EER, Robustness and Generation Condition of Fingerprint Templates Based on the Fractional Cosine and Sine Transforms

Hiroyuki Yoshimura
Graduate School of Engineering, Chiba University, Japan

Abstract

Recently, we have proposed new fingerprint templates based on the 1D discrete fractional Fourier, cosine and sine transforms (DFRT, DFCT and DFST) in order to realize the fingerprint recognition system with high recognition accuracy and high robustness against attacks. In this study, the generation condition of the fingerprint templates, i.e., a range of the transforms' orders, p_i*, is investigated in more detail to realize higher recognition accuracy. In addition, the EERs and the robustness are compared between the cases that a set of the transforms' orders is changed for each person and the set is unchanged for each person. As a result, in the case that the set is changed for each person, the most appropriate templates can be obtained as the phase distributions (PDs) of the DFCTs and the DFSTs under the condition that* $0.0< p_i \leq 0.3$ and $0.0< p_i \leq 0.5$.*The EER is an order of* 10^{-7}*% and fully smaller than that (2.45%) of the original fingerprint images. On the other hand, in the case that the set is unchanged for each person, the PDs of the DFCTs is the most appropriate templates under the condition that* $0.0< p_i \leq 0.3$*. The EER is 3.81% and a little bit higher than that of the original fingerprint images. The PSNRs are an order of several dB for both of the cases and it is found that proposed fingerprint templates have fully high robustness.*

1. Introduction

Individual recognition using the biological information has been recently increasing everywhere, for example, in the automatic logging into a PC, the immigration at the airport, and so on. In particular, the fingerprint recognition system has been widely used because of its high reliability and reasonable price [1]. In general, enrolled fingerprint images are stored as templates in the database referred in the fingerprint recognition process. The information of the templates should be hidden to keep individual biological information secret. Many methods have been recently proposed, for example, the biometric cryptosystems [2]-[5], the cancellable fingerprint templates [6]-[10], and so on. However, in these methods, since the minutia-based templates are basically used, the recognition accuracy tends to become low in comparison with that of the image-based templates.

In order to realize the fingerprint templates with high recognition accuracy and high robustness against attacks, we have first proposed a new generation method for the templates based on the DFRT [11]. In our method, the 1D DFRTs with different transforms' orders were applied to the 1D data extracted from the 2D original fingerprint image in a specific direction. Moreover, the fingerprint templates based on the DFCT and the DFST have also been proposed and evaluated the properties [12], [13]. In these studies [11]-[13], however, the genuine distributions were obtained from the fingerprint templates generated from the fingerprint data to which Gaussian random noise was added, though the genuine fingerprint images should have been used in nature.

In the previous study [14], the genuine fingerprint data in the database named DB_1 of the FVC 2002 [1] were used to obtain more accurate genuine distribution. As a result, it was found that the most appropriate fingerprint templates are the amplitude distributions (ADs) of the DFCTs and DFSTs of the original fingerprint images under that condition that the range of the transforms' orders is $0.1 \leq p_i \leq 1.0$. The robustness of the generated fingerprint templates was also evaluated by use of the PSNR and it was found that the generated fingerprint templates have high robustness.

However, a set of the transforms' orders was changed for different fingers, i.e., person to person. This means that, in the process of the recognition or enrollment based on our method, each person would need to have an IC card where the information about a set of the transforms' orders is recorded.

In this study, the generation condition of the fingerprint templates to realize high recognition accuracy, i.e., the range of the transforms' orders, is investigated in more detail. In addition, the case that a set of the transforms' orders is unchanged for different fingers is investigated and compared with the case that a set of the transforms' orders is changed for different fingers. In the situation that a set of the transforms' orders is unchanged for different fingers, an IC card where a set of the transforms' orders is recorded would not be needed and lead to more excellent biometrics because only his or her finger is needed.

2. Appropriate image size extracted from original fingerprint images

Fig. 1(a) shows an example of the original fingerprint images used in the FVC2002 [1]. It is one of the images in the database named Db_1 and has a size of 388 by 374 pixels and 500dpi. In the database, there are 800 images, i.e., 8 impressions for 100 fingers. In this study, the fingerprint images of 26 fingers having more than two cores were excluded. The fingerprints without cores were also excluded. As a result, 557 images for 74 fingers were selected. The cores' coordinates were obtained by the software named Verifinger [15]. Fig. 1(b) shows the extracted fingerprint image from Fig. 1(a). It has a size of 96 by 96 pixels and its central coordinate corresponds to the core's one of Fig. 1(a). The grayscale was also binarized by Verifinger.

