"FINGERPRINT SPOOF DETECTOR ANALYSIS GENERALIZATION": DISCUSSION AND ANALYSIS

Cryptography Final Project for CSE667

Instructor: Dr. Bibak

Paper Authors: Tarang Chugh and Anil K. Jain

Published in IEEE Transactions On Information Forensics AND Security, Vol. 16, 2021

Group Members: Steven Yu and Noah Dunn

1 Introduction

1.1 The Physical Realm of Cybersecurity

When inhabiting the world of cybersecurity and cryptography, there is a great emphasis that is placed on the digital realm. As the rate of technology progressing advanced at a unprecedented rate in the past decades, computer scientists, mathematicians, and security professionals all rushed to find good ways to handle modern security concerns. Data and information became a game of capture-the-flag, with adversaries attempting to thwart one another at every turn, and yet, in all this organized effort, a critical layer remained a proper attack vector.

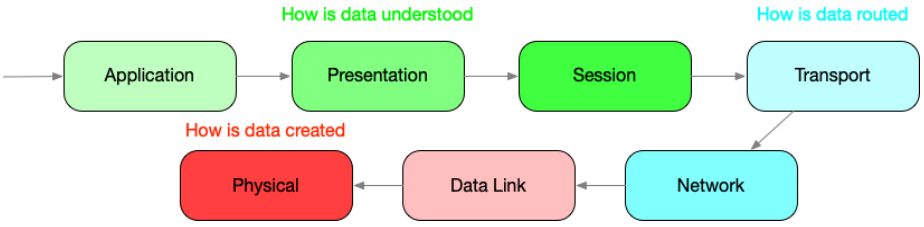


Figure 1: The Open Systems Interconnection (OSI) Stack

The Open Systems Interconnection (OSI) Stack, a systems standard established in 1994, dictates 7 unique layers of security[23]. At the top of the stack exists what many people today consider 'modern' vectors of attack: the application layer, the presentation Layer, and the session Layer, all of which are concerned with the transmission of human readable data. This layer is where many modern cryptography applications take their root (database encryption, data obfuscation, etc...). The next layers: transport, network, and data link make use of more primitive data and securing their transport and delivery. At the base of the pyramid, the critical attack vector for understanding the kind of work presented here, is the *physical* layer [12].

1.2 Understanding Physical Attacks

When some hear the term 'physical layer attack', they may imagine someone sneaking into a building they have access to late at night to plug their computer into a server and tamper or download some information. While this is still a very real threat and possible attack vector, the modern landscape of attacks on the physical layer has, much like its technology brethren, evolved to meet new demands.

A modern term, physical penetration testing, is used to describe a testing framework where real people attempt to gain access to places and information they are not supposed to by exploiting the physical security of rooms or buildings, as well as by manipulating people through social engineering techniques.

Dimkov and Pieters note, "Physical penetration tests are seldom done without social engineering, because when entering a location, it is imminent that the testers will have to interact with the employees and use deception to reach their target" [6]. Street, during his DEF CON (the largest Hacker conference in the world) presentation, explained how vulnerable companies, with immense digital protection, still fall fatal to physical attacks every day [24].

1.3 Modern Attacks for Modern Cybersecurity

In stark contrast to the modern focus on digital vectors of attack, Hutter notes that increase in existent technology has made "physical security...increasingly more difficult for organizations" [10]. His justification for this claim is that unlike the days of old, the modern convenience of desks "...filled with desktop computers and mobile laptops that have access to company data..." in addition to the ability of "...mobile users able to take their computers out of the facilities" makes the physical securing of data a progressively more difficult task [10].

If the theoretical implications of this kind of system are not enough to satiate, recent physical cyber attacks offers support. In a recent legal case, Coca-Cola had the personal information of 74,000 employees compromised when "hundreds" of work laptops were stolen from one of their offices. According to Opfer, the information able to be accessed on these laptops included, but were not limited to, **credit card numbers** and **social security numbers** [19]. As a more generalized statistical offering, Pritchard offers that "More than **one in 10 data breaches** now involve 'physical actions'". It is apparent from the data that the physical layer remains as a relevant and common vector of attack.

