Additive Manufacturing of 3D Face Masks for Biometric Spoofing

L. Christie[1], K. Mancuso[1], D. Fedorishin[2], P. Schneider[1], A. Stone[2], K. Oh[1,3]

[1] Dept. of Electrical Engineering , [2] Dept. of Computer Science and Engineering,
[3] Dept. of Biomedical Engineering
University at Buffalo, SUNY, email: kwangoh@buffalo.edu

ABSTRACT

Biometric security systems such as Apple's FaceID have replaced passwords for mobile device security, leaving users susceptible to biometric spoofing attacks. In response, Apple has implemented an anti-spoofing scheme, looking for autonomous ocular movement associated within the retina. This research aims to quantify the effectiveness of 3D printed spoof masks in regards to defeating a biometric anti-spoofing system such as Apple's iPhone X. 3D facial spoofs were created and tested using the iPhone X through 3D printing techniques and live casting. The 3D printed face masks were created from a 3D image utilizing a volumetric regression network. A series of anti-spoofing techniques were used as testing validation. These techniques range from measuring the thermal retention rate, stereoscopic facial image disparity map comparisons between a live face, and a spoof image, and implementation of multitask cascaded convolutional network for recognition of key facial features.

Keywords: additive manufacturing, biometrics, disparity map, facial spoofing, thermal retention rate

1 INTRODUCTION

In todays world, people are making the switch from conventional passwords, to biometric identification. Now that facial identification is becoming more prevalent, the data needed to unlock a persons phone is out in the open and posted all over the internet for the world to see i.e. pictures of one's face. This becomes problematic as now it is possible to pull photos from social media and create realistic 3D models [5]. Apple Inc. currently utilizes a facial recognition system called Face ID that operates by comparing two infrared generated images using pattern recognition to determine a match score for authentication [4]. In a parallel path, 3D printing has become more consumer friendly and has been used as the basis of spoofing a biometric system by hobbyists.

2 RELATED WORK

With mobile biometrics becoming more prevalent with systems like Apple's FaceID and Qualcomm's SENSEID, there are increased threat possibilities [1, 3]. Consequently companies now focus on implementing Liveness Detection Schemes as countermeasures. Apple implements a Liveness Detection Scheme which recognizes if the users eyes are open and ensures that they are directing their attention to the device before permitting access [2]. The rapid prototyping and modeling capabilities of 3D printing holds strong potential to be a means to generate accurate biometric spoofs.

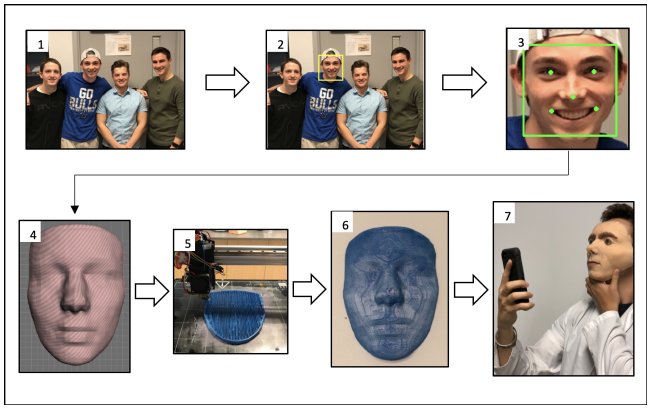

Figure 1: *Step (1) Pull a raw image from a public source. Step (2) Identify and crop the specific face to recreate. Step (3) The facial feature analysis conducted via software. Step (4) 3D modeling and post processing through MeshMixer and other 3D modeling programs. Step (5) The FDM printing of the face mask on the Folger Tech FT-5. Step (6) Analysis and post processing of the physical facial mask. Step (7) Use of the spoof to attempt to breach the iPhone X.*

3 METHODS

Two different forms of spoofs were created using both advanced manufacturing and traditional manufacturing methods. Using a fused deposition modeling method for printing of PLA and ABS, plastic face masks were created through a series of facial scans and volumetric regression networks [5]. Live cast masks were created through common molding techniques and were then formed using silicon rubber.