For the 557 extracted fingerprint images, the EER [16] was investigated by use of the peak value (PV) of the normalized correlation function (NCF) between the two images, D_1 and D_2. The PV can be defined as

$$PV=\frac{\sum_{m=1}^{M}\sum_{n=1}^{N}D_1(m,n)D_2(m,n)}{\sqrt{\sum_{m=1}^{M}\sum_{n=1}^{N}D_1^2(m,n)}\sqrt{\sum_{m=1}^{M}\sum_{n=1}^{N}D_2^2(m,n)}}, \qquad (1)$$

where $D_1(m,n)$ and $D_2(m,n)$ are the grayscales of D_1 and D_2 at (m,n), respectively, and the size of the images is M by N pixels.

First of all, a basic fingerprint image which has the smallest average grayscale value was selected from 8 impressions (i.e., 8 genuine fingerprint images) for each finger. As mentioned above, there were 74 fingers so that the frequency of the impostor distribution was ${}_{74}C_2$=2,701. Next, the alignments of other genuine fingerprint images were also conducted using rotation and shift with the basic fingerprint image. The rotation alignment was conducted using the information about the PV of the NCF between the two images. The shift alignment was conducted using the information about the difference between the core's and PV's coordinates. The frequency of the genuine distribution was 1,836.

As a result, as shown in Table 1, it was found that the minimum EER is 2.45% under the condition that the size of the extracted images is 96 by 96 pixels. Moreover, on the basis of the PSNR expressed in terms of

$$PSNR=20\log_{10}\left(\frac{255}{RMSE}\right) \quad \text{[dB]}, \qquad (2)$$

where RMSE means the root-mean square error of the two different images, the EERs were also obtained as shown in Table 1. In general, if the value of PSNR is smaller than 20dB, then these two images may be regarded as different.

From this table, it was found that the minimum EER is 5.15% under the condition that the size of the extracted images is 64 by 64 pixels. In this study, the appropriate fingerprint image size could be selected as 96 by 96 pixels because the EER based on PV has the minimum value.

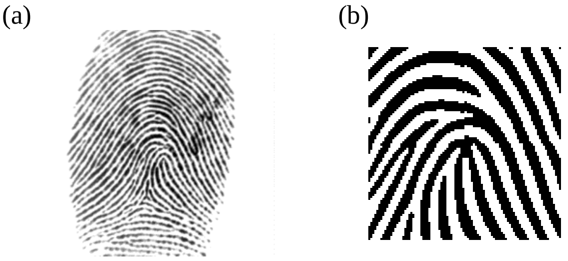

Figure 1. An example of fingerprint images. (a) Original fingerprint image named 1_1.tiff in Db1_a of the FVC2002, with a size of 388 by 374 pixels and 500 dpi. (b) Fingerprint image extracted from (a) with a size of 96 by 96 pixels and binarized by Verifinger. The central coordinate corresponds to the core's one of (a). (b) is also called the basic fingerprint image for the finger 1

Table 1. EERs based on the PV of the NCF and the PSNR for various extraction sizes of the fingerprint images

Size (pixels)	EER (%) based on *PV*	EER (%) based on *PSNR*
32×32	12.2	12.5
64×64	3.83	5.15
96×96	2.45	5.46
128×128	2.83	7.92

3. Generation method for proposed fingerprint templates based on DFCT and DFST

3.1. DFCT and DFST

The FRT is regarded as the generalization of a conventional Fourier transform (FT). The FRT of 1D input data $u(x)$ is defined as [17]

$$u_p(x_p)=\int u(x)\exp\left[\frac{i\pi\left(x_p^2+x^2\right)}{s\tan\phi}\right]\exp\left[-\frac{2\pi i x_p x}{s\sin\phi}\right]dx, \qquad (3)$$

where $\phi=p\pi/2$, p being the FRT's order, and s is a constant. When p takes a value of $4n$+1, n being an integer, the FRT data $u_p(x_p)$ corresponds to the conventional FT data. (3) can be easily calculated numerically by a computer [18] (i.e., DFRT).

