Electronic Letters on Computer Vision and Image Analysis 15(2):37-39, 2016

REMOTE AUTHENTICATION USING VAULTED FINGERPRINT VERIFICATION

Hamdan Ahmed Alzahrani

University of Colorado Colorado Springs, Department of Computer Science , VAST LAB, 1420 Austin Bluffs Pkwy, Colorado Springs, CO USA 80918

Advisors/s: Terrance E. Boult

Date and location of PhD thesis defense: 13 April 2016, University of Colorado Colorado Springs.

Received 31st August 2016; accepted 28th September 2016

Abstract

Traditional authentication systems rely on the possession of a token, generally a password or smartcard. Token-based identity transactions are relatively easy to repudiate since unauthorized persons may possess the token. A system that can guarantee a user's presence during authentication would greatly enhance the non-reputability of these transactions. Biometrics can provide this strong link between users and their identities. By measuring and comparing a feature of the user, we can increase the assurance that the user is present during authentication.

Fingerprint biometrics are increasingly used for identity verification. However, these require a careful balance of accuracy and privacy that is missing in many implementations. This dissertation describes a new biometric matching system, the protection of an existing data-type, and a model for matching security with error correction codes.

This dissertation constructs a fingerprint biometric remote authentication system capable of transmitting a session key. Other results include a modification to PMCC which significantly enhances privacy and a model for security with error correction.

VFV is built on blocks containing several minutia triangles. Selecting several minutia triangles within a block provides tolerance to common errors in fingerprint images. The blocks are permuted to store arbitrary data, such as encryption keys or an authenticator challenge. The data is combined with an error correcting code to provide tolerance to inter-image errors in fingerprint minutia. Figure 1 shows the creation of the vault. Figure 2 shows the creation of the challenge key by swapping blocks.

Correspondence to: halzahra@uccs.edu

Recommended for acceptance by David Vázquez Bérmudez

DOI http://dx.doi.org/10.5565/rev/elcvia.985
ELCVIA ISSN: 1577-5097
Published by Computer Vision Center / Universitat Autonoma de Barcelona, Barcelona, Spain

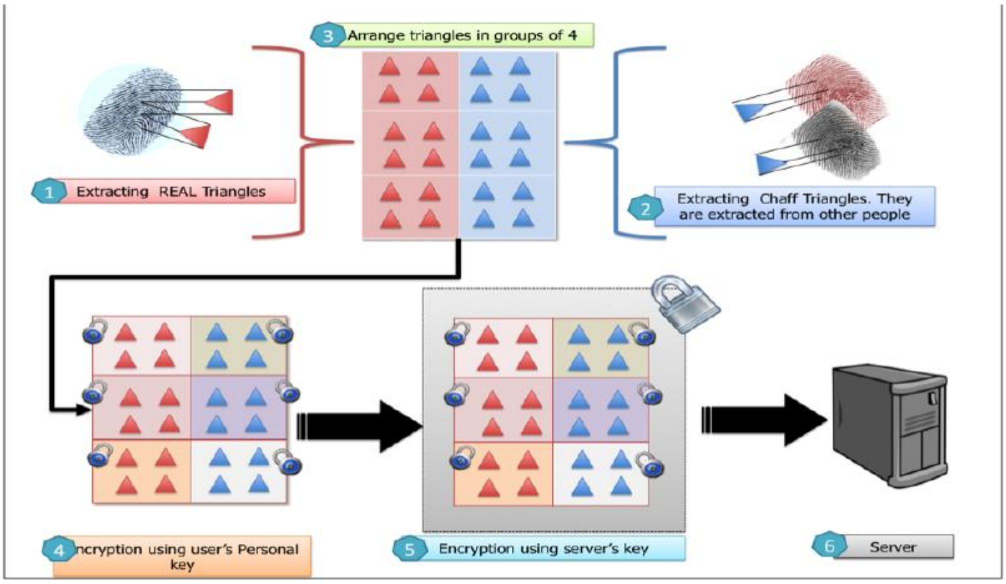
3 Arrange triangles in groups of 4
1 Extracting REAL Triangles
2 Extracting Chaff Triangles. They are extracted from other people
4 ncryption using user's Personal key
5 Encryption using server's key
6 Server

