RESEARCH ARTICLE OPEN ACCESS

Fingerprint Sensor with Presentation Attack Detection

Manoj Kumar[*1], *Suhaib Ah. Khan*[#2], *Harsh Gupta*[#3], *SSD Ravi Kiran*[#4], *Parikshit Singh*[#5]
[*]*Assistant Professor, Department of ECE, SRM Institute of Science and Technology,*
[#]*UG Student, Department of ECE, SRM Institute of Science and Technology*
[#1] *Email: suhaib96@gmail.com*

***Abstract*:**

One of the major challenges facing biometric technology is the growing threat of *spoofing* (or *presentation attacks*). This involves a hacker intentionally assuming the identity of unsuspecting individuals (victims) through stealing their fingerprints, fabricating spoofs with the stolen fingerprints and maliciously attacking fingerprint recognition systems with the spoofs into identifying the hacker as the victim. To tackle this issue, we are presenting the prototype of an optical fingerprint reader. This is a low cost and easy to assemble reader and it provides a seamless and simple method for gaining more control over the sensing component of fingerprint recognition system. This reader is customized with two cameras for fingerprint acquisition with one camera providing high contrast, frustrated total internal reflection (FTIR) images, and the other camera outputting direct images. Using both of these image streams, we extract complementary information which, when fused together, results in highly discriminative features for detecting spoofs.

Keywords:

Spoofing, Presentation Attack, Frustrated Total Internal Reflection (FTIR), Optical Fingerprint Readers, Presentation Attack Detection, Local Binary Pattern (LBP)

I. INTRODUCTION

Science and Technology plays such as essential role in virtually all facets of our everyday life. Technology has given us, and continues to give us, one powerful tool after another. In this age, where data plays an almost central role in all technological fields, the protection of this data is imperative. Over time, different methods have been put forward and evolved to ensure the safety of this data. Consider an average human today, he spends around 2 hours per day on social media alone[1]. Hence the need for protection the privacy and data cannot be emphasized enough. Biometric technology is one such area that needs to be advanced and polished further. One of the major challenges facing biometric technology is the growing threat of Presentation Attacks (or more commonly known as spoofing). Spoofing involves a hacker intentionally assuming the identity of unsuspecting individuals (victims) through stealing their fingerprints and maliciously attacking fingerprint recognition systems with the spoofs into identifying the hacker as the victim.

The need to prevent presentation attacks is paramount due to the monumental costs and loss of user privacy associated with spoofed systems. Failure to detect presentation attacks could cause the disruption of a commerce system, compromise emails, banking information and other confidential information.

In an effort to mitigate the costs associated with presentation attacks, a number of presentation attack detection techniques involving both hardware and software have been proposed. Special hardware embedded in fingerprint readers enables capture of features such as heartbeat, thermal output, blood flow and sub-dermal finger characteristics useful for distinguishing a live finger from a spoof. Presentation attack detection methods in software are based on extracting textural, anatomical, and physiological features from processed fingerprint. Alternatively, a Neural Network can be trained to distinguish a live finger from a spoof.

Given the limitations of state-of-the-art fingerprint presentation attack detection (both in hardware and software); it is evident that much work remains to be done in developing robust and generalizable presentation attack detection solutions. One of the biggest limitations facing the most successful spoof detection solutions to date is the processed Commercial-Off-the-Shelf (COTS) fingerprint images used to train spoof detectors. In particular, because