1.4 Understanding Biometrics and Biometric Attacks

One field of modern cybersecurity revolves around the use of biological data in order to provide or restrict access to certain areas, documents, or objects. As Norton Security states, "Biometrics are a way to measure a person's physical characteristics to verify their identity" [14]. Biometrics usually take the form of a physical trait that is unique to a single human, such as a fingerprint. In short, they are a modern way to solve an old problem, the "...automated recognition of individuals by using behavioral and/or biological characteristics..." for the goal of satisfying "An increasing demand for safety and security in both the public and private sectors..."[2].

As for any notion of security, adding more security layers to a problem offers adversaries more potential layers for exploitation. Biometrics are susceptible to a common general classification of attack known as a **presentation attack**. In any presentation attack, an individual presents something that they should not possess in order to act as though they are another person. Specifically, the UK's NCSC (National Cyber Security Center) offers a specific example for fingerprints: "If a fingerprint of the enrolled individual can be captured, this could be used to make a matching artefact" [3]. In other words, if an adversary can get someone's fingerprint, they can build a fake fingerprint using the original

fingerprint, described here as an 'artifact'. With this ability, an adversary can access all the information that only a particular individual is supposed to be allowed to access, which is a huge breach of safety and security.

1.5 Fingerprint Spoofing Attacks

The process of using of an artificial fingerprint (or artifact) in order to conduct a presentation attack on a system is referred to often as a *fingerprint spoof attack*. These attacks require only a fingerprint of a known user to gain access to a known system, after the 'spoof' is constructed, allowing an adversary access to secured systems [1]. In recent years, efforts have been made to combat spoof techniques, using "liveness detection systems" to determine if a real finger is being used or not [1]. The problem with these kind of systems; however, is that these systems have historically been based on "...unrealistic, ... known spoof fabrication systems materials" making them very unpredictable and inaccurate to individuals skilled in these kind of attack [1].

As a result of the known security vulnerabilities available in liveness detectors, Chugh et al. have developed a system to make liveness detectors more accurate, and thus, make systems more secure. Their research has resulted in the creation of a fingerprint spoof detector that attempts to build out a "locus" or a database of unknown, probable spoof materials [5]. In other words, the system takes existent real fingerprints, and existent real spoofs and uses a procedure to generate new "materials" for spoofs that have not yet been built or discovered. This provides the application of further securing a known problem and vulnerability in existing identity verification systems. In addition, this research is particularly useful for those constructing fingerprint based security systems, and future systems will be able to take advantage of these kind of techniques to buttress their security.

2 Previous Work

2.1 Origins of Fingerprint Spoofing Research

The study of fingerprint liveness detection appears to largely have been a recent study, taking place only within the past two decades [25]. The early 2000's saw an exploration into different techniques used to spoof fingerprints for automated detectors. Matsumoto et al. explored how "gummy" or artificial fingerprints could be forged to trick automated sensors, noting that "Security evaluation against attacks using such artificial fingers has been rarely disclosed" [17]. During the same year, other research groups were exploring the opposite side, detecting these kind of spoofs. Shuckers discussed the performance of various types of scanners against spoof fingerprints, and offered some theoretical protections in the form of "...anti-spoofing techniques that could be used that would make it more difficult to spoof a system" [22].

Following the discussion on ways to spoof fingerprints, In 2005, several papers were published that detailed approaches to what would become *liveness detection* in automated fingerprint scanners to start combating this issue. Moon et al. proposed a method for using wavelet (oscillation up and down) analysis on the tip of fingerprints to determine real fingerprints against fakes [18]. Rowe et al. used hybrid scanner technology, combining a "...multi-spectral imager with a conventional optical fingerprint sensor" in order to improve results with poor input finger data [21]. Jain et al. took advantage of scanner technology at the time in addition to configuring software to analyze fingerprint pores, which aided in spoof detection, and reduced fingerprint mismatches by up to 20% [13].

2.2 Modern Fingerprint Spoofing Research

The year 2008 saw one of the first uses of the phrase *liveness detection* in a paper published by Reddy et al. This paper proposed the use of "pulse oximetry" in combination with "...using the source of light originating from a probe..." to determine if a fingerprint was from a living individual or not [20]. The authors note that their experimental results "...demonstrate that the developed prototype can successfully thwart the spoof attacks (including those based on dismembered fingers)" [20].

