九州大学学術情報リポジトリ
Kyushu University Institutional Repository

A Note on Authentication Accuracy with Multiple Biometric Images

Baba, Kensuke
Research and Development Division, Kyushu University Library

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

https://hdl.handle.net/2324/25893

出版情報：Proc. Fourth International Conference on Intelligent Systems, Modelling and Simulation (ISMS2013), pp.52-55, 2013-01. IEEE
バージョン：
権利関係：

KYUSHU UNIVERSITY

A Note on Authentication Accuracy with Multiple Biometric Images*

Kensuke Baba† Serina Egawa

Abstract

This paper conducts an analysis on accuracy of biometric authentication. By increasing the number of biometric images for authentication, authentication accuracy is expected to be improved. However, the relation between the number of images and accuracy is not trivial. This paper considers simple algorithms for verification and identification with multiple biometric images for each person. The algorithms are based on the ideas of a majority vote and the mean of similarities for treating results of comparisons with multiple images. The effects of the number of images on the error rates of the algorithms are examined with practical palmprint images. The result implies that considering the mean of the similarities with multiple images is useful to improve authentication accuracy.

Keywords: authentication, accuracy, biometrics, pattern matching.

1 Introduction

Personal authentication has been an essential issue in many social infrastructure systems. Biometric authentication has attracted attention as a technology to compensate some weaknesses of token- and knowledge-based authentication [8]. With the spread of computers and networks, the scope of applications of personal authentication was extended into a wide area, and the number of persons who use each application system is supposed to become huge. Especially for biometric authentication, accuracy of personal authentication becomes an important factor by the increase of the number of persons.

The aim of our research is to find a way to improve accuracy of biometric authentication. One of the straightforward approaches for the improvement is increasing the amount of information for authentication such as the number of biometric images registered in an authentication system (such registered images are called gtemplatesh). This trial to improve authentication accuracy by several biometric images can be a typical application of statistical analyses [4]. However, in order to apply such analyses appropriately into biometric images, some knowledge of biology about the part of human beings or of image processing about the feature extraction will be required after all.

We simply focus on the results of comparisons of biometric images. Our approach is on the assumption that the basic authentication with a single template for each person is conducted on the basis of the result of a comparison between the template and an inputted image, and then the effects of the number of templates on accuracy are evaluated as the change from the basic authentication. Then, we consider two simple ideas in order to treat the results of comparisons for multiple templates, that is, a majority vote and the arithmetic mean of the similarities. There exist two possible procedures of biometric authentication, that is, verification and identification [8]. At least for identification, the effects of the number of templates for each person on accuracy are not trivial even for the simple methods to treat multiple results of comparisons.

In this paper, we define simple algorithms for verification and identification based on the idea of a majority vote and the mean of similarities. And then, we apply the algorithms to practical palmprint images in order to examine the error rates as accuracy of authentication. In order to measure the similarity of two images, we consider the matching of the features extracted by Scale-Invariant Feature Transform (SIFT) [9, 10]. There already exist some researches that apply SIFT to authentication with biometric images such as fingerprints [7, 12, 3] and palmprints [5, 11, 6]. The ideas to treat multiple comparisons in this paper are applicable straightforwardly to the previous researches. Additionally, it is expected to be applicable to general comparison-based authentication algorithms with multiple biometric images.

The rest of this paper is organized as follows. Section 2 formalizes the target problems, verification and identification, and the criteria for accuracy of algorithms. Section 3 introduces algorithms for verification and identification and the method of image matching in this paper. Section 4 reports the experimental results with practical palmprint images.

*An edited version of this report was published in: *Proc. Fourth International Conference on Intelligent Systems, Modelling and Simulation, pp. 52–55, IEEE, Jan, 2013.*

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

2 Preliminaries

We define two problems concerned with personal authentication with biometric images. Assume that each biometric image corresponds to a person and a set of biometric images (called *templates*) is given. Verification is to verify that the target person is a particular person. The input of verification is a pair of an image (called an *input image*) and the name of a person (called an *input person*), and the output is "accept" (that is, the input image corresponds to the input person) or "reject" (that is, the input image does not correspond to the input person). *Identification* is to search who the target person is. The input of identification is an input image and the output is the name of the person judged to correspond to the input image. The output of identification can be "null" (that is, the input image corresponds to no one in the persons of the templates) if a threshold is given with the input.

We consider the standard error rates in verification [8]. The *false rejection rate* (*FRR*) is the rate that the output is "reject" and the input image corresponds to the input person, and the *false acceptance rate* (*FAR*) the rate that the output is "accept" and the input image does not correspond to the input person. FRR and FAR depend on the threshold for the image similarity, and then the *equal error rate* (*EER*) is the value of FRR and FAR at the threshold where the two error rates have the same value. For identification, the *error rate* (*ER*) is the rate that the person who corresponds to the output image is different from the person who corresponds to the input image.