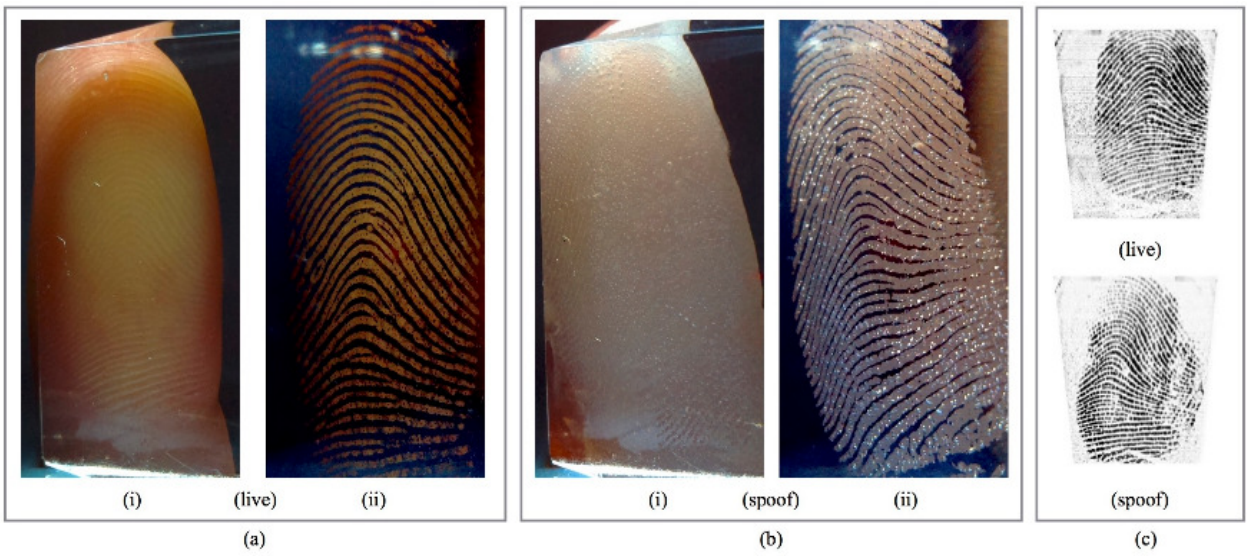

Fig 1. Fingerprint images acquired using the reader. Images in (a) were collected from a live finger during a single acquisition. Images in (b) were collected from a spoof finger during a single acquisition. Using features extracted from both raw image outputs ((i), direct) and ((ii), high-contrast FTIR), our spoof detection algorithms are able to discriminate between live fingers and spoof fingers. In particular, because the images in (i) and (ii) contain color information, discriminative color local binary patterns (CLBP) can be extracted for spoof detection. The raw FTIR image output (ii) can be post processed (after spoof detection) to output images suitable for fingerprint matching. Images in (c) were acquired from the same live finger (a) and spoof finger (b) on a normal optical reader. The close similarity between the two images in (c) qualitatively illustrates why current spoof detectors are limited by the low information content, processed fingerprint images output by fingerprint readers.

COTS fingerprint readers output fingerprint images which have undergone a number of image processing operations (in an effort to achieve high matching performance), they are not optimal for fingerprint spoof detection, since valuable information such as color and textural aberrations is lost during the image processing operations. By removing color and minute textural details from the raw fingerprint images, spoof fingerprint impressions and live fingerprint impressions (acquired on COTS optical readers) become very similar (Fig. 1 (c)), even when the physical live/spoof fingers used to collect the respective fingerprint impressions appear very different.

This limitation - inherent to many existing spoof detection solutions - motivated us to develop a custom, optical fingerprint reader, with the capability to output 2 raw images (from 2 different cameras) for spoof detection. By mounting two cameras at appropriate angles to a glass prism (Fig. 2), one camera is able to capture high contrast FTIR fingerprint images (useful for both fingerprint spoof detection and fingerprint matching) (Fig. 1 (ii)), while the other camera captures direct images of the finger skin in contact with the platen (useful for fingerprint spoof detection) (Fig. 1 (i)). Both images of our reader visually differentiate between live fingers and spoof fingers much more than the processed fingerprint images output by COTS fingerprint readers (Fig. 1 (c)).

Because both image outputs of the reader are raw and contain useful color information, we are able to develop robust fingerprint presentation attack detection algorithms. In particular, we can extract discriminative color local binary patterns (CLBP) from each of the image outputs. The color local binary patterns from each image contain complementary information such that when the features are fused together and passed to a binary SVM classifier, state-of-the-art spoof detection performance can be achieved.

Hence, the use of two cameras enables robust fingerprint spoof detection, since we can extract features from two complementary, information rich images instead

of processed gray-scale images output by traditional COTS optical fingerprint readers.

II. Construction And Calibration

In this section, the construction of the reader is explained. Below is the list of all the components.

A. Components

The following components are used in the design of the fingerprint reader:

1. Raspberry Pi
2. Raspberry Pi Camera Module
3. Camera Multiplexer[8]
4. Right Angle Prism
5. LEDs
6. Resistors

*1) Raspberry Pi:*A Raspberry Pi is a *Single Board Computer* (SBC) with 1.2 GHz 64-Bit quad-core CPU. It includes 1 GB RAM, a MicroSDHC Card slot. This device is used because of its excellent capability to handle image processing operations and its high processing abilities.

*2) Raspberry Pi Camera Module:*It's a 5.0 megapixel, 30 frames per second and a fixed focal length camera module for the Raspberry Pi SBC.

3) Camera Multiplexer: This module splits the Raspberry Pi camera slot into 2 slots, enabling the connection of 2 cameras simultaneously.

*4) Right Angle Prism:*An acrylic prism is used to allow the 2 cameras to take images at proper angles. Its sides have a dimension of 25mm.