This academic undertaking opened up the door into the study of a variety of liveness detection based systems to reduce fingerprint spoofing. Kumar et al. used liveness detection techniques to analyze finger veins in low quality images, ensuring liveness in the fingers being scanned as an anti-spoof measure. In their work, they established a fully automated pipeline for removing potential errant fingerprints and reducing spoofing by a significant margin [15]. Gragnaniello et al. analyzed prints, pixel-by-pixel, in combination with a optimizer to improve spoof detection significantly [7]. Later on, the same research group used a multi-phase analysis process to filter all fingerprints through a pipeline with machine learning techniques (using the public LivDet 2011 database). Eventually, the final phase, a classification system, made a binary decision on whether or not a print was real or fake [8].

2.3 Recent Anti-spoofing Results

The paper being examined, "Fingerprint Spoof Detector Generalization", details two specific approaches that the authors used to compare their results to. Both of these approaches, *Fingerprint Spoof Buster* and *Slim-ResCNN* are considered "...state-of-the-art spoof detectors..." [5]. Since these two are considered state-of-the-art, prior to the publication of "Fingerprint Spoof Detector Generalization", the results of both are considered the most recent anti-spoofing results available.

The first paper mentioned, "Fingerprint Spoof Buster", was also written by the research group of "Fingerprint Spoof Detector Generalization". The authors focused on using three datasets (LivDet 2011, LivDet 2013, LivDet 2015), in pair with a deep convolutional neural network to evaluate liveness spoof detection

on these datasets [4]. Their proposed system was tested across many common types of fingerprint sensors using four different techniques: intra-sensor, cross-material, cross-sensor, and cross-dataset. On the LiveDet 2015 dataset alone, the author's proposed system performed at 99.03% accuracy across all sensors, as opposed to the highest prior to that point of 95.51%.

As to the second paper, "Slim-ResCNN: A Deep Residual Convolutional Neural Network for Fingerprint Liveness Detection", this research group tackled the problem in a similar but different way. They, like the "Fingerprint Spoof Buster" group chose to use a CNN, or convolutional neural network, in order to attempt to perform liveness detection on images of fingerprints. The authors of this paper note that normally, "...the CNN structure used on natural images does not achieve good performance on fingerprint liveness detection..." [26]. In order to combat this limitation, the group made use of their custom framework, toting a "...lightweight yet powerful network structure..." that is "...specifically designed for fingerprint liveness detection without over-fitting and [uses] less processing time" [26]. The Slim-ResCNN outperformed the top models for LivDet 2013 and LivDet 2015, and won first place in the Fingerprint Liveness Detection Competition 2017, with an overall accuracy of 95.25% [26].

2.4 Datasets

There are various datasets published by previous researchers. Marasco et al., summarized 24 different datasets and classify them based on the sensor and technology [16]. 3 different technology have been widely used: Capacitive, Electro-optical, and optical. In the paper we are analyzing, Chugh et cl., use 3 different LiDet datasets (2011, 2013, 2015) and the MSU dataset.

Dataset	Sensor	Technology	Dataset	Sensor	Technology
LivDet 2011	Biometrika	Optical	LivDet 2015	Green Bit	Optical
	Sagem	Optical		Biometrika	Optical
	Digital Persona	Optical		Digital Persona	Optical
	Italdata	Optical		Crossmatch	Optical
LivDet 2013	Biometrika	Optical	MSU	Identix	Optical
	CrossMatch	Optical			
	Swipe	Optical			
	Italdata	Optical			

Table 1: 4 Main Datasets Used in the Paper [4]

3 Main Results

3.1 UMG Results Overview

As stated previously, the technique discussed in the paper "Fingerprint Spoof Detector Generalization" is based on the two older performance models: Fingerprint Spoof Buster and Slim-ResCNN. The new model, proposed by the "Fingerprint Spoof Detector Generalization" paper, is called the Universal Material Generator (UMG). The UMG is architectured specifically to perform well

"...against spoofs made from materials not seen during training..." [26]. In detail, the authors do this by taking the texture features of given, known, fingerprint images and synthesizing new materials to be added to the existing database.