3 Algorithms

This section defines algorithms for verification and identification and the similarity on images for image matching in this paper.

3.1 Verification

We consider verification algorithms on the situation that multiple templates correspond to a single person. Let k be the number of templates that correspond to each person. Any algorithm for verification first conducts the following process.

1. Compare the input image with the k templates of the input person.

Then, the *n/k-algorithm* for verification is,

2. If at least n similarities in the k similarities are larger than the threshold, then output "accept" and terminate;
3. Otherwise, output "reject" and terminate.

Intuitively, this method is based on the idea of a majority vote about the similarities of multiple templates.

We also consider another algorithm based on the idea of the mean of similarities. The *mean algorithm* is, after the process 1,

2. If the arithmetic mean of the k similarities is larger than the threshold, then output "accept" and terminate;
3. Otherwise, output "reject" and terminate.

Note that the n/k-algorithm for $(k, n) = (1, 1)$ is same as the mean algorithm for $k = 1$.

3.2 Identification

As the base algorithm for identification, we consider the *nearest algorithm*, that is,

1. Compare the input image with all templates;
2. If the largest similarity is larger than the threshold, then output the person of the template and terminate;
3. Otherwise, output "null" and terminate.

The *mean nearest algorithm* is obtained by replacing the process 2 in the nearest algorithm with the following process.

2. If the largest value of the arithmetic mean of the similarities with k templates for a person is larger than the threshold, then output the person of the k templates and terminate;

Clearly, the mean nearest algorithm for $k = 1$ is the nearest algorithm for $k = 1$.

We also consider the *linear search algorithm*, that is,

1. Compare the input image with each template successively in an order;
2. If a template whose similarity with the input image is larger than the threshold is found, then output the person of the template and terminate;
3. If the similarities with every template are not larger than the threshold, output "null" and terminate.

In the similar way of the n/k-algorithm, we define the *n/k-linear search algorithm*

1. Compare the input image with each set of k templates for a person successively in an order;
2. If at least n similarities in the k similarities are larger than the threshold, then output the person of the k templates and terminate;

3. If no set of k templates has n similarities larger than the threshold, output "null" and terminate.

We also consider the idea of the mean of similarities for identification. The *mean linear search algorithm* is, after the process 1 in the previous algorithm,

2. If a set of k templates such that the arithmetic mean of the similarities with the input image is larger than the threshold is found, then output the person of the k templates and terminate;

3. If the arithmetic mean of the similarities with every set of k templates is not larger than the threshold, output "null" and terminate.

Note that when $k = 1$ the n/k- and the mean linear search algorithms are same as the linear search algorithm.

3.3 Image Matching

The experiments in this paper are conducted with practical palmprint images. We consider a matching of SIFT features for the comparison of palmprint images. SIFT is one of the popular methods for image matching and object recognition, and the detailed mechanism can be found in [9, 10].

Prior to applying SIFT feature extraction to palmprint images, the region of interest (ROI) on each palmprint should be extracted. In the SIFT-based verification by Chen and Moon [5], the ROI on a palmprint is extracted as a square based on the method in [13]. In this paper, we extract the ROI as the circle that covers the maximal part on a palm.

SIFT translates an image into a set of key points and each key point has a vector as its feature. Then, a comparison of two images is done by matching two sets of key points. There exist several possible procedures for the matching of key points. In this paper, the similarity on images (that is, sets of key points) is defined as follows. Let P and Q be two sets of key points and $v(p)$ the feature vector of a key point p.

- For any $p \in P$, $q_p \in Q$ satisfies that $\|v(q_p) - v(p)\|$ is the smallest in Q.
- For any $q \in Q$, $p_q \in P$ satisfies that $\|v(p_q) - v(q)\|$ is the smallest in P.
- m is the number of the pairs of $p \in P$ and $q \in Q$ such that $q_p = q$ and $p_q = p$.

Then, the similarity of two images whose features are respectively P and Q is defined to be

$$\frac{m}{\max\{|P|, |Q|\}}.$$

Table 1: The EERs of the n/k-algorithm and the mean algorithm for $1 \leq n \leq k \leq 4$.

	$n \backslash k$	1	2	3	4
n/k-algorithm	1	6.32	4.48	3.69	3.34
	2	-	6.27	3.66	3.14
	3	-	-	5.49	4.19
	4	-	-	-	5.15
mean algorithm		6.32	3.94	3.09	2.72

4 Experiments

We evaluate the algorithms in Section 3 with practical palmprint images in terms of the criteria in Section 2.