3.1 3D Printed Spoofs

Two different kinds of 3D printed facial spoofs were created. The first facial spoof was created through a 3D scan of the face, using a *XYZ Printing 3D Scanner 1.0 A*. This apparatus equipped with stereoscopic cameras, creates a 3D mesh of the face that can then be manipulated and trimmed using a common modeling software, Meshmixer. This face was then printed with polylactic acid (PLA) and Acrylonitrile butadiene styrene (ABS) using a FolgerTech FT-5 fused deposition modeling (FDM) printer. This is a market available FDM 3D printer that allows for a large surface print area and a 0.05mm print resolution. For the PLA face we printed with a hot end of 195°C, a build plate of 60°C, and infill of 15%. This print took roughly 8 hours and could be preformed with no support due to the structure. The ABS face required a hot end of 240°C, a build plate temperature of 70°C, and once again 10% infill density. This face allowed for an accurate representation of macro scale facial features such as eyebrows, lips, and nose and can be seen in Figure 2. For the ABS face spoof, alcohol vapor was used in order to smooth the edges of the mask.

Figure 2: *The side profiles of both the actual face (1) and the 3D printed face (2). The accuracy of the facial depth can be seen through nose structure and mouth structure. The front profile of a 3D printed face mask (3). The final scan 3D file from the facial scanner(4).*

A process flow for creating the second face model is outlined in Figure 1. The 3D face masks were created by implementing a volumetric regression network in order to predict the 3D features of the face from a single 2D image [5]. The network is capable of making accurate predictions due to its learned mapping between 2D images and 3D scans of the same faces in the images. The reconstructed 3D print file is a low resolution mesh structure requiring mesh optimization implementation in order to smooth the face model for better accuracy. This was then printed using the same process as the 3D scanning method and a final spoof can be seen in Figure 2. The ability to print a 3D reconstruction of the face from a single 2D image has large implications in the spoofing realm due to it's ability to create a facial spoof through easily accessible images pulled from something as easy as a social media profile.

3.2 Live Cast Spoofs

A live cast is the process of creating an accurate representation of a human feature or body part using molding material and in this case was used in order to replicate the facial features of a test subject. The process for mask creation can be seen in Figure 3. here a series of silicone based rubber materials were used to simulate human tissue [7] First, BodyDouble (Smooth-On, Macungie, PA 18062) was applied to a human test subjects face and allowed to dry for 20 minutes. It should be noted that this material is a non-toxic, non-hazardous material. After application and drying, the rubber BodyDouble was peeled off from the subject's face leaving a negative mold impression in the now solid rubber material. A sub-centimeter layer of Dragon Skin 10 Fast (Smooth-On, Macungie, PA 18062) was coating on the inside layer of the mask. This layer acts as the skin layer of the face and other features were recreated through other dyed silicon rubbers. Both a solid silicon face and a wearable mask with micro feature details were creating using this method and can be seen in Figure 3.

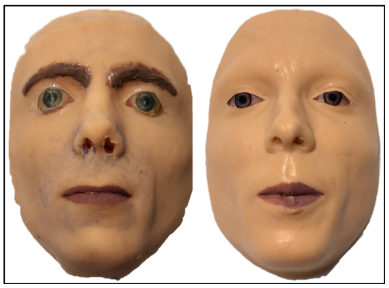

Figure 3: *Both Live Casted face spoofs. On the left is the face mask and on the right is the solid face mask.*

4 EXPERIMENTS

4.1 Facial Recognizer

To evaluate the general accuracy of our created face masks, we will employ a state of the art facial recognizer to determine whether these spoofs are classified as a face. To create a bounding box with facial key points around a detected face, we use a multitask cascaded convolutional network (MTCCN) [6]. In addition to detecting the face along with its key points, the MTCCN also aligns the face with respect to the size of the target image. An MTCCN works by predicting various bounding boxes across the image where the network believes there is a face. These bounding boxes are minimized down to a single bounding box using non maximum suppression, leading to the final detection of the face. Once the suppression is a applied, the facial key points are determined and categorized by five points located on the face. As shown in Figure 4, the MTCCN classifies both

the image of a real face and its corresponding spoof as true faces. The MTCCN also accurately predicts the location of the five facial key points on both the real and spoof face [6].