Figure 1: Vault Creation

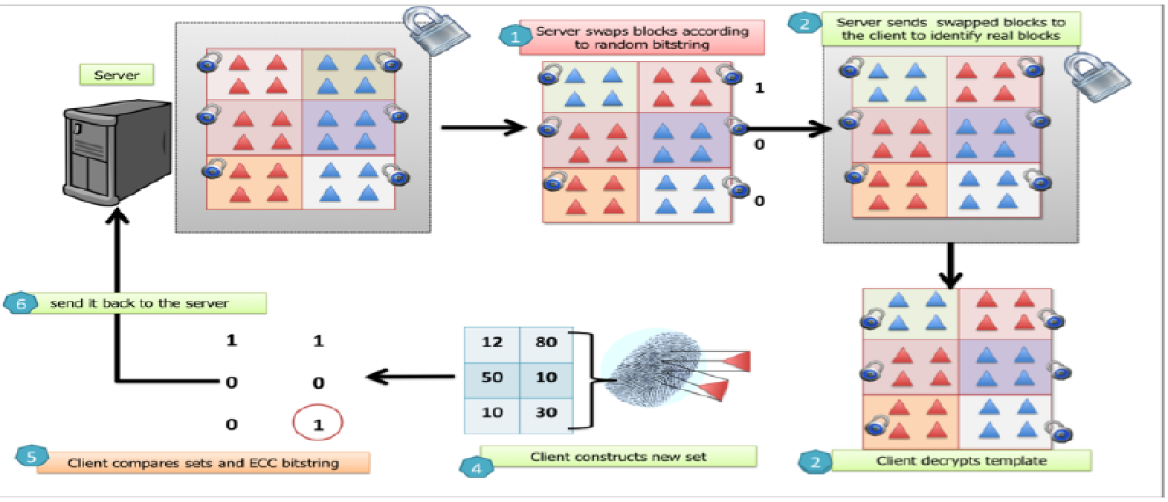
Server
1 Server swaps blocks according to random bitstring
2 Server sends swapped blocks to the client to identify real blocks
1
0
0
2 Client decrypts template
12 80
50 10
10 30
4 Client constructs new set
1 1
0 0
0 1
5 Client compares sets and ECC bitstring
6 send it back to the server

Figure 2: Challenge Creation and Verification Process

VFV allows for key exchange and remote authentication using the challenge response protocol. Protected biometric template is used to preform the authentication. Privacy and security of the user's biometric data is preserved through multiple levels of protection. First, the system uses a protected transmission protocol to transmit the authentication token. Second, minutia triangles are difficult to invert. Third, VFV is compatible with protected minutia data types.

A session key or other data can be shared within the VFV template. The key is stored in the permutation of the minutia triangles. The data is decoded by matching to the user's fingerprint. VFV can store an arbitrary amount of data. The thesis demonstrates 100 and 256 bit payloads. Combined with the Vaulted Verification authentication protocol, this allows the transmission of a session key in a biometrically secured template. The key is protected from errors in biometric matching by error correcting codes.

The primary result from VFV is a fingerprint minutia triangle matcher that is order independent. VFV's matcher does not require minutia or minutia triangles to be ordered prior to matching. This simplifies the matcher process, allows more data-types, and allows the order of the triangle set to be used for data transmission.

VFV is compatible with privacy enhanced fingerprint data-types. Any data-type that can be associated with a minutia triangle or subsets of a minutia triangle can be used. This flexibility is demonstrated by including Protected Minutia Cylinder Code (PMCC) a privacy enhanced minutia descriptor, into VFV [1], [2], [3], [4]. PMCC is known for its ability to enhance the accuracy of matching fingerprint minutia while being difficult to invert. Augmented VFV features with PMCC enhance the accuracy of the system.

The fingerprint minutia triangles used in VFV allow for improvements of privacy enhanced data-types. This thesis improves the privacy of PMCC by combining the individual PMCC minutia values into a single triangle value. This enhancement of PMCC maintain matcher accuracy, reduces template size, and significantly improves the privacy of the user's data by enhancing the non-invertiblity of PMCC.

A model for the security of a key with error correction is constructed. The use of error correcting codes reduces the effective security provided by the key. A model is constructed to estimate the effective security of keys with error correction. The model shows that there are some non-trivial combinations of error detection and correction that minimize effective security. Further research is needed to fully determine the impact of error correction codes on key security.

References

[1] R. Cappelli, M. Ferrara and D. Maltoni, "Minutia Cylinder-Code: a new representation and matching technique for fingerprint recognition", IEEE Transactions on Pattern Analysis Machine Intelligence, vol.32, no.12, pp.2128-2141, December 2010. doi:10.1109/tpami.2010.52.

[2] R. Cappelli, M. Ferrara, and D. Maltoni, "Fingerprint Indexing based on Minutia Cylinder Code," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 5, pp. 1051 - 1057, May 2011. doi:10.1109/tpami.2010.228.

[3] M. Ferrara, D. Maltoni and R. Cappelli, "Noninvertible Minutia Cylinder-Code Representation", IEEE Transactions on Information Forensics and Security, vol.7, no.6, pp.1727-1737, December 2012. doi:10.1109/tifs.2012.2215326.

[4] M. Ferrara, D. Maltoni and R. Cappelli, "A Two-Factor Protection Scheme for MCC Fingerprint Templates", in proceedings International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, September 2014.