Fingerprint Replication Utilizing Latent Fingerprints for Conducting Forensic Analysis on Mobile Devices with Biometric Security

R.J. McDown,[1] BS*; Josh Sablatura,[1] BS*; Lei Chen,[1] PhD; and Jorn C.C. Yu,[2] PhD, D-ABC

[1] Department of Computer Science, Sam Houston State University, Huntsville, TX 77340
[2] Department of Forensic Science, Sam Houston State University, Huntsville, TX 77340

ABSTRACT

A fingerprint replicate was successfully produced from a latent fingerprint in our lab in order to test biometric security. In our process, a latent fingerprint was first visualized from the surface of a mobile device and a 3D mold of the fingerprint was created from this 2D image. The fingerprint replicate produced from this 3D mold could successfully login to the mobile device via a biometric fingerprint scanner. Our process potentially can be used to gain access to a mobile device during the course of a forensic investigation for both civil and criminal cases.

INTRODUCTION

In recent years, there has been a substantial increase in the number of mobile devices that society uses everyday. According to the 2012 IBM Tech Trends Report, which surveyed more than 1,200 IT professionals, "[b]y the end of 2012, mobile devices are expected to outnumber people […] with the world generating 15 petabytes of new data every day." [1]

With the increasing presence of mobile devices in society, these devices can be an indispensable source of evidence in both criminal and civil prosecutions. Evidence that can be obtained from these devices include photos, emails, calendar events, GPS data, message data, and call history. [2] This data can be essential in the reconstruction of timelines and events in the prosecution of the case.

In order for this evidence to be admissible in court it must be extracted from the mobile device in a forensically sound manner. Current forensic extraction techniques require the use of hardware devices such as a JTAG, or the use of software tools to obtain either a logical or physical extraction of the data. These tools often rely on the ability to interact with the devices operating system or hardware in order to execute arbitrary code on the device either during a reboot, or at runtime. This often requires the device to be unlocked prior to data extraction, meaning that the investigator must have prior knowledge of the user's password, or the resources to brute force the password.

However, these methods are not always implementable under the following conditions: the device allows a limited number of pin code entries before the device locks itself or wipes the data, the operating system does not have a known security bypass, or the data on the device is encrypted rendering a physical data extraction useless.