The DFRT is defined as

$$u_p(n\delta x_p) = \sum_{m=-N/2}^{N/2-1} u(m\delta x)\exp\left[\frac{i\pi\left\{(n\delta x_p)^2 + (m\delta x)^2\right\}}{s\tan\phi}\right]$$
$$\times \exp\left[-\frac{2\pi imn\delta x_p\delta x}{s\sin\phi}\right]\delta x, \qquad (4)$$

where δx and δx_p are the sampling periods in x and x_p spaces, m and n are integers, and N is the number of samples. In addition, the DFRT can be expressed in terms of a combination of the DFCT of the even input function of u and the DFST of the odd input function of u, and given by [19]

$$DFRT_p = DFCT_p + \exp(-ip\pi/2)DFST_p \;, \qquad (5)$$

where p denotes the DFRT's, DFCT's and DFST's orders simultaneously. p is called the transform's order in the following.

3.2. Examples of proposed fingerprint templates

In order to obtain the fingerprint templates, the 1D DFCTs in the transverse lines of the extracted (and aligned) fingerprint images were performed by changing the transforms' orders uniformly and randomly in different transverse lines. The left-hand side of Fig.2 shows the same image as Fig. 1(b) and each line indicates 20th, 50th or 80th transverse line where the transform's order is given by p_{20}, p_{50} or $p_{80.}$ Basically, $p_{20} \neq p_{50} \neq p_{80}$, i.e., $p_i \neq p_j$ $(1 \leq i, j \leq 96)$ if $i \neq j$. The right-hand side of the figure shows an example of the PD of the DFCT with p_{20}, p_{50} or p_{80} in each line.

As an example, the transforms' orders, p_i, were changed uniformly and randomly between 0.0 and 0.3, i.e., $0.0<p_i \leq 0.3$, for Fig. 1(b) to obtain fingerprint templates. Figs. 3(a) and 3(b) are the PDs of the DFCTs and the DFSTs, respectively. These obtained templates have a size of 96 by 96 pixels. From these figures, it was found that the obtained templates look like random patterns.

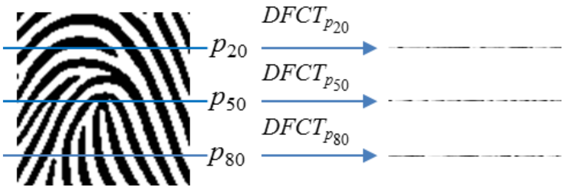

Figure 2. Method for generating the fingerprint template. The left-hand side of the figure shows the same image as Fig.1(b) and each line indicates 20th, 50th or 80th transverse line where the transform's order is p_{20}, p_{50} or p_{80}. The right-hand side of the figure shows an example of the PD of the DFCT with p_{20}, p_{50} or p_{80} in each line

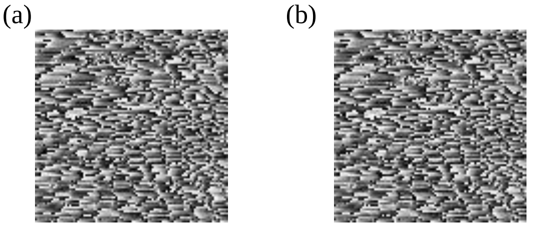

Figure 3. Examples of the fingerprint templates corresponding to the PDs of the DFCTs and DFSTs of Fig.1(b), respectively. The orders were changed uniformly and randomly with a range of $0.0<p_i \leq 0.3$. The size of these images is 96 by 96 pixels

In the next section, the EERs of the obtained fingerprint templates, i.e., the recognition accuracy, would be analysed quantitatively in order to decide the kinds of transforms (DFCT and DFST) and the range of the transforms' orders appropriately.

4. Basic ideas of the fingerprint recognition systems based on proposed templates

Fig.4 shows one of the ideas of the fingerprint recognition system based on our proposed fingerprint templates. Each person has to have an ID card where a set of the transforms' orders is recorded. In the recognition, each person needs his or her ID card and finger. A set of the transforms' orders is different from person to person. However, in this method, there is a defect that the merit of biometrics is not be used fully.

Fig.5 also shows the other idea of the fingerprint recognition system based on our proposed fingerprint templates. Each person does not need to have an ID card where a set of the transforms' orders is recorded. In the recognition, each person only needs his or her finger. A set of the transforms' order is recorded to the fingerprint recognition system.

In the following section, the EERs of our proposed templates are investigated in cases of Figs. 4 and 5, respectively.