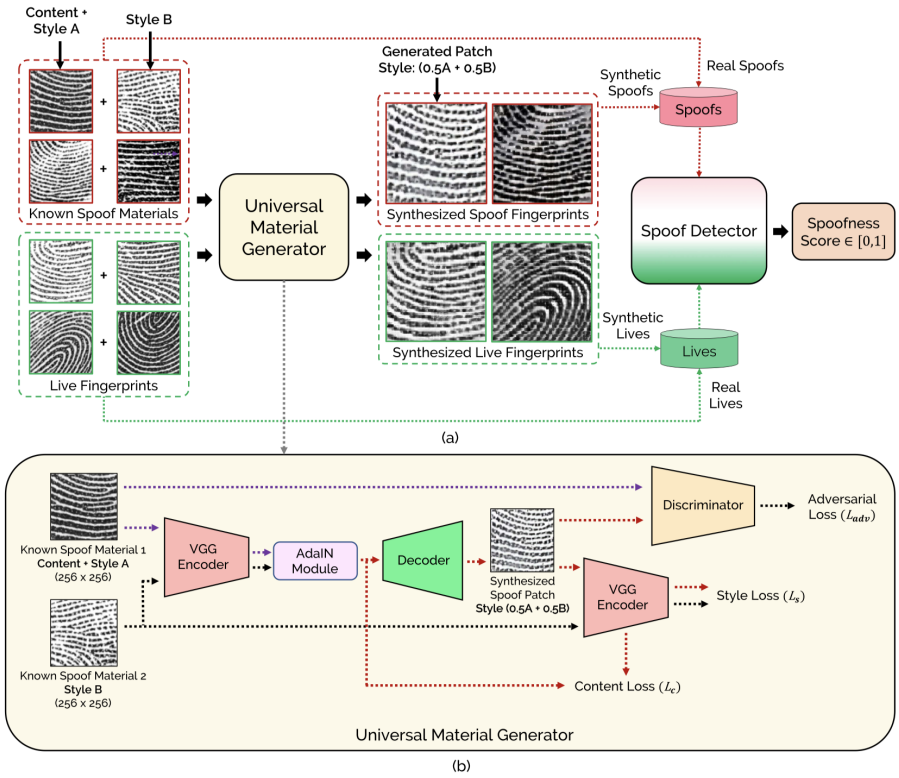


Figure 2: The structure of the Universal Material Generator (UMG) proposed by Chugh et al. [5]

3.2 UMG Input Data

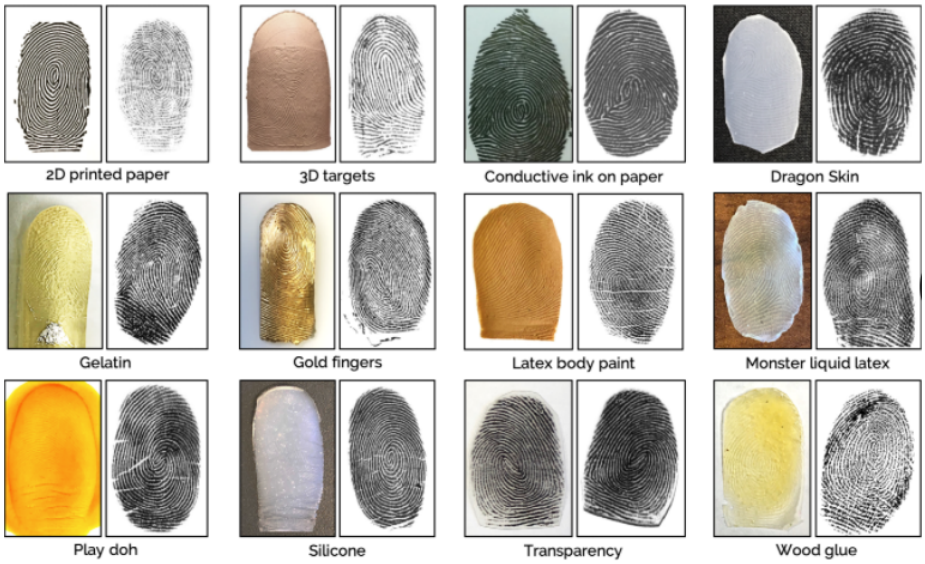
The first dataset the authors used to train and test their models against, the **MSU Fingerprint Presentation Attack Database** was a large dataset that contained **5,743 live images** and **4,912 spoof images**. This dataset in particular was used for the UMG as well; however, the UMG used this data to generate new spoof materials that it could train on. The dataset in question contained twelve different material types by default, all of which were represented to test the dataset [5]. These materials are displayed in Image 3. Inclusions that may appear particularly unorthodox are: Play Doh, wood glue, and gold.

The second dataset the authors used was the LivDet database, specifically the 2017 edition of the sets. This database has a collection of 17,500 images

and is publicly available. An additional feature of this dataset that makes it particularly useful for this research group is the fact that it makes use of three different types of fingerprint readers, and includes additional spoof materials that are not present in the MSU dataset [5].