5) Resistors and LEDs: These are used to illuminate the finger so that its features can be captured by the cameras and also to output the results and different stages of execution.

B. Construction

The construction of this reader adheres to the following steps. First the components enumerated above are assembled together according to the specifications as mentioned. The basic schematic diagram is shown in the Figure 2.

Because the Raspberry Pi only has a single camera connection port, a camera port multiplexer is used to enable the use of multiple cameras on a single Pi[8].Using the Raspberry Pi GPIO pins and the camera multiplexer, one can easily extend the Raspberry Pi to use multiple cameras.

An alternative approach is to attach one camera to the Pi's camera connection port, and a separate USB webcam to the Raspberry Pi USB port. This method was experimented with; however, the frame rate of the USB camera is significantly reduced on the Pi due to the latency of its Pi's graphics card. As such, using a camera multiplexer is recommended.

Once the components have been assembled, and the camera port multiplexed for two cameras, python scripts can be used to acquire two images from the fingerprint reader (one raw FTIR fingerprint image and another raw direct fingerprint image)

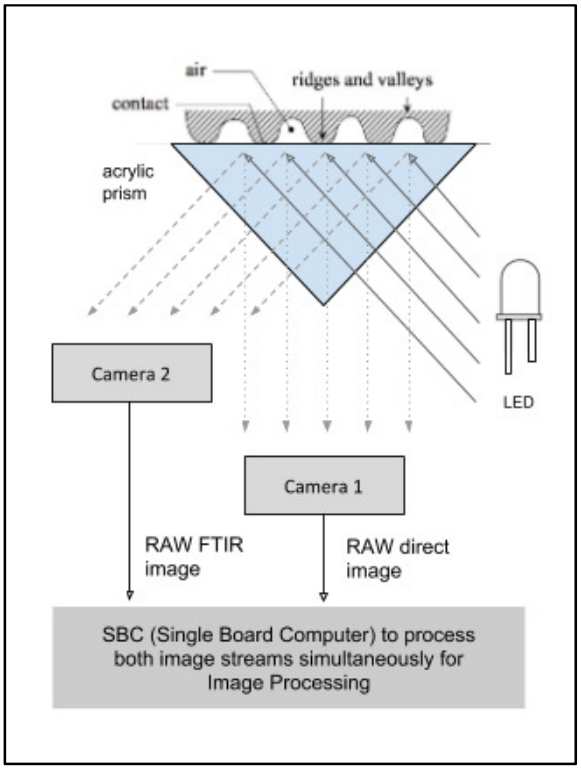

Fig 2. Schematic illustrating functionality. Incoming white light from three LEDs enters the prism. Camera 2 receives light rays reflected from the fingerprint ridges only (light rays are not reflected back from the valleys due to FTIR). This image from Camera 2, with high contrast between ridges and valleys can be used for both spoof detection and fingerprint matching. Camera 1 receives light rays reflected from both the ridges and valleys. This image from Camera 1 provides complementary information for spoof detection.

C. Image Processing

In order to be used for spoof detection, the reader must also demonstrate the ability to output high quality fingerprint images suitable for fingerprint matching. As previously mentioned, it performs spoof detection on non-processed, raw fingerprint images. While these raw images

are shown to provide discriminatory information for spoof detection, they need to be made compatible with processed images output by other commercial fingerprint readers.

Therefore, after spoof detection, the reader performs (1) *image enhancement* operations and (2) *image transformations* on the raw high contrast, FTIR image frames in order to output high fidelity images.

III. Results

Given a collection of live and spoofed fingerprint images, a number of spoof detection tests are carried out. Acquiring a fingerprint on the reader involves the same user interactions that any other regular optical reader does. A user simply places their finger on an acrylic prism. Then, the LEDs illuminate the finger surface and images are captured from both cameras over a time period of 1 second. The only difference in the acquisition process between any other reader and our reader is that this reader acquires two complementary images of the finger in contact with the acrylic platen from two separately mounted cameras.