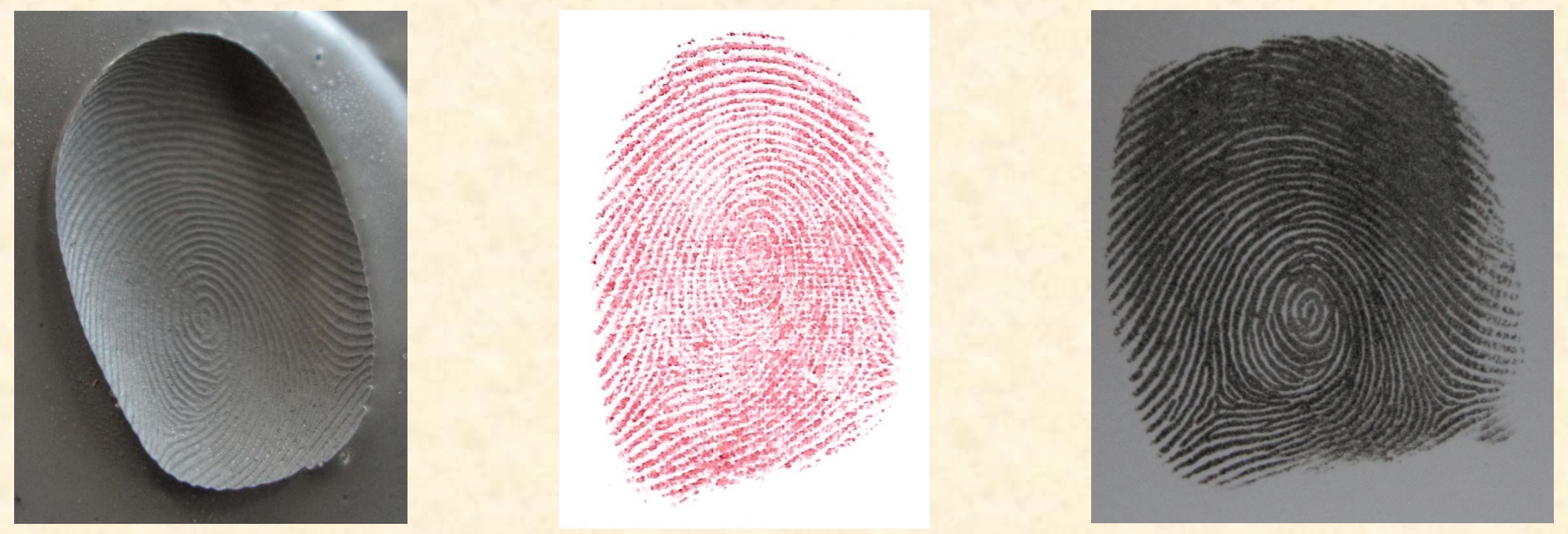

Figure 1: (L-R) (1) Negative mold of a fingerprint captured by directly molding the finger with forensics molding putty. (2) Raw inked print created with a stamp ink pad. (3) Raw inked print created with a fingerprinting ink pad.

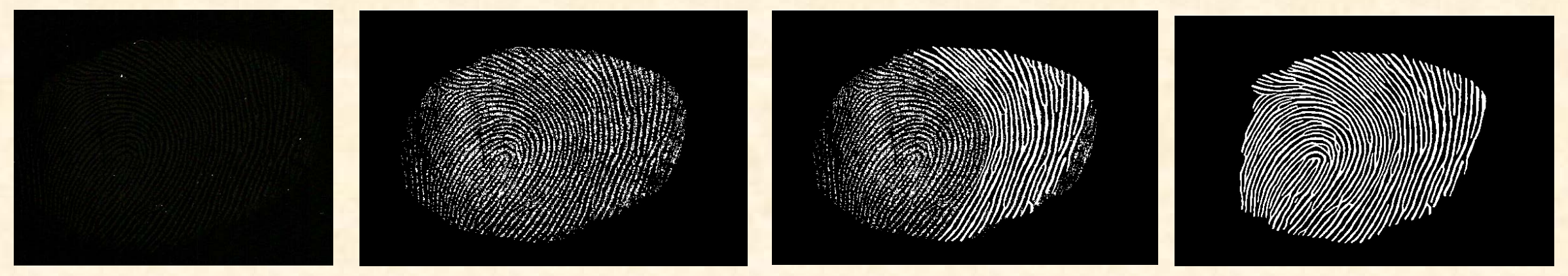

Figure 2: The progression of a latent fingerprint that was captured from the surface of the mobile device only using a scanner without any lifting powders as it is enhanced with a photo editing software package.

MATERIALS AND METHODS

Preliminary Testing Basic Replication Techniques

The primary goal of the preliminary tests was to discover an adequate medium to use for the replication of a fingerprint under ideal circumstances – using a direct mold of the finger. These tests used the following combinations of materials:

- Soft modeling clay / white school glue
- Soft modeling clay / spray on rubber coating
- Forensics molding putty / white school glue
- Forensics molding putty / gelatin*

*Gelatin was mixed with a 1:1 ratio gelatin mix and hot water

These tests were evaluated on the effectiveness of the materials used for creating the mold and effectiveness at replicating the fingerprint.

Replication using Inked Prints

The primary goal for this series of tests was to develop a method to enhance and replicate a print from a non 3 dimensional representation of the print. Various tests were conducted using a print captured with a standard store bought stamp ink pad, and an ink pad that is commonly used for fingerprinting.