In each experiment for any of the three techniques, an image is selected from a dataset. That image is centered, aligned, and split into several 96 x 96 pixel portions of the original image. These smaller "patches" focuses on all of the significant features of a given fingerprint, called "minutiae", at a given orientation and location [5]. Each of these patches is given a spoofness score, and once they have all been analyzed, the average spoofness score of all of these patches is determined and evaluated.

Figure 3: All Twelve Stock Spoof Materials Used in the Dataset [5]



3.3 UMG Performance Results

By making use of the same neural net (CNN), used by Slim-ResCNN and Fingerprint Spoof Buster and modifying it with the wrapper and additional synthetic spoofs, UMG was able to outperform both models in practice. The criteria the authors used for this particular paper is TDR @ FDR, provided by IARPA's Project Odin, which is based on their effort to perform accurate liveness detection [11]. TDR, or True Detection Rate is the ability of the fingerprint model to correctly distinguish a valid print. The FDR, or False Detection Rate is similar to an error term in a machine learning model, in that it shows how often the model makes a mistake. The UMG modification models' out-performance of the other two base models is clearly demonstrated in Table 2, all placed at a FDR @ 0.2% [26].

Performance Category	**Fingerprint Spoof Buster (TDR %)**	**UMG With Fingerprint Spoof Buster (TDR %)**	**Slim-ResCNN (TDR %)**	**UMG With Slim-ResCNN (TDR %)**
Overall	75.24	91.78	73.09	90.63
Cross-Sensor	67.60	80.63	64.62	77.59

Table 2: Performance of UMG against FSB and Slim-ResCNN

4 Techniques

4.1 Overview of the System Design

The authors' proposed methodology and system for processing and filtering real and fake fingerprints is a three step process [5].

1. "**Training** the Universal Material Generator (UMG) wrapper using the spoof images of **known** materials (with one material left-out from training)"
2. "Generating **synthetic** spoof images using randomly selected image pairs of **different but known** materials"
3. "Training a spoof detector on the **augmented dataset** to evaluate its performance on the 'unknown' material left out from training"

All of these are outlined in detail in the subsequent blocks.

4.2 Training the UMG Using Known Spoofs

The authors adopted a common, but effective tactic in order to train their initial UMG model with the already established and built data. They began using a pre-existing data of real, spoofed images called S^m_{real}, built from m different materials. They utilize a leave-one-out protocol, which is popular in many machine learning applications, and split the data into two sets. The first set contains spoof images that were made using the first $m-1$ materials, and is called the *known material set*. This set is used for training the system that is described in the subsequent section. The m_{th} material is deemed the *unknown material set*, and these are used for "...computing the generalization performance..." of the UMG. The results for which, are displayed in the previously shown Table 2.

4.3 Generating Synthetic Spoof Images using UMG Wrapper

The UMG, the authors' synthetic spoof generator, referred to for the sake of their research as G is comprised of two parts. The first part, called the *encoder*, is represented as $f(\cdot)$. The function $f(\cdot)$ makes use of the neural net used by Zhao et al. known as *VGG-19*, and takes the first four layers of this neural net

with pre-trained values [27]. In this case, pre-trained means that the weights for the whole network are completely fixed the entire time.

For the encoder stage, the available feature space (possible outputs) for all source images is called $f(c)$ or x and the available feature space for all target images is called $f(s)$ or y. These two parameters, x and y, are passed into an equation known as Adaptive Instance Norm (AdaIN), developed by Huang et al. [9]. This equation takes the general form:

$$AdaIN(x, y) = \sigma(y) \left(\frac{x - \mu(x)}{\sigma(x)} \right) + \mu(y) \tag{1}$$

In essence, this equation outputs the desired feature space $AdaIN(x, y)$ as a variable called t when provided the x and y from the encoder. AdaIN takes a source feature space, x, normalizes it to the proper domain bounds with $\sigma(y)$ and then shifts it appropriately using $\mu(y)$.