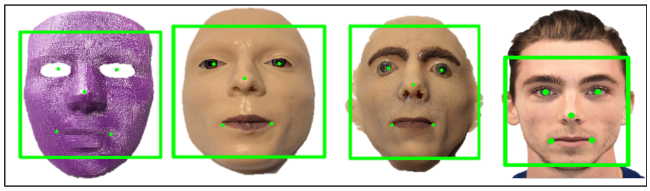

Figure 4: *Facial Recognizer tested on a 3D printed spoof, two Live Casted spoofs and a real person.*

4.2 Thermal Retention Rate

Thermal images of faces have proven useful in biometric identification systems [7]. Current biometric modalities for Face ID use thermal retention rate in order to preform Liveness detection. Thermal retention rate is the change in temperature over a selected period of time. When considering the human anatomy, the body can be treated as a capacitance of thermal energy with a continuous self regulating heat source known as the vascular system. As such one can expect to see an exponential decay in temperature difference between the body and surrounding environment. However, facial heat maps can be spoofed by heating a synthetic material spoof face to any desired temperature. A more robust thermal method for thermal anti-spoofing is by implementation of not a facial temperature change over time (dT/dt), but yet a rate of change of the temperature over time. This difference in heat dissipation time constants, or τ, can be seen in equation 1.

$$\Delta T(t) = \Delta T(0)e^{-t/\tau} \tag{1}$$

Where *T(t)* is the temperature of a body at time t Specifically, in the face there is a very consistent retention of temperature roughly being 37°C which can be measured by the infrared capabilities of a Face ID sensor. This retention has a very flat slope with a value of 0.0007 °C/s and can be seen in Figure 6. The three separate materials ABS, PLA, and silicon rubber used for facial spoofs were then tested under the same conditions. The faces were heated uniformly to a temperature that would represent the body temperature at the specific location of the lips. A FLIR infrared camera (FLIR Systems, Wilsonville, OR) was then used in order to measure live time temperature change on the face while also recording temperature maps of both the real face and the masks (Figure 5). The temperature data was taken over a period of 45 seconds the results of which can be seen in Figure 6.

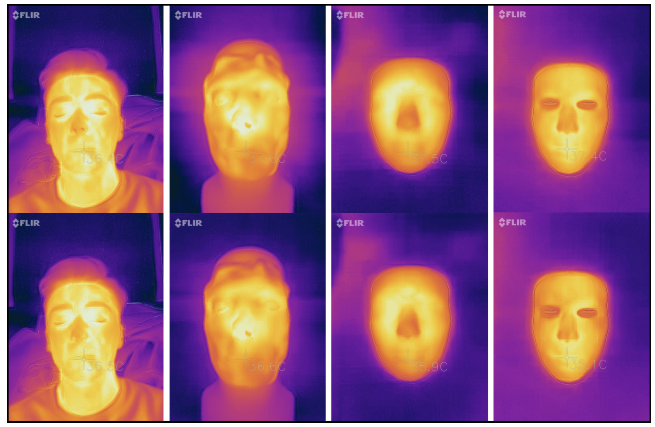

Figure 5: *Thermal Retention Rate in a real face, a live cast, PLA and ABS. The rate at which materials loose heat over time is shown through thermal images taken the second after heat has been applied (top) and again after 45 seconds (bottom).*

The material with the largest rate of change was the ABS facial spoof with a negative slope of -0.0361 °C/s. The PLA face was very similar to the slope of the ABS face with a value of -0.0351 °C/s. The closest match to the retention of the human face was -0.0158 °C/s.

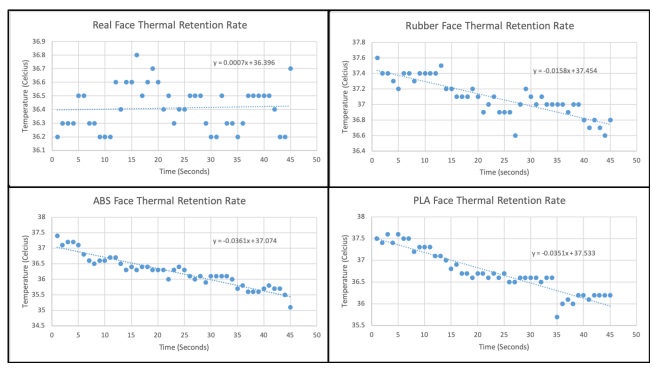

Figure 6: *Thermal retention rate graphs of three masks and the live face. Top left graph displays the Live face. The top right shows the synthetic spoof face. The bottom left shows the ABS mask and the bottom right is the PLA mask.*

4.3 Disparity Map Analysis

Disparity maps are respective 2D image representations of a 3D surface. 3D features can be seen as a gradient of colors from black to white with white being the closest proximity and black colors being the farthest. Four disparity maps for the actual face and consecutive spoof faces were created using the ZED Mini Stereo Camera. The camera resolution was set to 1920x1080 pixels per eye, combining to a total resolution of 3840x1080 pixels. The distance of the scans were set at two feet in order to receive an optimum scan of the face with mini-

mal noise from the surrounding environment. The four calculated disparity maps can be seen in Figure 7.

