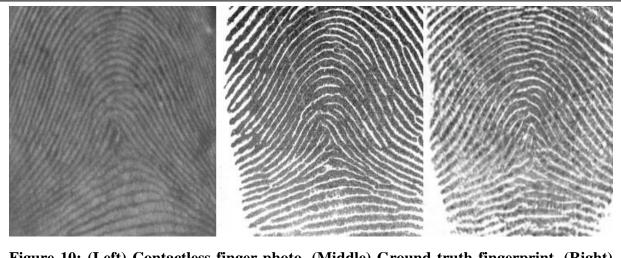
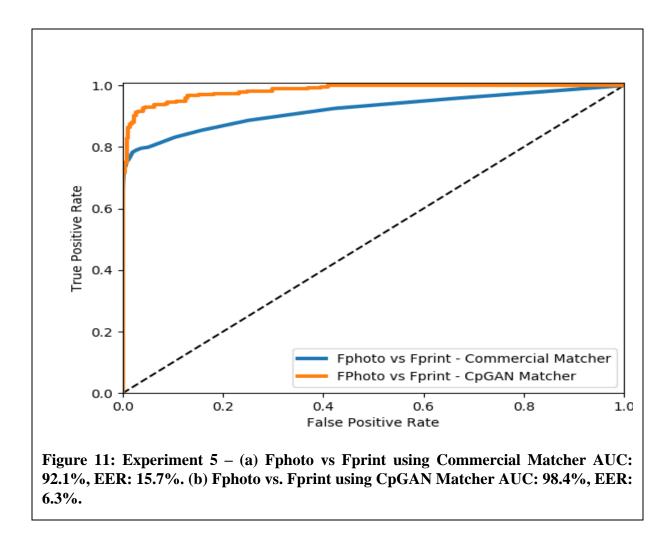


Figure 10: (Left) Contactless finger-photo. (Middle) Ground truth fingerprint. (Right) Synthetic fingerprint from PDRM without CpGAN Verifier.

The best results are obtained so far is when we were using the PDRM model with both the CpGAN and MinutiaeNet modules. All module information is important in creating a high-quality synthetic fingerprint, including the embedded domain features from the CpGAN module to the

minutiae points from the MinutiaeNet module. We need to also keep a balance between looking too much like the input finger-photo and being too fuzzy for the matcher to properly identify minutiae points. While it appears the CpGAN module holds more weight than the MinutiaeNet module, the MinutiaeNet module gives the synthetic fingerprints the boost the PDRM needs to outperform the baseline commercial matcher when matching the finger photos to fingerprints directly. Perhaps if the results of just the MinutiaeNet module in the PDRM were not so fuzzy the MinutiaeNet module could hold a lot more weight in how important the module is in making a realistic synthetic fingerprint.

In Experiment 5, as shown in Fig. 11, we used the CpGAN module as a verifier to directly match the finger-photos to fingerprints like the commercial matcher. The accuracy of the CpGAN matcher is 6.4% higher than the commercial matcher and is 2.0% higher than the PDRM accuracy. Using CpGAN as a matcher to directly match finger-photos to fingerprints is more effective than all other methods outlined in this paper. However, to use this matcher, it would require the entire existing fingerprint matching system to be replaced with this CpGAN matcher. This contradicts one of the main goals we had for this paper, where any method created should be unintrusive to the already existing fingerprint matching systems.



Chapter 6: Conclusion and Future Work

Conclusion

Matching finger-photo and fingerprint images is challenging due to the elastic and perspective distortions between the two modalities. However, the PDRM model outlined in this paper can overcome these issues and estimates the fingerprint version of a given fingerphoto sample. This paper also incorporated a deep model to identify features capable of direct matching of finger-photos against fingerprints. In fact, it was demonstrated that the embedded domain of the CpGAN was able to match samples from the two modalities. We also proposed a non-intrusive network that could be used in tandem with any existing commercial fingerprint matching software using this CpGAN as a verifier to make sure the generator was creating realistic synthetic fingerprints from the finger-photos. Just the verifier alone was not enough to create usable synthetic contact-based fingerprints because the minutiae of these fake images were blurry and ill-defined. Hence, a MinutiaeNet verifier was added to pix2pix to have the pix2pix model focus more on the minutiae points when synthetizing images. This provided great synthetic images, and the accuracy of using these synthetic images was only slightly worse than using the CpGAN matcher but had the bonus of being able to be incorporated into any existing commercial fingerprint

