A Dependability Analysis of Smart Cards for Biometric Authentication

Baba, Kensuke
Research and Development Division, Library, Kyushu University

Egawa, Serina
Graduate School of Information Science and Electrical Engineering, Kyushu University

出版情報：Proc. International Conference e-Society, pp.463-466, 2013-03. IADIS
バージョン：
権利関係：

A Dependability Analysis of Smart Cards for Biometric Authentication*

Kensuke Baba† Serina Egawa

Abstract

This paper conducts an analysis of dependability of smart cards for biometric authentication. Dependability is an important factor for evaluating social infrastructure systems, and suitable formalizations of dependability are required from various aspects. This paper formalizes a kind of dependability of smart cards for biometric authentication on the basis of leakage of confidential information. As an example of evaluation based on the formalization of dependability, this paper examines the effects of preventing leakage of biometric information from smart cards on accuracy of authentication with practical palmprint images. This evaluation gives a trade-off between dependability of smart cards and efficiency of the application system of smart cards.

Keywords: dependability, smart card, authentication, personal information, palmprint.

1 Introduction

Smart card has been an essential technology in many social infrastructure systems such as ATMs and ticket gates for transportation facilities. In addition to efficiency such as the processing time of smart cards, dependability is an important factor for evaluating such social infrastructure systems. In order to estimate dependability of systems, a suitable formalization and a quantitative evaluation are necessary.

A simple idea of dependability of smart cards can be defined by considering leakage of confidential information stored in a smart card. At the system LSI level, the difficulty to access a particular memory can be controlled by setting physical obstacles, applying scrambling or cryptography [5], and so on. However, applying such a measure to prevent information leakage might lead some inconveniences. For example, some researchers point out a conflict between this kind of dependability and the testability of circuits [8]. We focus on the effects of preventing information leakage on the efficiency of smart cards at the application level rather than the system LSI level.

Personal authentication is one of the simple and essential applications of smart cards, and especially a combination with biometric authentication is expected to compensate some weaknesses of token- and knowledge-based authentication [4]. We consider personal authentication with biometric images as the application of smart cards and the accuracy of authentication as the criteria of efficiency. The goal of this paper is showing the relation between the difficulty of information leakage and the authentication accuracy as an example of a trade-off between dependability and efficiency of a system.

In this paper, first, we formalize personal authentication by smart cards with biometric images and accuracy of authentication. Next, we define an idea of dependability of smart cards by considering the possibility of personal identification by leaked biometric information from the smart card. Additionally, we conduct experiments of authentication and identification with practical palmprint images. The relation between the two values can be regarded as a trade-off between dependability and efficiency of the system.

2 Preliminaries

Assume that any biometric image corresponds to a person. Personal authentication with biometric images (called *authentication*) is verifying that the target person is a particular person. The input of authentication is a pair of an image and the name of a person, and the output is "accept" or "reject".

The players in authentication with a smart card system are a smart card, an authentication system, and the person who want to use the system. The smart card has a biometric image for authentication (called a *template*). The authentication system can capture a biometric image for authentication from the person. Then, the straightforward protocol of authentication is defined as follows.

1. The authentication system reads the template from the smart card and captures a biometric image from the person,

*An edited version of this report was published in: *Proc. International Conference e-Society*, pp. 463–466, IADIS, Mar, 2013.

†Library, Kyushu University, *baba.kensuke.060@m.kyushu-u.ac.jp*

2. The authentication system compares the template and the captured image and judges "accept" or "reject".

As an idea of accuracy of authentication, we consider the standard error rates of verification. The *accuracy* of authentication is the difference of the equal error rate (EER) from unity.

3 Formalization of Dependability

The idea of dependability of a smart card is defined by the possibility of identification of the person by biometric information leaked from the smart card. Assume that the attacker tries to steal the template from a smart card and identify the person, and the identification is conducted with a list of pairs of a biometric image and the name of the corresponding person. That is, the input of the identification is an image and the output is the name of the person judged to correspond to the image. Then, the possibility of identification is the rate that the person of the output equals to the person of the input image. The output can be "null" if the image is judged to correspond to no person in the list. The *dependability* is the rate that the identification with a stolen image by the attacker fails.

4 Evaluation

The accuracy in Section 2 and the dependability in Section 3 are examined with practical palmprint images.

4.1 Algorithms for Authentication and Identification

We consider a matching of features extracted by Scale-Invariant Feature Transform (SIFT) [6, 7] for the comparison of palmprint images. SIFT translates an image into a set of key points and each key point has a vector as its feature. The similarity of two palmprint images is defined on the basis of a straightforward matching of the key points as [3]. The samples of palmprint images were taken from PolyU Palmprint Database [1].

In order to define the amount of information that affects the accuracy and the dependability, we consider multiple biometric images conceptually instead of a single image, that is, we examine the accuracy for different numbers of templates in authentication and the dependability for different numbers of input images in identification.

First, we examine the accuracy of authentication with the palmprint images. For k templates, we consider two algorithms of authentication. The *at-least-1 algorithm* is

1. Compare the input image with the k templates;
2. Output "accept" if at least one similarity in the k similarities is larger than a threshold, and "reject" otherwise.

