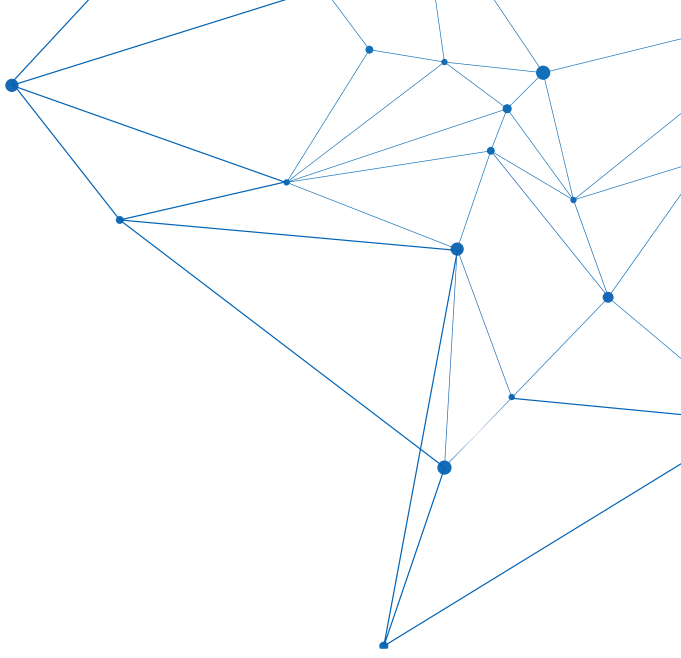
NOVETTA

Spoofing Capacitive Fingerprint Sensors:

Creating and Testing Conductive Artifacts

July 2014 | novetta.com |



NOVETTA

Spoofing Capacitive Fingerprint Sensors

NOVETTA

INTRODUCTION

Successful, secure applications of biometric technology require government and commercial users to assess vulnerabilities to spoofing or masquerade attacks. Such attacks are made with artificial physical biometric samples, also known as artifacts.

This white paper discusses methods and findings from one of Novetta's many approaches to vulnerability assessment: the fabrication of non-gelatinous artifacts for capacitive fingerprint sensors. We present methods of evaluating artifact performance relative to that of live presentations and gummy fingerprint artifacts. Two sets of artifacts are comprised of latex face paint or acrylic fabric paint and coated with a thin layer of Bare Conductive Paint. The third set of artifacts is comprised of latex face paint coated with a thin layer of delicatessen gold leaf.

The novelty of these artifacts is their stability in shape and function over periods of time and repeated presentations to the sensor.

FINGERPRINT SENSORS: PREVALENCE AND SECURITY

Fingerprint sensors are considered especially susceptible to physical spoofing attacks. Fingerprint artifacts can be fabricated using a cooperative donor, a non-cooperative donor, a reverse-engineered presentation from a biometric template, or a latent fingerprint.

Proliferation of biometric devices is not limited to deployment at borders and in access control. Consumer and government applications increasingly integrate biometric devices for unsupervised user authentication. Disruptive solutions in the fields of health, education, travel, and banking aim to deliver authentication at the user's convenience, anytime and anywhere. Realization of this aim complicates biometric security by adding corresponding requirements for scalable infrastructure, identity data management, and security measures against physical spoofing attacks.

The following examples are use-cases and environments requiring effective user authentication and counter-spoofing measures.

Securing Mobile Biometrics

Mobile devices are increasingly used for tasks that require reliable user authentication and signal transmission security. Companies are progressively relying on completion of tasks outside of their facilities. Reliable remote access and authentication is necessary to ensure the security of proprietary information. Reliable authentication adds value to the private sector by adding security to business functions otherwise compromised by mobile device platforms.

Preventing eGovt Abuse

Electronic government services allow streamlined processes to be completed using electronic signatures instead of physical verification and hardcopy documents. A case of stolen identity can have immense consequences to a user spanning multiple areas of the eGovernment service infrastructure.

Ensuring Mobile Healthcare Integrity

Mobile health enables seamless coordination with medical professionals, communication of sensitive information over distances, and real-time analysis of medical device and sensor feedback. Compromised information from false authentication can have serious implications for these processes.