Future Work

This thesis can be expanded on, there is still room to grow in the fingerprint reconstruction field. While the best results of finger-photo to fingerprint conversion is promising when it comes to matching minutiae points, visually the reconstructed fingerprints look fuzzy around the edges (Fig. 10). If this tool is to be used more universally used it needs to be better at creating synthetic images visually as well as in the embedded domain to allow for any existing fingerprint matching system to use the reconstructed fingerprint. The dataset should also be screened to account for any biases in the types of fingerprints. There are three distinct types of fingerprint including the whorl, loop, and arch. Our dataset could have an uneven distribution of these fingerprint types since they do not occur evenly among the population, the existing network could have a bias towards a specific one of these fingerprint types and needs to be identified moving forward so the bias can be removed or accounted for.

The MinutiaeNet weights that were copied over and used in the MinutiaeNet module of the PDRM were pre-existing weights trained on a completely different dataset with slightly different domains, to improve accuracy the MinutiaeNet and PDRM could be trained on the same dataset

to clear the images up. However, this would require a dataset that had finger-photos, fingerprints, as well as minutiae point ground truths for both the finger-photos and fingerprints. Also, the actual MinutiaeNet module didn't use the entire MinutiaeNet weights, it used a copy of the weights that were recreated on a separate network. Finding a better way to implement this PDRM model to allow the original MinutiaeNet to be properly implemented could also improve accuracy.

In the PDRM the input image size was set to 256x256 and in the case of this dataset that cut each dimension in half losing 75% of the total images size. Reducing the image size so much was required by our systems to allow for quick training of the networks, within a day to two days for most training sessions, however this massive reduction in size could have a major impact on this sort of project by removing much needed small details that were inside the area affected my perspective distortion needed by the PDRM to reconstruct those areas. Future versions of the PDRM should use a larger image size to allow for more details to be passed through.

Ultimately, the goal of this project was to create synthetic fingerprints from finger-photos that is better for matching then not modifying the images, and that was proven to be possible. Now it's just a matter of cleaning the resulting images through more precise testing.

References

- [1] O. Ronneberger, P. Fischer, and T. Brox, "U-net: Convolutional networks for biomedical image segmentation," in *International Conference on Medical image computing and computer-assisted intervention*. Springer, 2015, pp. 234–241.
- [2] S. Chopra, R. Hadsell, and Y. LeCun, "Learning a similarity metric discriminatively, with application to face verification," in 2005 IEEE Conference on Computer Vision and Pattern Recognition (CVPR'05), vol. 1. IEEE, 2005, pp. 539–546.
- [3] I. Phillip, et al. "Image-to-image translation with conditional adversarial networks." in *Proceedings of the IEEE conference on computer vision and pattern recognition.* 2017.
- [4] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A.
 Courville, and Y. Bengio, "Generative adversarial nets," in *Advances in neural information* processing systems, 2014, pp. 2672–2680.
- [5] H. Tan and A. Kumar, "Towards More Accurate Contactless Fingerprint Minutiae Extraction and Pose-Invariant Matching," in *IEEE Transactions on Information Forensics* and Security, vol. 15, pp. 3924-3937, 2020, doi: 10.1109/TIFS.2020.3001732.
- [6] J. Libert, J. Grantham, B. Bandini, S. Wood, M. Garris, K. Ko, F. Byers and C. Watson,
 "Guidance for Evaluating Contactless Fingerprint Acquisition Devices," *National Institute* of Standards and Technology, 2018.
- [7] A. Kumar and Y. Zhou, "Contactless fingerprint identification using level zero features," *Conference on Computer Vision and Pattern Recognition Workshop*, Colorado Springs, CO, USA, 2011, pp. 114-119, doi: 10.1109/CVPRW.2011.5981823.
- [8] C. Lin and A. Kumar, "Matching Contactless and Contact-Based Conventional Fingerprint Images for Biometrics Identification," in *IEEE Transactions on Image Processing*, vol. 27, no. 4, pp. 2008-2021, April 2018, doi: 10.1109/TIP.2017.2788866.
- [9] D.-L. N. a. K. C. a. A. K. Jain, "Robust Minutiae Extractor: Integrating Deep Networks and Fingerprint Domain Knowledge," in *the 11th International Conference on Biometrics*, 2018, 2018.