Figure 7: *Disparity map of the two facial spoofs and the actual face. Change in disparity can be seen as a gradient from black to white, being far to close proximity respectively.*

4.4 Breach Attempts

After the spoofs were successfully produced, they were then used in an attempt to breach the iPhone X's FaceID. Due to the fact that Face ID only offers acceptance or rejection feedback, additional metrics were necessary to quantify the accuracy of the spoofs. For this reason, the spoofs were first held up to the iPhone X and it was observed whether or not FaceID recognized the spoofs as faces. After observations were made, the spoofs that were recognized as faces were then used in an attempt to be registered in FaceID as a user. Finally, the spoofs were then used in an attempt to breach the iPhone X as seen in Figure 1.

5 CONCLUSION

Advanced manufacturing has proven its ability to spoof facial recognition biometric systems in terms of fast prototyping and accuracy. A series of 4 separate types of facial masks were created and tested. These masks used multiple materials such as PLA, ABS, and silicone. Advanced manufacturing and traditional manufacturing methods were also used and compared when creating these facial masks. It was found that the retention rate of plastic advanced manufacturing materials had a slope of -0.0351°C/s as compared to the real face with .0007°C/s. This requires adjustment in material and experimentation with new materials in the future. A facial recognizer utilizing a multitask cascaded convolutional network was created in order to identify specific facial features from a 2D image. This has applications such as picking specific faces from a crowd of people. We also were able to create disparity maps of the face and it's respective spoofs. This will be expanded on allowing for a confidence score to be assessed between a disparity map of the face and a disparity map of the spoof.

6 Future Work

Receiver operating curves (ROC) displaying both false acceptance and false rejection rates allow for a quantification of the validity of a biometric system. This research into spoofing could be applied to a facial scanner and then used to create a ROC curve showing the ability for the spoofs to effectively spoof the system. Further disparity map analysis on the 2D images utilizing a machine learning algorithm comparing the map of the real face to the masks will be done. This will allow for a confidence score rating of the spoofs as a comparison to the real face on a scale of 0-1. An increased amount of thermal retention rate testing could be done accompanying specific retention rates to different locations on the face such as the nose, lips, eyes. A material could also be found that closer resembles the trend of retention that the real face has, meaning that it would retain heat for a longer period of time. Finally, techniques such as stereo lithography will be implemented to attempt a higher resolution facial spoof.

REFERENCES

[1] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, 2013, pp. 1-6.doi: 10.1109/BTAS.2013.6712688

[2] N. Kose and J. Dugelay, "Countermeasure for the protection of face recognition systems against mask attacks," 2013 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), Shanghai, 2013, pp. 1-6.doi: 10.1109/FG.2013.6553761

[3] A.O. Alaswad, A.H. Montaser, F.E. Mohamad. "Vulnerabilities of Biometric Authentication Threats and Countermeasures". International Journal of Information and Computation Technology. Vol. 4. 2014. p 947-958.

[4] Apple Inc. "About Face ID Advanced Technology." 7 Nov. 2018, support.apple.com/en-us/HT208108.

[5] J.S. Aaron et al. "Large Pose 3D Face Reconstruction from a Single Image via Direct Volumetric CNN Regression". International Conference on Computer Vision, 2017.

[6] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao. "Joint face detection and alignment using multitask cascaded convolutional networks." IEEE Signal Processing Letters 23, no. 10. 2016. p 1499-1503.

[7] J.L. Sparks, et al. "Use of silicone materials to simulate tissue biomechanics as related to deep tissue injury." Advances in skin and wound care 28.2 (2015): 59-68.

[8] N. Sankaran, D. Mohan, et al. "Representation Learning Through Cross-Modality Supervision." International Conference and Workshops on Automatic Face and Gesture Recognition (FG), 2019.