4.1 Method

For the actual process of SIFT, the function "`SiftFeatureDetector`" in OpenCV [1] was used. The parameter "`threshold`" of the function was fixed at 0.01, and the other parameters were set to the default values.

The experiments were conducted on the PolyU Palmprint Database [2]. The sample set contains $1,200$ images that consists of 150 persons times 8 images. We separated the sample set into two sets of 150×4 images. An experiment was conducted with one set for templates and another set for input images, and repeated with swapping the sets. Additionally, we separated the set for templates into four sets of 150×1 images in order to construct template sets with different number of images for each person. For an experiment with k templates for each person, ${}_4C_k$ kinds of template sets are considered. Therefore, any value in the experiments is the arithmetic mean of the results for ${}_4C_k \times 600 \times 2$ trials.

4.2 Results

Fig. 1 shows the FRRs and FARs of the n/k-algorithm for $(k, n) = (1, 1)$ and $(4, 2)$, and the mean algorithm for $k = 4$. The mean algorithm for $k = 1$ equals to the n/k-algorithm for $(k, n) = (1, 1)$. The EERs of the n/k-algorithm and the mean algorithm for $1 \leq n \leq k \leq 4$ are shown in Table 1. As the result, we found that some improvements of the EER can be achieved by the simple methods from multiple templates for each person. Especially, considering the arithmetic mean of similarities yielded a larger reduction of the EER than a majority vote. For example, when $k = 4$, the EER of the mean algorithm was 2.72% while the optimum EER of n/k-algorithm is 3.14% for $n = 2$.

Fig. 2 shows the ERs of the nearest algorithm and the mean nearest algorithm for $k = 1$, 2, and 4. The mean nearest algorithm for $k = 1$ equals to the nearest algorithm. Fig. 3 shows the ERs of the linear search

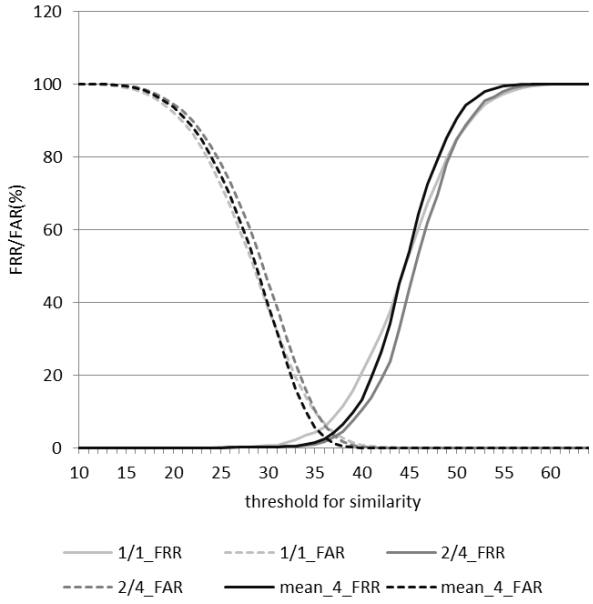

Figure 1: The FRRs and FARs against the threshold for the similarity of images of the n/k-algorithm for $(k, n) = (1, 1)$ and $(4, 2)$, and the mean algorithm for $k = 4$.

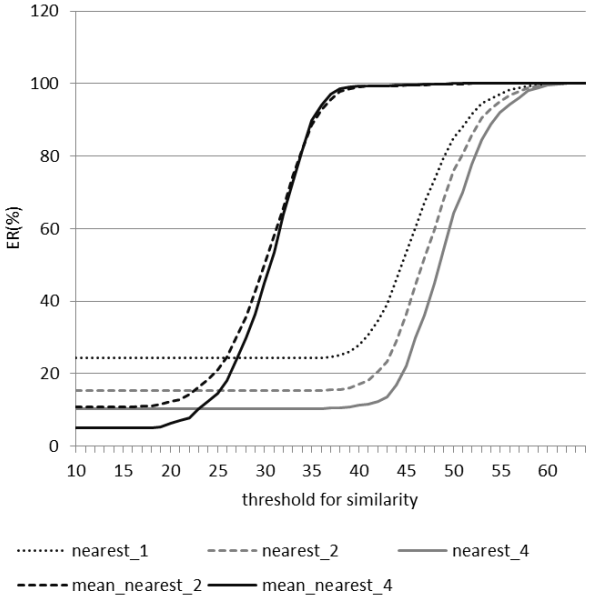

Figure 2: The ERs against the threshold for the image similarity of the nearest algorithm and the mean nearest algorithm for $k = 1$, 2, and 4.

algorithm for $k = 1$ and 4, the n/k-linear search algorithm for $(k, n) = (4, 2)$, and the mean linear search algorithm for $k = 4$. The n/k-linear search algorithm for $(k, n) = (1, 1)$ and the mean linear search algorithm for $k = 1$ respectively equal to the linear search algorithm for $k = 1$. The optimum ERs of the five algorithms are shown in Table 2.