- [10] A. Jain, Lin Hong and R. Bolle, "On-line fingerprint verification," in *IEEE Transactions* on Pattern Analysis and Machine Intelligence, vol. 19, no. 4, pp. 302-314, April 1997.
- [11] R. D. Labati, A. Genovese, V. Piuri, and F. Scotti. Contactless fingerprint recognition: a neural approach for perspective and rotation effects reduction. in *Computational Intelligence in Biometrics and Identity Management (CIBIM)*, 2013 IEEE Workshop on, pages 22–30. IEEE, 2013.
- [12] Kumar, Ajay, and Cyril Kwong. "Towards contactless, low-cost and accurate 3D fingerprint identification." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2013.
- [13] X. Liu, M. Pedersen, C. Charrier, F. A. Cheikh, and P. Bours. An improved tep contactless fingerprint image enhancement approach for minutiae detection. in *6th European Workshop on Visual Information Processing (EUVIP)*, pages 1–6. IEEE, 2016.
- [14] Grosz, Steven A., Joshua J. Engelsma, and Anil K. Jain. "C2CL: Contact to Contactless Fingerprint Matching." arXiv preprint arXiv:2104.02811 (2021).
- [15] A. Sankaran, A. Malhotra, A. Mittal, M. Vatsa, and R. Singh. On smartphone camera based fingerphoto authentication. in IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1–7, 2015.
- [16] M.-Y. Liu and O. Tuzel, "Coupled generative adversarial networks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2016, pp. 469–477.
- [17] F. Taherkhani, et al., "PF-CpGAN: Profile to frontal coupled GAN for face recognition in the wild," 2020 IEEE International Joint Conference on Biometrics (IJCB), Houston, TX, USA, 2020, pp. 1-10.
- [18] Wang, Lirong, et al. "A novel contactless aliveness-testing (CAT) fingerprint sensor."
 Novel Optical Systems Design and Optimization XII. Vol. 7429. International Society for Optics and Photonics, 2009.
- [19] Zhou F, et al. "A Coarse-To-Fine Subpixel Registration Method to Recover Local Perspective Deformation in the Application of Image Super-Resolution." Ieee Transactions

on Image Processing : A Publication of the Ieee Signal Processing Society, vol. 21, no. 1, 2012, pp. 53–66., doi:10.1109/TIP.2011.2159731.

- [20] Lin, Chenhao, and Ajay Kumar. "Contactless and partial 3D fingerprint recognition using multi-view deep representation." Pattern Recognition 83 (2018): 314-327.
- [21] R. M. Bolle, R. S. Germain, R. L. Garwin, J. L. Levine, S. U. Pankanti, N. K. Ratha, and M. A. Schappert. System and method for distortion control in live-scan inkless fingerprint images, May 16 2000. US Patent 6,064,753.
- [22] Y. Fujii. Detection of fingerprint distortion by deformation of elastic film or displacement of transparent board, Feb. 9 2010. US Patent 7,660,447.
- [23] Yin, Xuefei, et al. "Contactless Fingerprint Recognition Based on Global Minutia Topology and Loose Genetic Algorithm." Ieee Transactions on Information Forensics and Security, vol. 15, 2020, pp. 28–41., doi:10.1109/TIFS.2019.2918083.
- [24] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2016, pp. 770–778