IMAGE ENHANCEMENT: During the course of these tests, several different enhancement techniques were tested and refined including:

- **Tracing:** The print was scanned, then enlarged to an 8.5 x 11 size sheet of paper. Then using a transparent sheet, the image was traced using a permanent marker. This image was then scanned and shrunk back to normal size (**Figure 3**).
- **Software:** The print was scanned, then using photo editing software, the print was enhanced to produce a clearer version of the print. Techniques involved using the Threshold Adjustment Tool, Color Range Selection Tool, and Pencil Tool to produce the best image (**Figure 2**).

REPLICATING THE PRINT: Next, a negative mold of the print must be produced so the print can be replicated. This process is outlined as follows:

- The enhanced image is printed on standard paper using a toner based printer.
- This image is then transferred to a copper clad board using a heat source and gentle pressure to transfer the image.
- The image is gently washed with hot water to remove the paper, leaving behind the ink transfer.
  NOTE: Care must be taken not to remove the ink, but to remove any paper residue that may be left behind.
- The copper clad board is then etched using a solution of ferric chloride. This will remove the copper from any exposed areas (**Figure 3**).

After the mold has been created, the print can be reproduced using one of the fingerprint replication materials from the preliminary tests.

Replication using Latent Prints

The primary goal for this series of test was to take the techniques developed in the previous series of tests and to further refine them so they can be implemented using latent fingerprints. During this series of tests the latent prints were captured using the following techniques:

- **No visualization:** The print was captured directly from the surface of the device with a scanner or cell phone camera without the aid of fingerprint powders to visualize the print (**Figure 2**).
- **Fingerprint Powder Substitute:** The print was first visualized with the help of a cheap fingerprint powder substitute purchased at a local store.
- **Fingerprint Powder:** The print was first visualized with the help of either a magnetic or a white fingerprint powder.

RESULTS

Preliminary Test Results

- Successfully able to login to the device with the print replicated with the forensic molding putty and gelatin mixture
- The molding putty produced the most durable and well defined negative mold of the print (**Figure 1**).
- Gelatin was able to mimic the pliability of an actual finger with minimal air pockets that distort the reproduction.

Replication using Inked Prints

- **Capturing the print:** Significant defects were found in the prints created with the stamp ink pad compared to the fingerprint ink pad. This made the process of enhancing the quality of the print much harder (**Figure 1**).
- **Tracing:** The process of tracing the print was time consuming and there was a significant loss in quality of the print, attributed to the fact that the ridges of the print are typically not a uniform width. Tracing with a permanent marker produced a uniform ridge requiring multiple passes. The image still needed to be processed with the photo editing software to ensure that all of the ridges had a consistent black color (**Figure 3**).
- **Software:** This method produced the best results for enhancing the print. However, it was very time consuming to implement. The varying widths of the ridges could easily be recreated and any mistakes could easily be undone (**Figure 2**).
- **Replicating the Print:** This technique requires a bit of time to master. The biggest problem was transferring the printed image to the copper plate. Applying firm pressure with an iron set to the highest temperature setting for about 8 minutes, in combination with printing the image on matte photo paper, produced the best results. Successful login was obtained using this method with the software reproduced image, but not the hand traced image.