By the results, we found that the ER of identification was improved in the five algorithms by the number of templates for a single person, especially, by considering the arithmetic mean of similarities we achieved a larger reduction of ER than the other simple methods. When $k = 4$, the optimum ER of the nearest algorithm was improved from 10.4% to 5.00% by considering the mean of similarities. The optimum ER of the linear search algorithm was improved from 24.9% to 16.1% by the idea of the mean, while the optimum value by the idea of a majority vote was 20.5%.

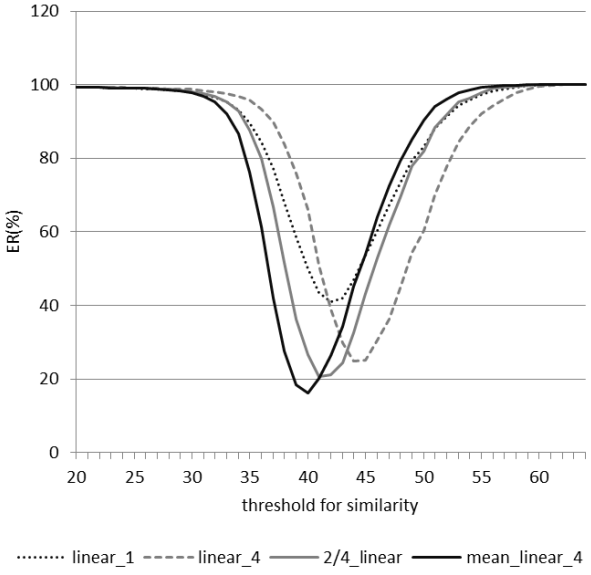

Figure 3: The ERs against the threshold for the image similarity of the linear search algorithm for $k = 1$ and 4, the n/k-linear search algorithm for $(k, n) = (4, 2)$, and the mean linear search algorithm for $k = 4$.

5 Conclusion

We conducted an accuracy analysis of personal authentication with biometric images. The effects of the number of templates for each person on accuracy of verification and identification were examined by considering simple algorithms based on the ideas of a majority vote and the arithmetic mean of similarities. As the result of the experiments with practical palmprint images, we achieved improvements of the error rates in verification and identification, especially, the algorithms based on the mean of similarities yielded better results than the algorithm based on the idea of a majority vote.

Table 2: The optimum ERs of the nearest algorithm, the mean nearest algorithm, the linear search algorithm, the n/k-linear search algorithm, and the mean linear search algorithm for $1 \leq n \leq k \leq 4$.

	$n\backslash k$	1	2	3	4
nearest algorithm		24.3	15.4	12.0	10.4
mean nearest algorithm		24.3	10.9	6.81	5.00
linear search algorithm		40.9	31.2	26.8	24.9
n/k-linear search algorithm	1	40.9	31.2	26.8	24.9
	2	-	32.9	25.0	20.5
	3	-	-	29.4	23.3
	4	-	-	-	27.6
mean linear search algorithm		40.9	26.3	19.5	16.1

Acknowledgement

This work was partially supported by 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 and CREST program of Japan Science and Technology Agency (JST) from 2008 to 2012.

References

[1] OpenCV. http://opencv.willowgarage.com/wiki/.

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

[3] I. Awad and K. Baba. Evaluation of a fingerprint identification algorithm with sift features. In *Proc. 2012 IIAI International Conference on Advanced Applied Informatics*, pages 129–132. IEEE, 2012.

[4] C. M. Bishop. *Pattern Recognition and Machine Learning*. Springer, 2006.

[5] J. Chen and Y.-S. Moon. Using SIFT features in palmprint authentication. In *Proc. 19th International Conference on Pattern Recognition*, pages 1–4. IEEE, 2008.

[6] 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.

[7] G. Iannizzotto and F. L. Rosa. A SIFT-based fingerprint verification system using cellular neural networks. In *Pattern Recognition Techniques, Technology and Applications*, pages 523–536. In-Tech, 2008.

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

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

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

[11] A. Morales, M. A. Ferrer, and A. Kumar. Improved palmprint authentication using contactless imaging. In *Proc. IEEE Fourth International Conference on Biometrics: Theory Applications and Systems*, pages 1–6. IEEE, 2010.

[12] U. Park, S. Pankanti, and A. K. Jain. Fingerprint verification using SIFT features. In *Proc. SPIE Defense and Security Symposium*, 2008.

[13] D. D. Zhang. *Palmprint Authentication*. Kluwer Academic Publishers, 2004.