With the output of t from the encoder, the second phase of the spoof generation begins with the decoder. The output of the decoder takes the form:

$$T(c, s, a) = g((1 - \alpha) \cdot f(c) + a \cdot t)$$

where c and s are the same as before, and alpha represents the degree of newness to introduce to a new image. An α of 0 will rebuild the source image, and an α of 1 will construct a completely new image. The authors opted for a value of 0.5, to provide a middle ground between the source and the target, with equal blending. This function is combined with a patch loss function, whose purpose is to ensure that the "...synthesized spoof patches, i.e $g(t)$ do match the style statistics of the target material spoof..."[5]:

$$\mathcal{L}_s = \sum_{i=1}^{L} \|\mu\left(\phi_i(g(t))\right) - \mu\left(\phi_i(s)\right)\|_2 + \sum_{i=1}^{L} \|\sigma\left(\phi_i(g(t))\right) - \sigma\left(\phi_i(s)\right)\|_2 \tag{2}$$

The intricacies of this function are not detailed in the scope of this paper, but the authors do note that the four ϕ_i terms represent information gained through the four layers of the VGG-19 neural net.

4.4 Validating Synthetic Spoof Images

At this point, the functions have generated a synthetic spoof images of some description. However, the generated image is not guaranteed to appear as a real fingerprint image, nor does it face the same constraints that a naturally generated fingerprint image would possess. To combat this, the authors add two constructs to their pipeline: content loss and an adversarial supervision function.

The loss function is presented as so:

$$\mathcal{L}_c = \|f(g(t)) - t\|_2 \tag{3}$$

The purpose of this function is to make sure that spoofed images retain what the authors describe as "friction ridge", or the standard markings present in all fingerprints [5]. The function performs essentially a Euclidean distance calculation between the features of the synthetic image created, and the target features used from the original image.

In order to compliment the loss function, the authors make use of a generative adversarial network, or GAN, which consists of a generator G, and an adversary D. The goal of G is to generate real and spoofed fingerprint images to send to D, and D's objective is to tell G whether or not the image is legitimate or not. A given fingerprint spoof image is evaluated with the following functions:

$$\min_G \mathcal{L}_G = \lambda_c \cdot \mathcal{L}_c + \lambda_s \cdot \mathcal{L}_s + \mathcal{L}_{\text{adv}}^G \tag{4}$$

$$\max_D \mathcal{L}_D = \mathcal{L}_{adv}^D \tag{5}$$

which as can be seen, takes advantage of both the ability of the aforementioned patch loss function $\mathcal{L}_s$ and content loss function $\mathcal{L}_c$, combined with a weight parameter for each: λ_s and λ_c [5].

4.5 Training the Spoof Detector on Synthetic Images

After the UMG pipeline has been built and trained using the previous steps, the UMG needs to generate synthetic images for use in the two spoof detectors (Fingerprint Spoof Buster and Slim-ResCNN). The authors grab a set of fingerprint pair, which are unique and chosen at random. These images are all procured randomly from the total set of known spoofs. For every image pair in the created set, $(I_{m_1}^i, I_{mi}^i)$ s.t. $i \in \{1, \ldots, N_{synth}\}$ sourced from known but different materials $m_a, m_b, a \neq b$, the "friction ridge" representing the content of a fingerprint is chosen from the first selected image, and the "source material" representing the style of a fingerprint is chosen from the second image [5].

These two parameters are placed into the UMG, and used to generate a new spoof image S_{synth}^k [5]. After this is done for the entire set of the selected pairs, the new spoofed fingerprints are inserted into the old datasets to build new augmented training sets. A new UMG, called UMG_{live} is trained on the augmented dataset, and the process is repeated to build more spoof images. These spoof images are used to train the two spoof detectors (Fingerprint Spoof Buster and Slim-ResCNN), and thus, the detectors are able to achieve even better results on the original scanner runs and the hybridized scanner runs as well.

5 Discussion

5.1 Noah's Thoughts

This entire field of research seems very interesting to me, primarily because I had no idea that this was something that people in academia even researched. In the background reading and the paper we analyzed, it is evident that this line of research is much more populated that I had ever imagined. I also really enjoy how they are able to cross several domains like Machine-Learning, Cybersecurity, and Visual Processing into a single objective with very practical, very current applications. The topic will be of interest and concern as long as humanity chooses to use biometrics, which has no evidence of slowing down anytime soon.

Honestly, my biggest concerns for this paper have been from the reader's perspective as opposed to the integrity or value of the research. The over-reliance on the abstract description of the system they built through mathematics, as opposed to the lack of demonstration of the the physical meaning of their symbols made some parts very difficult to understand and read through. As a single example, the authors describe the synthetic fingerprint images with symbols like $I^i_{m_a}$ with no explanation of what computer science structure this is analogous to in their code. Does this represent an array, a bitmap, an actual file? With no link to the code for their system, I have very little understanding of what is going on from the computer science perspective to allow these systems to work.