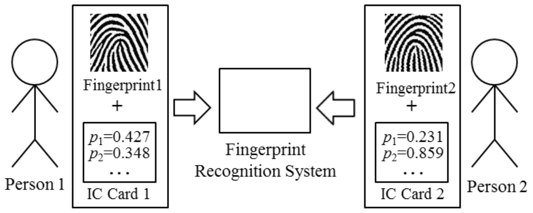

Figure 4. Basic idea of the fingerprint recognition system using proposed templates in the case that each person has to have an IC card where a set of the transforms' orders is recorded

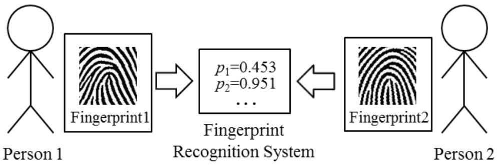

Figure 5. Basic idea of the fingerprint recognition system using proposed templates in the case that fingerprint recognition system has only one set of the transforms' orders. Therefore, each person does not need to have an IC card where a set of the transforms' orders is recorded

5. EER of proposed fingerprint templates

In this section, first, the behavior of the EERs of the fingerprint templates is investigated in case of Fig.4, that is, different sets of the transforms' orders for different fingers. The EERs are obtained based on the PV of the NCF. Next, the behavior of the EERs of the fingerprint templates is also investigated in case of Fig.5, that is, same set of the transforms' orders for different fingers. Finally, the appropriate generation condition of the templates would be indicated.

5.1. In case of different sets of transforms' orders for different fingers

Table 2 shows the result for various ranges of the transforms' orders. The order of zero was excluded because it corresponds to no transform for the original fingerprint image. From this tables, it is found that the values of the EERs of the fingerprint templates are fully smaller than that (i.e., 2.45%) of the original fingerprint images. This means that the proposed fingerprint templates have much higher recognition accuracy than that of the original fingerprint images. In particular, it is understood that the EER has the smallest value, i.e., the orders of 10^{-7}, in case of the DFCT and the DFST when the ranges of the transforms' orders are $0.0< p_i \leq 0.3$ and $0.0< p_i \leq 0.5$.

Table 2. EERs(%) for the proposed fingerprint templates in case of different sets of the tramsforms' orders for different fingers

	DFCT	DFST
$0.0< p_i \leq 1.0$	4.59×10^{-4}	4.96×10^{-4}
$0.1\leq p_i \leq 1.0$	1.01×10^{-3}	9.94×10^{-4}
$0.3\leq p_i \leq 1.0$	8.51×10^{-3}	9.23×10^{-3}
$0.5\leq p_i \leq 1.0$	9.37×10^{-2}	9.45×10^{-2}
$0.7\leq p_i \leq 1.0$	1.88	1.92
$0.0< p_i \leq 0.1$	1.73×10^{-6}	1.81×10^{-6}
$0.0< p_i \leq 0.3$	5.17×10^{-7}	5.63×10^{-7}
$0.0< p_i \leq 0.5$	6.78×10^{-7}	4.58×10^{-7}
$0.0< p_i \leq 0.7$	4.32×10^{-6}	4.17×10^{-6}

5.2. In case of same set of transforms' orders for different fingers

In the previous subsection, a set of the transforms' orders was changed for each different finger, i.e., person to person. This means that each person needs an IC card or something where the information about the set was recorded, when the recognition or the enrollment is conducted. However, such an IC card had better not be used to make use of a merit of biometrics. Therefore, the EER is investigated in the case that only one set of transforms' orders is used for different fingers. In this case, the information about the set could be installed in the recognition or enrollment system.

Table 3 shows the result. From this tables, it is found that the values of the EERs of the fingerprint templates have almost the same order as that (i.e., 2.45%) of the original fingerprint images. This means that the proposed fingerprint templates have almost the same recognition accuracy as that of the original fingerprint images. In particular, it is understood that the EER has the smallest value (i.e., 3.81%) in the case of the DFCT when $0.0< p_i \leq 0.3$. Because this value is a little bit larger than that of the original fingerprint images, the method for minimizing the EER should be considered.

Table 3. EERs(%) for the proposed fingerprint templates in case of same set of the tramsforms' orders for different fingers

	DFCT	DFST
$0.0< p_i \leq 1.0$	4.57	4.57
$0.1\leq p_i \leq 1.0$	4.78	4.69
$0.3\leq p_i \leq 1.0$	5.18	5.11
$0.5\leq p_i \leq 1.0$	5.87	5.94
$0.7\leq p_i \leq 1.0$	7.25	7.16
$0.0< p_i \leq 0.1$	3.94	3.95
$0.0< p_i \leq 0.3$	3.81	3.90
$0.0< p_i \leq 0.5$	3.85	3.83
$0.0< p_i \leq 0.7$	3.83	3.88

6. Robustness of proposed fingerprint templates

The robustness of the proposed fingerprint templates was analyzed by use of the PSNR between the extracted (and aligned) fingerprint image and the inverse-transformed image of the fingerprint template. The inverse-transformed image was obtained under the condition that inverse transform's order was the same as the transform's one in each transverse line.