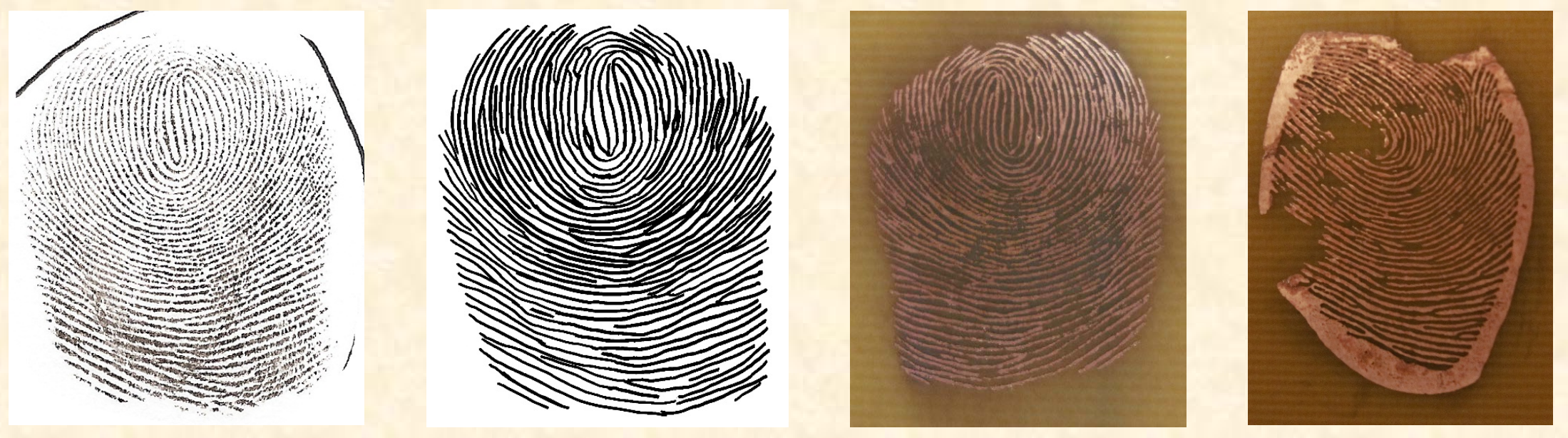

Figure 3: (L-R) (1) Raw print captured with stamp ink pad, then traced by hand to produce image (2). (3) Negative mold of print in image (2) produced via the printed circuit board method. (4) Negative mold of print that was enhanced in **Figure 3** via the printed circuit board method.

Replication using Latent Prints

- Replicating these prints proved to be more difficult than the inked prints because the starting image was not as well defined.
- The tracing method was not attempted with this set.
- The software reproduction of the prints was improved greatly. Successful login was obtained using a print that was captured from the surface of the device without the help of any powders.

DISCUSSION

During the process of enhancing the print care must be taken to ensure that the correct aspects of the image are represented in the image to be transferred to the copper plate. For example, when the print seen in **Figure 2** was enhanced the actual print was represented in white. All of the black portions correspond to the valleys of the print. When etched, these portions will remain, creating a negative image. If the print is lifted i.e. the actual ridges are represented in black, the colors must be inverted.

There are several limiting factors that must be taken into consideration when implementing this technique to gain access to a mobile device:

- In the default configuration, the device will revert to pin access only after 48 hours of inactivity.
- Likewise, after 5 failed attempts to login via the biometric scanner, the phone will default to pin access only.
- If the device is restarted, it will default to pin access only.

CONCLUSIONS

Based on our results, this is a plausible means of gaining access to a mobile device that uses biometric identification systems given that certain time constraints are met.

Future work on this project should include further refinement of the techniques to reduce the time to implement them and to improve their reliability. This can include developing an automated image processing tool that would allow the user to quickly enhance the latent print. Furthermore, the image transfer process can be improved by using photo sensitive copper clad plates.

REFERENCES

[1] Lo, J., Wyble, C., & Hupfer, S. (2012). Fast track to the future. The 2012 IBM Tech Trends Report. Retrieved February 2, 2015, from http://public.dhe.ibm.com/common/ssi/ecm/xi/en/xie12346usen/XIE12346USEN.PDF

[2] Tassone, C., Martini, B., Choo, K., & Slay, J. (2013). Mobile device forensics: A snapshot. *Trends & Issues in Crime and Criminal Justice, 460* (ISSN 1836-2206), 441-460. Retrieved February 2, 2015, from http://www.aic.gov.au/publications/current series/tandi/441-460/tandi460.html

ACKNOWLEDGEMENTS

2014 Summer Faculty and Student Team Awards for Enhancing Undergraduate Research Experiences and Creative Activities (EURECA) from the Sam Houston State University Center was greatly appreciated. A special thanks to Andy Bennett, Director for the Center of Excellence in Digital Forensics for his technical support.