Parameterizing Fingerprints to Protect Against "Sniff and Suppress" Attacks

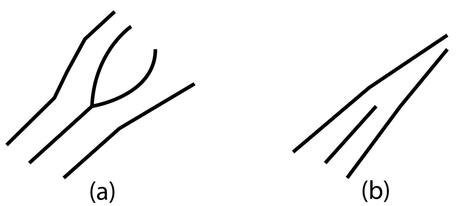
Marcus Aqui and Terence Pocklington
Ernst Leiss, University of Houston

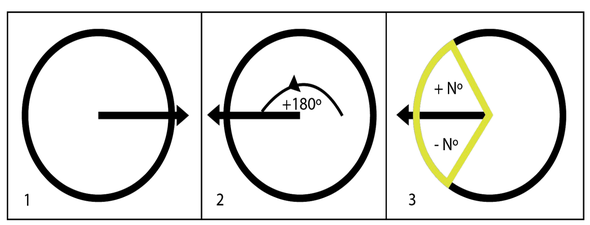
Background

The attack vector we are focusing on is called "Sniff and Suppress." This occurs when an attacker intercepts data and suppresses it. This signals an error to the user, who suspects nothing. Meanwhile, he attacker now has a legitimate copy of the biometric data. This is especially harmful because biometric data cannot be replaced if it is compromised. We will create a method to protect fingerprints from these attacks.

Objective

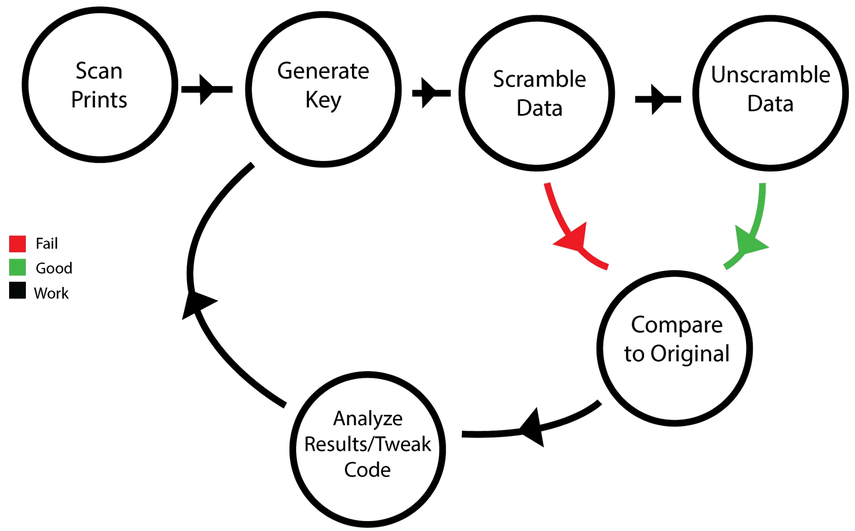
1. Determine fingerprint attributes (bifurcation and ridge endings)
2. Create a tool to scramble the data
3. Test data set by scrambling and unscrambling print data, then comparing it to the original prints





1. Fingerprint angle is found
2. To switch the type of minutia, rotate the angle 180 degrees
3. Based on the key's attributes, add some variance to the angle

Methods



Results

When compared to the original fingerprint data, the scrambled prints were different enough to fall below our threshold for similarity. This represents a successful encryption that reduces the risk of discovery of the original fingerprint data values.

Original v Original

1_1_1_1 - Notepad

File Edit Format View Help

```
418 C:/Users/starr/Desktop/Fingerprints/Original/1_1_1_1.xyt
94 C:/Users/starr/Desktop/Fingerprints/Original/1_1_1_2.xyt
163 C:/Users/starr/Desktop/Fingerprints/Original/1_2_1_1.xyt
93 C:/Users/starr/Desktop/Fingerprints/Original/1_2_1_2.xyt
75 C:/Users/starr/Desktop/Fingerprints/Original/1_3_1_1.xyt
74 C:/Users/starr/Desktop/Fingerprints/Original/1_3_1_2.xyt
108 C:/Users/starr/Desktop/Fingerprints/Original/1_4_1_1.xyt
101 C:/Users/starr/Desktop/Fingerprints/Original/1_4_1_2.xyt
```

Scrambled v Original

28_3_1_2 - Notepad

File Edit Format View Help

```
4 c:/users/starr/desktop/fingerprints/original/28_2_7_2.xyt
4 c:/users/starr/desktop/fingerprints/original/28_2_8_1.xyt
5 c:/users/starr/desktop/fingerprints/original/28_2_8_2.xyt
5 c:/users/starr/desktop/fingerprints/original/28_2_9_1.xyt
4 c:/users/starr/desktop/fingerprints/original/28_2_9_2.xyt
4 c:/users/starr/desktop/fingerprints/original/28_3_10_1.xyt
3 c:/users/starr/desktop/fingerprints/original/28_3_10_2.xyt
3 c:/users/starr/desktop/fingerprints/original/28_3_1_1.xyt
6 c:/users/starr/desktop/fingerprints/original/28_3_1_2.xyt
3 c:/users/starr/desktop/fingerprints/original/28_3_2_1.xyt
```

Discussion

Based on our tests with 17 keys, the scrambled prints do not match their original counterparts, while the unscrambled versions of the fingerprints are identical to the original fingerprints.

The implications of this approach to fingerprint security are that under this method, fingerprint biometrics are more impervious to attacks from malicious actors. If a fingerprint is compromised from an attack, you can recover from the attack by simply scrambling the fingerprint with a different key.

Next Steps

Our next steps include testing more keys and fingerprints and publishing a paper over our findings.

Acknowledgments

This research was made possible by a NSF grant to the University of Houston Computer Science Department (NSF CNS-1551221).

A. Sankaran, M. Vatsa and R. Singh, Multisensor Optical and Latent Fingerprint Database, IEEE Access, vol.3, no., pp. 653 -665, 2015.
A. Sankaran, M. Vatsa and R. Singh, Latent Fingerprint Matching: A Survey, IEEE Access, vol.2, pp.982-1004, 2014.
Ernst L. Leiss: Safeguarding the Transmission of Biometric Measurements Used for Authenticating Individuals, Proc. IFIP World Computing Congress, NetCon, Santiago, Chile, August 20-25, 2006.
Ernst L. Leiss: Requirements for the Safe Transmission of Biometric Measurements for Authenticating Individuals, CLEI 2008 – Conferencia Latinoamérica de Informática, Sept. 1-5, 2008, Santa Fe, Argentina.