PRIOR EVALUATIONS OF CONDUCTIVE ARTIFACTS

Artifact resistance testing can mitigate anticipated attacks by identifying vulnerabilities, quantifying the practical risks associated with such vulnerabilities, and establishing effective counter-measures. It is crucial to utilize testing procedures that enable a fair and accurate evaluation of the true performance of a sensor against a realistic spoofing attack.

A central component of artifact resistance testing is the artifact itself. Artifact resistance testing of capacitive sensors is often carried out using artifacts that change in dimension over time. Using dimensionally stable artifacts for these tests allows for a more realistic, representative, and broader range of testing opportunities, particularly for silicon sensors based on capacitive technology. Capacitive sensors function based on the conductivity of human skin. Upon finger contact with the sensor platen, the platen and skin form a capacitor.

Initial spoofing studies focused on the fabrication and use of gelatinous artifacts to circumvent capacitive sensors [1]. Successful presentations were possible due to the water content of these artifacts. A variety of gelling materials were used including gelatin and glycerin [1] [2]. A drawback of gelatinous or water-based artifacts is their change in shape over a period of hours or days. Dimensional changes of these artifacts prevent testing over extensive durations.

While these studies provided useful foundational insights into fingerprint sensor vulnerabilities, the limitation of spoofing experiments to gelatinous materials is not realistic for simulating biometric sensor attacks in the field. The growing amount of multi-purpose materials in consumer markets has increased the number and variety of potential artifacts.

Improved capacitive artifacts were discussed by Tsutomu Matsumoto. Using silicone rubber loaded with 12-16% carbon black produced the required conductivity to produce a biometric presentation on the platen [3]. These silicone/carbon black artifacts were reported successful against capacitive fingerprint sensors. Silicone rubber was used in liveness detection studies and by attackers in the field [1] [4]. Carbon black is a popular and readily available additive used to improve electrical properties of materials. Physical stability is not discussed; however, the absence of water content in these artifacts is an important step in improving artifact resistance studies.

Development of standardized measurements and customizable artifacts has the potential to mitigate threats directed at capacitive biometric sensors.

DESIGN CONSIDERATIONS WHEN CREATING ARTIFACTS

Creating stable capacitive artifacts includes several design considerations described below. Formulations of artifacts used in this study were designed based on these considerations. All artifacts used in this study were fabricated from molds of genuine fingerprints.

Design Consideration 1: Similarity of Material Properties to Human Skin

Fingerprint sensors of various types (e.g. optical, capacitive) each respond to specific properties of human skin. In the case of capacitive sensors the inherent electrical conductivity of human skin drives the biometric collection. Use of materials that mimic human skin is necessary for sensors to successfully record a fingerprint. Core material properties are listed in Table 1.

Material Property	Target Value	Artifact Application
Tensile Strength	7 MPa	Force exerted on artifact
Tensile Strain	100%	Deformation during fabrication and use
Compressive Strength	20 MPa	Limit for non-elastic materials
Shear Strain	100%	Requirement to imitate skin during shear
Hardness	15-40 (Shore A)	Enables presentation on sensor platen
Electrical Resistance	0.002-20 MΩ	Presentation will be visible by sensor

Table 1: Properties of ideal capacitive artifact

The first five properties in Table 1 are requirements for all fingerprint artifacts presented to the platen during fingerprint collection; however, the last is specific to spoofing capacitive fingerprint sensors. Artifacts used on capacitive sensors must conduct electricity similar to glabrous human skin, which typically has a resistance of 2 kΩ – 2 MΩ [5], but can be up to 20 MΩ for dry skin.

An artifact with low electrical conductivity (high electrical resistance) may result in a capacitive sensor collecting a fingerprint similar to dry skin. However, if the conductivity is too low or too high, the sensor may not recognize the presence of the artifact and fail to collect any fingerprint.