The results of this paper seem fantastic, especially with how accurate they were able to make some the modern spoof busters using their modified techniques. I have no idea how someone is going to manage to top the results for the dataset in question for the overall results, because the amount is already nearing close to 100%. The hybridized models might be able to improve by testing even more unique fingerprint detector's data. In addition, I believe that building spoofs from uncommon materials and scanning pictures of these into a database would improve results even more.

I see no reason why something like the UMG system can't be applied to other facets of biometric analysis. Face scanners, hand scanners, various other kinds of biometric identification seem to be easy candidates for this kind of research.

I don't see an easy way to simplify their techniques; however, I think a lot of their writing can be streamlined for easier understanding. On the ordering of the UMG pipeline, it seemed like there was an abundance of unnecessary detail that did not follow through with proper symbol description, particularly in the mathematics heavy areas. The pipeline itself seemed to be a very cohesive process that used state-of-the-art pieces to build a complete end goal.

As for future work, I think this field is very data-dependent, and benefits when there is a new database published with more fingerprints and more fingerprint spoofs. As data accumulates, the researchers in this field will be able to construct even more accurate models from known spoofs and continue to improve their systems for the purpose of more accurate fingerprint spoof detection.

5.2 Steven's Thoughts

This paper introduces one way to generate unknown material spoofed fingerprints and offers a different view about defensing the spoofed fingerprint. Previous research focuses on what kinds of characters the real fingerprints have and spoofed fingerprint don't have, such as perspiration, while this paper does it reversely by focusing on the spoofed fingerprint and generating unknown material spoofed fingerprint for the recognition system to defense.

This model may encounter adversarial attacks. For any deep learning work, adversarial attacks are a huge problem. The generation of perturbation images can be relatively simple, but it could be really difficult defend potential attacks. The image below illustrates one kind of adversarial attack, where the researcher add some noise to the panda's picture to confuse the model; as a result, the model detect the image as a gibbon (with high confidence level) instead of a panda 4.

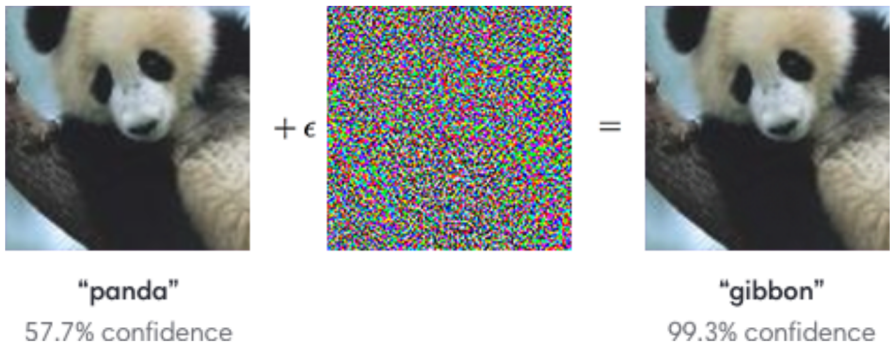


Figure 4: Adversarial Attack Example

In the paper we are analyzing, the same problem also presents. For a write-box attack, the attacker can use different ways to adjust spoofed fingerprint until the model wrongly predicts that it is a human with great high confidence. Similarly, in a black-box attack, this attacker can try different spoofed fingerprints to find the weakness of the system.

As we discussed in the dataset section, there are various fingerprint scan technologies, such as Capacitive, Electro-optical, and Optical. However, this paper only focuses on three LivDet data sets, LivDet 2011, 2013, and 2015. Since all LivDet datasets use optical technology, it provides a risk of mis-identification for data collected by capacitive or any other technologies.

For future work, I believe we can try to evaluate and adjust this model with other datasets that contain fingerprints collected by other scan technologies and that are even not from a real scan system to make it more complete.

References

[1] Zahid Akhtar, Christian Micheloni, and Gian Luca Foresti. Biometric liveness detection: Challenges and research opportunities. *IEEE Security Privacy*, 13(5):63–72, Sep 2015.

