Bull. Aust. Math. Soc. **80** (2009), 347–349
doi:10.1017/S0004972709000665

SECURE AND PRIVATE FINGERPRINT-BASED AUTHENTICATION

ARATHI ARAKALA

(Received 14 May 2009)

2000 *Mathematics subject classification*: primary 94A62.
Keywords and phrases: authentication, secret sharing.

One of the vital applications for biometrics is its ability to replace passwords or PINs in a secure authentication system. Two biometric samples from the same person will rarely be identical, even if taken within minutes of each other, due to the nature of the biometric and the sampling technique. Consequently, standard matching techniques that match the enrolled template with the query template presented for verification require storage of the enrolment template. As a biometric is irreplaceable, raw template storage is severely detrimental to biometric security.

The principal aim of this thesis was to implement a fingerprint minutiae-based authentication system where the minutiae template is secure during storage and during comparison. In order to achieve this, we employed 'biocryptographic constructs' that is cryptographic constructs that provide security of the template in spite of the error prone nature of biometric data. It provides an implementation of a secure authentication system using PinSketch [1] where the templates are built from fingerprint minutiae and where the encryption process has a negligible effect on the system accuracy and clear bounds are provided for template security. This thesis focuses on the fingerprint biometric as it is one of the most popularly used modalities in commercial systems and security issues with this modality could have a negative impact on the uptake of biometrics as a whole. We also focussed on minutiae-based templates as they are easily extracted by standard fingerprint feature extractors and their comparison mimics the traditional method of fingerprint comparison by eye.

In order to build any secure authentication system we identified four main steps to be conducted: identification of a suitable match threshold based on a difference or commonality based measure that takes template size into account, quantization of the data that comprise the templates, evaluation of the matching performance before and

Thesis submitted to RMIT University, June 2008. Degree approved, November 2008. Supervisors: Professor K. J. Horadam and Dr Jason Jeffers.

after use of the chosen biocryptographic construct and analysis of the robustness of the secure authentication system to a masquerade attack.

To implement a secure minutiae-based authentication system, we chose eight different techniques to extract repeatable patterns from the spatial distribution of a set of extracted minutiae, giving rise to eight distinct minutiae-based templates, each represented as a set of elements from a finite universe. We tested the accuracy of a matching algorithm when each of these template types was used. As the templates were treated as sets, the variation between templates was measured using a set difference metric. Two biocryptographic constructs based on the set difference metric—the fuzzy vault [2] and PinSketch were evaluated for their suitability to build secure minutiae-based authentication systems.

The fuzzy vault was found to be unsuitable to protect three specific template types that were tested, for a fundamental reason that would apply to the other five template types considered in this thesis. We then explored the suitability of the PinSketch construct to protect all of the eight template types. Three algorithms using the PinSketch construct were proposed in this thesis. All three had caused some reduction in system's matching accuracy when compared with that before using the construct. When subject to a security analysis, however, two of the algorithms failed to provide security of the template due to large natural intra-sample variation between templates from the same finger. The third algorithm used a two-stage process and a combination of a set difference-based measure and a commonality-based measure to compare two templates. This allowed some randomness to be retained in the template types protected by this PinSketch-based authentication algorithm. This algorithm successfully kept the template secure during storage as well as comparison at a threshold where the false match rate was 0%, making it well suited to high security applications.

Our research demonstrated that when biometric templates possess a large intra-sample variation between them, it becomes infeasible to protect them using a set difference-based construct. One solution involving a two-stage process was demonstrated in the third algorithm. A second solution is to use an efficient commonality-based biocryptographic construct. In the thesis we list the desirable characteristics of such constructs but are not aware of the existence of any such construct to date.

The main conclusions of this thesis are as follows.

(1) Quantization error degrades the matching performance of minutiae-based templates by 10–20% across all structure types.
(2) A matching threshold that takes set sizes into account gives significantly better matching performance than an absolute threshold used across all fingerprint comparisons.
(3) A generalized Reed–Solomon decoding-based fuzzy vault can be realized when samples of the same fingerprint have at least 33% of the minutiae structures in common between them.

https://doi.org/10.1017/S0004972709000665 Published online by Cambridge University Press

(4) To realize a secure PinSketch-based authentication system the size of the sets being compared must be greater than the maximum set difference errors that need to be corrected for a secure system to be realized.
(5) Uniform quantization of minutiae features in templates gives rise to template-quantized features having a nonuniform distribution. This can reduce the complexity of an attacker's efforts to significantly less than brute force.
(6) A structure representation using triangle patterns formed from a minutiae point pattern showed potential to be used for secure pre-alignment of templates prior to use in a cryptographic construct.

References

[1] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, 'Fuzzy extractors: how to generate strong keys from biometrics and other noisy data', *SIAM J. Comput.* **38** (2008), 97–139.
[2] A. Juels and M. Sudan, 'A fuzzy vault scheme', *Des. Codes Cryptogr.* **38** (2006), 237–257.

ARATHI ARAKALA, School of Mathematical and Geospatial Sciences,
GPO Box 2476V, Melbourne 3001, Australia
e-mail: arathi.arakala@rmit.edu.au

https://doi.org/10.1017/S0004972709000665 Published online by Cambridge University Press