Design Consideration 2: Time Scale of Consistency

Effective artifacts must sustain deformation during fabrication and use, have physical stability during handling, and maintain performance characteristics through storage and repeated use. The main deficiency with gelatinous artifacts used in prior work is their limited shelf life. Gelatinous material's electrical resistance is due to water content, which leaves the material extremely susceptible to degradation due to changes in environmental temperature and humidity.

Design Consideration 3: Availability of Materials

Ideal artifacts should be made of readily and consistently available materials. In the past, readily available materials only included those attainable from common brick and mortar stores. Today, globalization and the internet allow more specialized, high-quality materials to be considered readily available due to specialty websites and international shipping.

In this white paper, readily available materials were defined as materials available to and used by consumers without needing specialized facilities for handling and those that contain no known hazardous materials. Modification of materials

was considered provided the modification process was not more complex than that of gelatinous artifacts.

CREATING CONDUCTIVE ARTIFACTS FOR TESTING

This study involved designing, creating, and testing conductive artifacts with the purpose of:

- Showing that comparable artifacts are not limited to traditionally-used materials
- Evaluating these artifacts' functional constraints in realistic attack settings

It is difficult to find a single material that emulates both the mechanical properties of human skin and skin's conductivity. Therefore this study focused on layering materials to create a stable artifact that does not rely on liquid content for its conductivity. The designed artifacts contain two layers for distinct functions: one for emulating physical deformation, and one for emulating conductivity.

Three kinds of artifacts were created in this study. Two used latex face paint and one used acrylic fabric paint for the first layer. These materials were chosen for their ability to replicate fingerprint features. Edible gold leaf and Bare Conductive Paint were chosen for the second layer. Although gold leaf is typically used in gourmet dishes for aesthetic reasons, it is conductive without modification and can form a sufficient contact with many surfaces. Bare Conductive Paint is a paintable conductor used for designing circuits on non-traditional surfaces such as paper. An example of these artifacts is shown in Figure 1 through Figure 3.

Artifact fabrication includes depositing layers of latex face paint or acrylic fabric paint into a cooperative mold, then coating it with edible gold or Bare Conductive Paint. Typical of gold leaf surface depositions, the thin gold layer must be gently pressed, and guided to the desirable area on the surface. The thickness that produced enough conductivity to appear on the sensor was 0.13 microns. Bare Conductive Paint was deposited onto the substrate surface in a single layer and allowed to fully dry before use. The gold leaf and Bare Conductive Paint depositions determine the appearance of the print on the sensor and the number of details present including creases, interstitial ridges, and unwanted artifacts

Figure 1: Conductive artifact – latex face paint with edible gold leaf coating

Figure 2: Conductive artifact – latex face paint with Bare Conductive Paint coating

Figure 3: Conductive artifact – acrylic paint with Bare Conductive Paint coating

Gelatinous artifacts are relatively easy to fabricate. Due to the delicate nature of working with gold leaf, the latex face paint and edible gold leaf artifact is more difficult to fabricate.

TESTING CONDUCTIVE ARTIFACTS

Performance of the designed artifacts was compared to the performance of traditional gelatinous artifacts and live presentations. Three evaluation criteria were used:

- Ability to replicate biometric details and present them to a capacitive fingerprint sensor
- Stability of form and function of the artifact
- Ease of fabrication from materials that are readily available

The prime goal of testing a capacitive artifact is to present it as a genuine biometric to the capacitive fingerprint sensor. This includes effective replication of features and maintained conductivity for the desired amount of presentations.

Initial biometric testing was conducted using the following artifact types:

- Gold / latex artifacts
- Bare Conductive Paint / latex artifacts
- Bare Conductive Paint / fabric paint artifacts
- Gelatin artifacts

Ten artifacts of each type were used per testing iteration; each testing iteration included twenty presentations. For reference, live (non-artifact) presentations were also taken.

The tests were conducted using an UPEK Eikon model 700 fingerprint sensor. Neurotechnology VeriFinger software was used for fingerprint enrollment and matching.

In this study, the match threshold used is represented by false acceptance rate (FAR). The FAR used was 0.01% (1 in 10,000). For the software used this FAR corresponds to a comparison score of 48. Any comparison score < 48 is not considered a match.