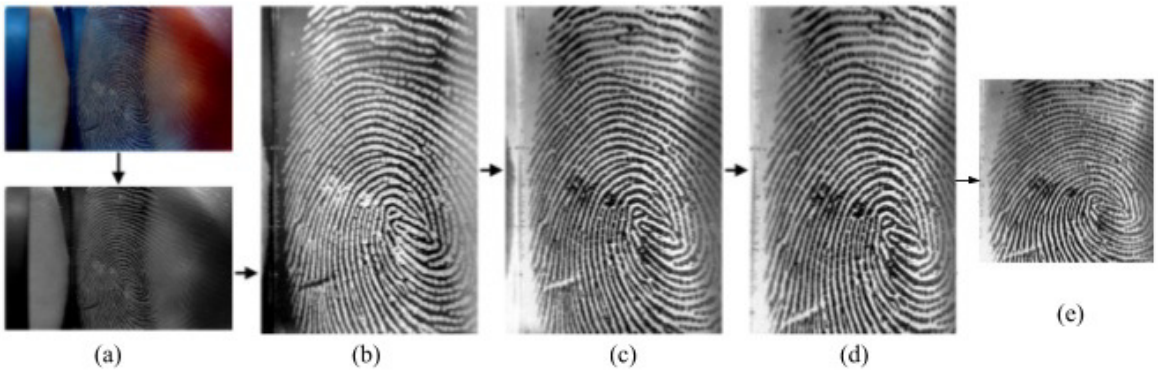

Fig 3. Processing a raw FTIR fingerprint image (a) The RGB raw FTIR image is first converted to grayscale. (b) Histogram equalization is performed on the grayscale FTIR image to enhance the contrast between the fingerprint ridges and valleys. (c) The fingerprint is negated so that the ridges appear dark, and they valleys appear white. (d) Calibration. (e) Scaling is applied to frontalize the fingerprint image to the image plane and down sample (by averaging neighborhood pixels) to 500 ppi in both the x and y directions.

1) Fingerprint Image Enhancement: Let a raw (unprocessed) FTIR fingerprint image from the reader be denoted as $FTIR_{raw}$.This raw image $FTIR_{raw}$ is first converted from the RGB color space to gray scale ($FTIR_{gray}$) (Fig. 3 (a)). Then, in order to further contrast the ridges from the valleys of the fingerprint, histogram equalization is performed on $FTIR_{gray}$ (Fig. 3 (b)). Finally, $FTIR_{gray}$ Is negated so that the ridges of the fingerprint image are dark, and the background of the image is white (Fig. 3 (c)).

2) Fingerprint Transformation: Following the aforementioned image processing techniques, the FTIR fingerprint images are further processed by performing a perspective transformation (to frontalize the fingerprint to the image plane) and scaling its PPI to 500 (the native resolution of the camera images is around 900 ppi) (Fig. 3 (d)).

All the above mentioned image processing is done using Python and OpenCVlibraries[9].

IV. Conclusion

We have designed and prototyped a custom fingerprint reader with ubiquitous components. By customizing our reader with two cameras for fingerprint image acquisition rather than one, we were able to extract discriminative color local binary patterns (CLBP) from both raw images which, when fused together, enabled us to match the performance of state of the art spoof detection methods (CNN).

Finally, by processing the raw FTIR images, we were able to output fingerprint images compatible for matching with COTS optical fingerprint readers.

We plan to integrate specialized hardware into this reader to enables future integration and modification of these additional hardware components.

V. REFERENCES

[1] Social Media Today, *How Much Time Do People Spend on Social Media?* https://www.socialmediatoday.com/marketing/how-much-time-do-people-spend-social-media-infographic

[2] Young-Hyun Baek. (2017). *Smart Optical Fingerprint Sensor for Robust Fake Fingerprint Detection. IEIE Transactions on Smart Processing & Computing*, 6(2), pp. 71-75. http://www.dbpia.co.kr/Journal/ArticleDetail/NODE07157699

[3] *Altered Fingerprints: Analysis and Detection*, Soweon Yoon, Student Member, IEEE, JianjiangFeng, Member, IEEE, and Anil K. Jain, Fellow, IEEE http://www.cse.msu.edu/~yoonsowo/Publications/AlteredFp_PAMI_2012.pdf

[4] *Spoofing Protection for Biometric Systems,* http://www.ijste.org/articles/IJSTEV1I10150.pdf *An Analysis of Altered Fingerprint Detection,Recognition and Verification* http://www.ijcsmc.com/docs/papers/January2016/V5I1201626.pdf

[5] Antonelli, Athos &Cappelli, Raffaele&Maio, Dario &Maltoni, Davide. (2006). *Fake Finger Detection by Skin Distortion Analysis. Information Forensics and Security*, IEEE Transactions on. 1. 360 - 373.

https://www.researchgate.net/publication/3455258_Fake_Finger_Detection_by_Skin_Distortion_Analysis

[6] *History of Fingerprint Removal - Case Studies* http://jimfisher.edinboro.edu/forensics/fire/print.html

[7] *Multi Camera Adapter module for Raspberry Pi* https://www.robotshop.com/en/arducam-multi-camera-adapter-module-raspberry-pi.html

[8] OpenCV Python library, https://pypi.python.org/pypi/opencv-python