[2] Christoph Busch. Facing the Future of Biometrics. Demand for Safety and Security in the Public and Private sectors is Driving Research in this Rapidly Growing Field. *EMBO reports*, 7 Spec No(Spec No):S23–S25, Jul 2006. 16819444[pmid].

[3] UK National Cyber Security Centre. Biometric recognition and authentication systems. Jan 2019.

[4] Tarang Chugh, Kai Cao, and Anil K. Jain. Fingerprint Spoof Buster. 2017.

[5] Tarang Chugh and Anil K. Jain. Fingerprint spoof detector generalization. *IEEE Transactions on Information Forensics and Security*, 16:42–55, 2021.

[6] T. Dimkov and Wolter Pieters. Physical Penetration Testing: A Whole New Story in Penetration Testing. 2011.

[7] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva. Fingerprint Liveness Detection Based on Weber Local Image Descriptor. In *2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications*, pages 46–50, 2013.

[8] Diego Gragnaniello, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva. Local Contrast Phase Descriptor For Fingerprint Liveness Detection. *Pattern Recognition*, 48(4):1050–1058, Apr 2015.

[9] Xun Huang and Serge Belongie. Arbitrary style transfer in real-time with adaptive instance normalization, 2017.

[10] David Hutter. Physical security and why it is important. volume Information Security Reading Room. SANS Institute, Jun 2016.

[11] IARPA. Odin, Jun 2016.

[12] ISO Central Secretary. Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model. Standard ISO/IEC 7498-1:1994, International Organization for Standardization, Geneva, CH, 1994.

[13] A. K. Jain, Y. Chen, and M. Demirkus. Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(1):15–27, 2007.

[14] Alison Johansen. *Biometrics and Biometric Data: What is it and is it secure?*, Feb 2019.

[15] A. Kumar and Y. Zhou. Human Identification Using Finger Images. *IEEE Transactions on Image Processing*, 21(4):2228–2244, 2012.

[16] Emanuela Marasco and Arun Ross. A survey on antispoofing schemes for fingerprint recognition systems. *ACM Computing Surveys (CSUR)*, 47(2):1–36, 2014.

[17] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of Artificial "Gummy" Fingers on Fingerprint Systems. In Rudolf L. van Renesse, editor, *Optical Security and Counterfeit Deterrence Techniques IV*, volume 4677, pages 275 – 289. International Society for Optics and Photonics, SPIE, 2002.

[18] Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo. Wavelet Based Fingerprint Liveness Detection. *Electronics Letters*, 41(20):1112–1113, 2005.

[19] Chris Opfer. The Coca-Cola Hack and Who's on Hook for Office Cybersecurity. *Bloomberg Law*, Jan 2018.

[20] P. Venkata Reddy, Ajay Kumar, S. M. K. Rahman, and Tanvir Singh Mundra. A new antispoofing approach for biometric devices. *IEEE Transactions on Biomedical Circuits and Systems*, 2(4):328–337, Dec 2008.

[21] Robert Rowe, K.A. Nixon, and S.P. Corcoran. Multispectral fingerprint biometrics. pages 14 – 20, 07 2005.

[22] Stephanie A.C Schuckers. Spoofing and anti-spoofing measures. *Information Security Technical Report*, 7(4):56–62, Dec 2002.

[23] I Standardization. Iso/iec 7498-1: 1994 information technology–open systems interconnection–basic reference model: The basic model. *International Standard ISOIEC*, 74981:59, 1996.

[24] Jayson E. Street. Steal Everything, Kill Everyone, Cause Total Financial Ruin! (Or How I Walked In And Misbehaved). DEF CON, 2011.

[25] United States and Department of Justice. *The Fingerprint Sourcebook*. 2014.

[26] Y. Zhang, D. Shi, X. Zhan, D. Cao, K. Zhu, and Z. Li. Slim-ResCNN: A Deep Residual Convolutional Neural Network for Fingerprint Liveness Detection. *IEEE Access*, 7:91476–91487, 2019.

[27] Zhong-Qiu Zhao, Jian Hu, Weidong Tian, and Ning Ling. Cooperative adversarial network for accurate super resolution. pages 98–114, 2019.

6 Contributions

6.1 Contributions of Noah Dunn

Noah Dunn wrote the entirety of Draft 1 of this paper, updated presentation slides, accounting for 50% of the total project.

6.2 Contributions of Steven Yu

Steven Yu update the draft 2 based on Noah's draft 1, prepare the entirety presentation slides (Draft 1), accounting for 50% of the total project.