Gelatinous artifacts did not survive the biometric testing procedure. Artifacts cracked after repeated presentations. The quantity of presentations is drastically lower for gelatinous artifacts, around 5-6 per artifact, due to physically breaking during testing.

Figure 4: Biometric sample from a gold leaf and latex face paint artifact

Artifacts comprised of edible gold leaf did not have the same issue. A biometric presentation using these artifacts is shown in Figure 4.

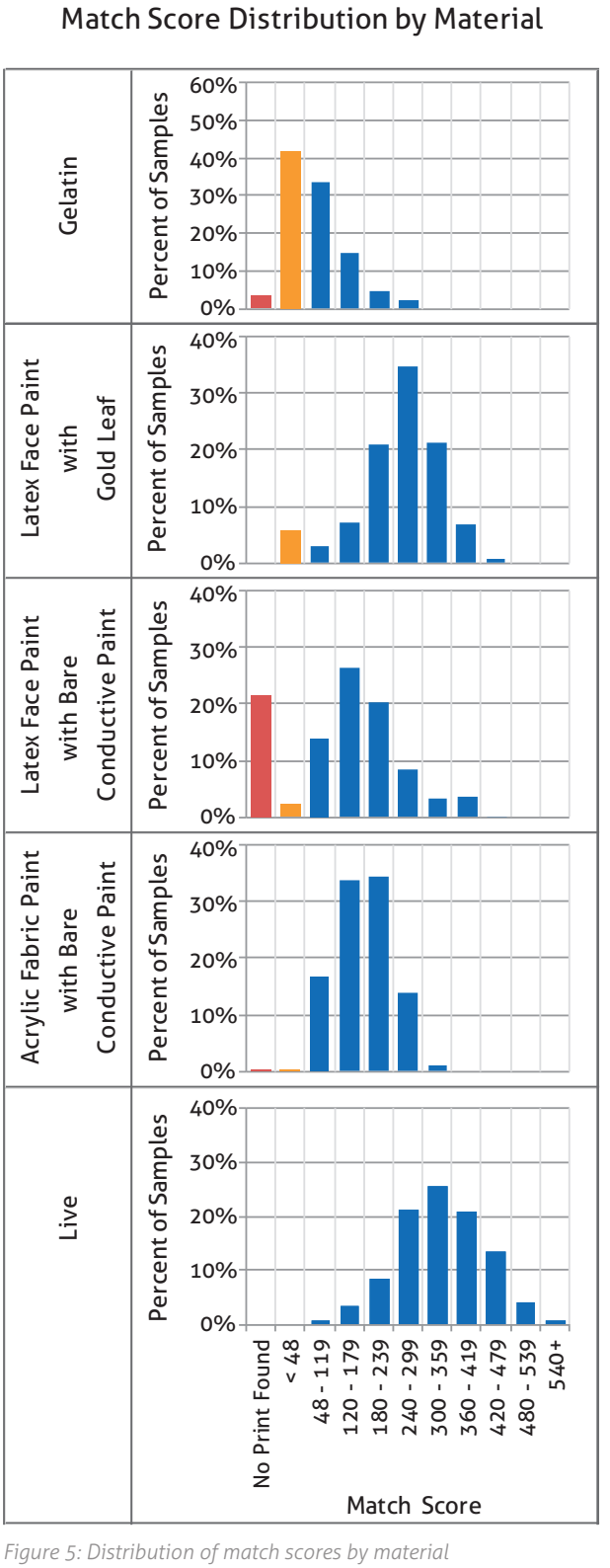


Figure 5: Distribution of match scores by material

TEST RESULTS: OVERVIEW

Figure 5 shows the match score distribution for the five materials tested (four distinct artifact types and live, genuine presentations). Scores below 48 are considered non-matches; scores above 100 can be considered strong matches. For identification, scores above 200 may be necessary. Presentations in which the sensor could not detect a print are shown as No Print Found.

Results indicate acrylic with Bare coating artifacts produce the fewest samples that fail to positively match. Latex with gold coating artifacts obtain the highest match scores in a spread most similar to live presentations. However, no artifact types achieved the same performance as live presentations.

