Prosthetic Replacement for Fingerprint Biometric Authentication

Mian Wei
Prosthetic Aesthetics
Instructor: Paolo Cardini

ABSTRACT

The word prosthesis comes from Greek. It means 'in addition' (pros), 'to place' (tithenal). In English language, the meaning changes constantly. It is impossible now to obtain a definite explanation of what a prosthesis actually is. We could look into this puzzle through two perspectives and get a better understanding of the subject. From a broader point of view, a prosthesis could be anything usable. Any object that could potentially be used to serve a purpose by certain organism could be a prosthesis. The question, from this interpretation, is no longer about the object, but about the user. Life becomes the actual question. The answer lies in the connection. The cognizant relationship between an organism and an object is therefore definitive. From a narrower view, a prosthesis is a replacement or extension of certain body parts that performs the similar function of the original. A temporary tool that offers unrelated function is therefore not a prosthesis in this narrow interpretation.

Humans have replaced body parts and extended them for thousands of years. However, there are functions that cannot be rebuilt and identities that cannot be replaced. In recent years, fingerprint sensing became widely available as a mean to unlock houses and personal devices. This behavior is dangerous, because it uses a body feature that cannot be replaced or modified. The identification process is a matchless mean for criminal investigation, but not so suitable for personal security.

There are two objectives for this project. The first one is to find a way to use the advantage of the identification system, without losing the advantage of the analog key. The second objective is creating a device to protect your one-off body, and preventing it from being digitally recorded and leaked.

BACKGROUND

Duplicating a fingerprint using current technology is easy, whether using a mold of the actual finger or just an image of the fingerprint. In a case study conducted in Yokohama National University, researchers used plastic and molten gummy bears to examine the security of fingerprint sensing authentication measures.[1] They used the fingerprint impression on glass to first create a plastic mold, and then recreated the pattern with molten gummy. The gummy fingers had an acceptance rate from 68%-100%. They passed every security system tested. This study proved that duplicating fingerprint from an impression is fairly easy even with limited material. It is viable and would be simple for a hacker to collect dozens of fingerprints from a trashcan in a cafe, and those would all be irreplaceable for the victims. Similarly, an online program Tested examined the TouchID sensor with silicone duplicates of the finger.[2] They created a version of duplicate directly molded from the testing finger. The duplication worked flawlessly as well.

The TouchID on iPhone has a resolution of 500 ppi. It is similar to the standard of FBI fingerprint authentication. The resolution is enough for capturing the ridge contour but not for Level 3 features, e.g., pores (~60 micra).[3] A typical fingerprint has as many as 150 ridges, and the ridge width varies around 0.427 mm in females and 0.483 mm in males.[4] The natural structure of fingerprint has its advantage. It is large enough to be captured in close, but small enough to evade a far camera.

It is viable with technologies like laser etching or controlled chemical reaction to create a pattern with similar density that could be registered and identified by fingerprint sensing devices. A replacement is therefore technically possible.

RATIONALE

People have used analog locks and keys for centuries. Recent technological progress has urged people to upgrade to a more secure replacement, because there is not a lock that cannot be picked. A mechanical lock is vulnerable because it relies on defenseless mechanics. However, when people started upgrading to digital security measures, the key becomes the problem. Every password could be hacked leaked and spread. It is safe to say now, that there is not a key that cannot be duplicated. Fingerprint has its advantage, it is born with a physical body, and unique to each one. It's uniqueness is what made it so desirable for digital authentication. However, humans as social beings, are constant touching object and disposing them. An object could even be a medium for communicate meaning or emotion. In an objectified physical world, human leaves fingerprints everywhere. If a person's fingerprint is digitally recorded and leaked, he could never use it as a security measure anymore. The fingerprint is therefore not

[1] Matsumoto, Tsutomu, *Impact of Artificial "Gummy" Fingers on Fingerprint Systems*, 2002, Yokohama National University

[2] Tested, *Testing Apple's Touch ID with Fake Fingerprints*, 2014, https://www.youtube.com/watch?v=2u4ZLGsw1zo

[3] NIST Fingerprint Data Interchange Workshop, 1998

[4] Ashbaugh, D., *Quantitative-Qualitative Friction Ridge Analysis*, 1999, CRC Press

as bulletproof as people perceive. Further, fingerprints are irreplaceable, and therefore should be protected. It is safer if your finger leaves no trace when touching a physical object casually. We need two types prosthetics for this problem, the first is to replace fingerprint, and the second is to protect it. These devices would be considered as a new form of prosthetics because of both its intimate connection with the user and its relatable function to the human body.

OBJECTIVE

As previously sated, fingerprints are easily traceable, duplicable and irreplaceable. The first objective would be to find a way to replace fingerprint as personal security measure. There could be an alternative, by creating a physical object with similar uniqueness with digital process, and using the object as the key. If the creation process could be erased and made untraceable, it is possibly a better replacement. Therefore we could have a combination of a digital lock and an analog key, and it would be more secure than all traditional methods. It is nonetheless possible to create a duplication of the key, but it is far safer than the fingerprint that leaves trace everywhere. By making the object personal and close to you, it is harder to obtain than a digital password or microchip.

The second objective would be creating a form of prosthesis that protects the user’s fingerprints. It should be comfortable and unobstructive, not making casual daily task difficult to perform. It might also serve decorative purpose. If the prosthesis can have the aesthetics of a jewelry piece, it would be more practical and realistic.

In a world where society is shifting to a more dynamic form. The biometric identity should be protected. I hope to develop ways to use the biometric authentication system while keep your unchangeable biological self unrecorded. It presents the possibility that people could have a more fluid and objectified identity in the modern society. This project also seeks to raise awareness of the problem this type of freedom might cause. It would no longer be your body that defines you, but your machines and objects.

POSSIBLE OUTCOME

There would be three stages to this project. I hope to complete all three and present all the outcomes in this limited timeframe.

Stage 1:

First stage is to develop a physical object that could potentially replace fingerprints. It would be a small object, enough to be kept on a keyring. The first step would be develop an algorithm to create a random pattern that has similar ridge density to a fingerprint. The pattern could then be 3D printed or laser etched to create a mold. This mold would then be used to create the actual prosthesis. The object would possibly be made of conductive silicon or rubber, that could be register capacitively and graphically on an iPhone TouchID sensor. After the object is recorded by the sensor, the possibility of using it daily as an iPhone 'key' is then examined.

Stage 2:

The second stage is to develop a more personal prosthesis. It could possibly be a ring or another form of body attachment. The micro pattern used on the object could have a personal connection with the user (e.g., the fingerprint of a deceased family member).The possibility of an analog way to create the micro pattern will also be examined. The ideal design would be a chemical kit that user could use to grow his own micro pattern by mixing different chemicals, because the unpredictable nature of the chemical process, each pattern would be unique, similar to fingerprints. The resulted pattern could then be mounted on a ring and wore by the creator as a unique 'key' for his personal devices.

Stage 3:

The third stage would be finalizing all the succeeded designs and creating another prosthesis. The new prosthesis would be a form of body ornament that has the function to hide your fingerprints. It would prevent the user from leaving fingerprints everywhere. Custom micro pattern would be possible to mount on this new prosthesis. Therefore, instead of leaving fingerprints everywhere, the user would leave a personalized pattern (e.g., a micro photo) on daily objects. It would also be possible to use this device to register on and unlock personal devices.