The mean algorithm is obtained by replacing the word "at least one similarity in the k similarities" in the process 2 with "the arithmetic mean of the k similarities".

Next, in order to examine the dependability, we consider two algorithms of identification for k input images. The *nearest algorithm* is

1. Compare the k input images with each image in the list, and find the image whose similarity is the largest in the list;
2. If the largest similarity is larger than a threshold, then output the person of the image, and "null" otherwise.

The *mean-nearest algorithm* is

1. Compare the k input images with each image in the list and compute the arithmetic mean of the k similarities;
2. If the largest value of the arithmetic means is larger than a threshold, then output the person of the image, and "null" otherwise.

4.2 Trade-off between Accuracy and Dependability

The sample set contains 1,200 images that consist of 150 persons with 8 images for each. We separated the sample set into two sets of 150×4 images. An experiment was conducted with one set for templates and the other set for input images, and repeated with swapping the two sets. Additionally, the number of templates for authentication and the number of input images for identification were respectively changed to be 1, 2, 3, and 4. Hence, for an experiment with k images, ${}_4C_k$ kinds of combination were considered. Therefore, any value in the experiments is the arithmetic mean of the results for ${}_4C_k \times 600 \times 2$ trials.

Figure 1 shows the accuracy with the two authentication algorithms and the dependability with the two identification algorithms. When $k = 1$, the accuracy of the two authentication algorithms was 93.68% and the dependability of the two identification algorithms was 24.27%. When $k = 4$, the accuracy of the mean algorithm was 97.28% and the dependability of the mean-nearest algorithm was 5.00%. Those results mean that by using a biometric image that equals to four palmprint images in the sense of an amount of information as a template, authentication with the accuracy

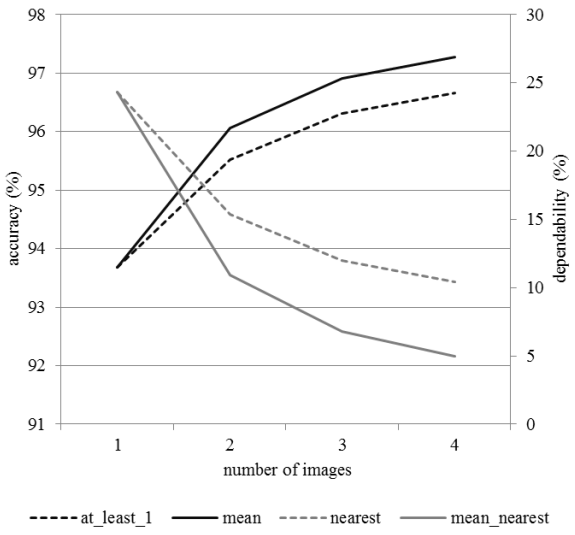

Figure 1: The accuracy of the at-least-1 and the mean algorithm where the number of templates is 1, 2, 3, and 4, and the dependability of the nearest and the mean-nearest algorithm where the number of input images is 1, 2, 3, and 4.

97.28% can be achieved, and an attacker can identify the person with the error rate 5.00% (on the assumption that the attacker has information that equals to the list of biometric images and the corresponding persons in the authentication system).

5 Conclusion

We formalized a kind of dependability of smart cards for biometric authentication on the basis of the leakage of confidential information. Additionally, we examined the effects of preventing the leakage of biometric information from smart cards on accuracy of authentication with practical palmprint images. By the results, we obtained a trade-off between dependability of smart cards and efficiency of the application system of smart cards. The results can be a factor to decide the kind and the strictness of the measure to prevent information leakage for smart cards. More detailed relation between the number of palmprint images and the accuracy of personal authentication can be obtained from [2].

Acknowledgement

This work was partially supported by CREST program of Japan Science and Technology Agency (JST) from 2008 to 2012 and the Grant-in-Aid for Young Scientists (B) No. 22700149 of the Ministry of Education, Culture, Sports, Science and Technology (MEXT) from 2010 to 2012.

References

[1] PolyU Palmprint Database. http://www.comp.polyu.edu.hk/˜biometrics/.

[2] K. Baba and S. Egawa. A note on authentication accuracy with multiple biometric images. In *4th International Conference on Intelligent Systems, Modelling and Simulation*, pages 52–55. IEEE, 2013.

[3] S. Egawa, A. I. Awad, and K. Baba. Evaluation of acceleration algorithm for biometric identification. In *Networked Digital Technologies, Part II*, volume 294 of *Communications in Computer and Information Science*, pages 231–242. Springer, 2012.

[4] A. K. Jain, A. A. Ross, and K. Nandakumar. *Introduction to Biometrics*. Springer, 2011.

[5] D. Lie, C. Thekkath, M. Mitchell, P. Lincoln, D. Boneh, J. Mitchell, and M. Horowitz. Architectural support for copy and tamper resistant software. *ACM SIGPLAN Notices*, 35(11):168–177, 2000.

[6] D. G. Lowe. Object recognition from local scale-invariant features. In *Proc. IEEE International Conference on Computer Vision*, pages 1150–1157, 1999.

[7] D. G. Lowe. Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, 60(2):91–110, 2004.

[8] K. Rosenfeld and R. Karri. Security and testing. In *Introduction to Hardware Security and Trust*, pages 385–410. Springer, 2012.