TEST RESULTS: DESIGN CONSIDERATIONS

Design Consideration 1: Materials

A large percentage of No Print Found errors indicates that the artifact material did not successfully mimic the material properties of human skin. This error occurred most often for latex with Bare coating artifacts. Gelatin and acrylic with Bare coating artifacts had some No Print Found errors, but at a much lower rate.

Design Consideration 2: Consistency

Artifacts with a large percentage of match scores < 48 failed to consistently present a stable and reliable biometric to the sensor. Although all materials tested (excluding live, genuine samples) resulted in some presentations with a match score < 48, this occurred most often for Gelatin artifacts and least often for acrylic with Bare coating artifacts.

Design Consideration 3: Availability

Gelatin artifacts are comprised of the most readily available materials and can be fabricated from any gelatinous substance and water. Fabrication of other artifact types requires edible gold leaf or Bare Conductive Paint. Although these materials are available in specialty stores and through delivery, both are less common than gelatin.

CONCLUSIONS

Testing artifact resistance of capacitive fingerprint devices is an integral part of the biometric problem space. The growth of capacitive fingerprint sensors in current and expanding applications including unattended scenarios is a motivation behind the developed conductive artifacts for capacitive sensors.

Performing comprehensive assessments of device security and vulnerability to spoofing should include stable artifacts that go beyond currently used gelatinous artifacts that lose form and biometric features beyond several hours at room temperature. This paper investigated efficacy of three stable artifacts against live and gelatin artifact presentations.

Gold leaf and latex face paint artifacts were fabricated and tested. It was shown that more diverse artifacts can be made using traditional spoofing techniques. These artifacts were compared with gelatinous artifacts from a cooperative mold. Although the gelatinous fingerprints were easiest to fabricate, artifacts comprised of latex and edible gold leaf were the most effective over a prolonged duration and successive applications to the sensor. They were able to present biometric features throughout the entirety of testing.

Both latex with gold coating and acrylic with Bare Conductive Paint coating artifacts show promise in creating conductive artifacts that can be used consistently for long term testing and security evaluation of capacitive fingerprint sensors.

KEY POINTS

- **Artifacts that emulate relevant physical properties of fingerprints outperform those based on generic materials (e.g. gelatinous).**
- **While live presentations generate higher comparison scores than artifacts, certain artifacts generate scores sufficient for reliable verification and identification.**
- **Practical evaluation of vulnerabilities to spoofing requires consideration of material availability and durability.**

References

[1] *T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of Artificial "Gummy" Fingers on Fingerprint Systems," Proceedings of SPIE,, vol. 4677, 2002.*

[2] *A. T. Claude Barral, "Fake Fingers in Fingerprint Recognition: Glycerin Supersedes Gelatin," Formal to Practical Security Lecture Notes in Computer Science, vol. 5458, pp. 57-69, 2009.*

[3] *T. Matsumoto, "Gummy and Conductive Silicone Rubber Fingers," International Association for Cryptologic Research, vol. 2501, pp. 574-576, 2002.*

[4] *"Doctor 'used silicone fingers' to sign in for colleagues," BBC, 12 03 2013. [Online]. Available: http://www.bbc.com/news/world-latin-america-21756709. [Accessed 15 04 2014].*

[5] *S. W. Wolfe, R. N. Hotchkiss, W. C. Pederson and S. H. Kozin, Green's Operative Hand Surgery, 6th Edition, Elsevier, 2011.*

NOVETTA

From Complexity to Clarity.

Headquartered in McLean, VA with over 700 employees across the US, Novetta has over two decades of experience solving problems of national significance through advanced analytics for government and commercial enterprises worldwide. Novetta's Cyber Analytics, Entity Analytics and Multi-INT Analytics capabilities enable customers to find clarity from the complexity of Big Data at the scale and speed needed to drive enterprise and mission success. Visit HYPERLINK "http://www.novetta.com/"www.novetta.com for more information.

7921 Jones Branch Dr, Suite 500
McLean, VA 22102

(571) 282-3000
novetta.com

@novettasol
novetta