Fig. 6 shows the examples of the inversed-transformed images of the proposed templates shown in Figs. 3(a) and 3(b) and the PSNRs are 5.98dB and

5.96dB, respectively. Therefore, it is found that the proposed fingerprint templates have high robustness.

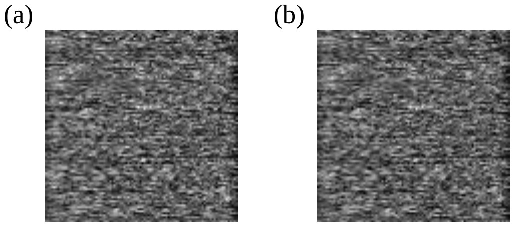

Figure 6. Examples of the inversed-transformed images of the proposed templates shown in Figs. 3(a) and 3(b)

In order to evaluate the robustness of the proposed fingerprint templates quantitatively, the averaged PSNRs were calculated for the proposed fingerprint templates, i.e., 557 PDs of the DFCTs and 557 PDs of the DFSTs, when the range of the transforms' orders was $0.0<p_{\mathrm{i}}\leq 0.3$, in case of different sets of p_{i} for different fingers. As a result, the averaged PSNRs of the PDs of the DFCTs and DFSTs became 5.98dB and 5.99dB, respectively.

The averaged PSNRs were also calculated in case of only one set of p_{i} for different fingers. As a result, the averaged PSNRs of the PDs of the DFCTs and DFSTs became the same value of 6.02dB.

Therefore, it is understood that the proposed fingerprint template could not be easily restored to the extracted (and aligned) fingerprint images even if the information about the transforms' orders is used. In this way, we can say that the proposed fingerprint templates have fully high robustness.

7. Conclusions

In this paper, the fingerprint templates generated by the DFCT and the DFST have been evaluated. Specifically, the generated fingerprint templates corresponded to the PDs of the 1D DFCTs and DFSTs with different transforms' orders for the grayscale distributions in different transverse lines of the extracted (and aligned) fingerprint image. In particular, the cases of different sets of the transforms' orders for different persons and only one set of the transforms' orders for different persons were compared to each other from the viewpoint of the EERs based on the PV of the NCF.

As a result, it has been found that the appropriate condition is $0.0< p_{\mathrm{i}} \leq 0.3$ and $0.0< p_{\mathrm{i}} \leq 0.5$ in case of different sets of the transforms' orders for different persons. The order of the EERs is 10^{-7} for PDs of the DFCTs and the DFSTs and fully smaller that (2.45%) of the original fingerprint images. However, in case of only one set of the transforms' orders for different persons, the minimum EER is 3.81% for PDs of the DFCTs when $0.0< p_{\mathrm{i}} \leq 0.3$ and a little bit larger than that of the original fingerprint images. In addition, the robustness related to the security of the generated templates is fully high, i.e., the PSNR is an order of several dB, for both of the two cases.

As a further study, how to minimize the EER without using the IC card should be considered well, for example, by generating a set of the transforms' orders based on the information about the fingerprint's minutiae of each person.

References

[1] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakr, *Handbook of Fingerprint Recognition*, Springer-Verlag, New York, 2003.

[2] U. Uludag and A. K. Jain, "Securing fingerprint template: Fuzzy vault with helper data," *Proceedings of 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, 2006, pp. 163-170.

[3] A. Nagar, K. Nandakumar and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," *Proceedings of 19th International Conference on Pattern Recognition, 2008 (ICPR2008)*, 2008, pp. 1-4.

[4] K. Xi, and J. Hu, "Biometric mobile template protection: A composite feature based fingerprint fuzzy valut," *Proceedings of IEEE International Conference on Communications 2009 (ICC'09)*, 2009, pp. 1-5.

[5] R. Wang, X. Yang, X. Liu, S. Zhou, P. Li, K. Cao and J. Tian, "A novel fingerprint template protection scheme based on distance projection coding," *Proceedings of 2010 20th International Conference on Pattern Recognition (ICPR)*, 2010, pp. 886-889.

[6] N. K. Ratha, S. Chikkerur, J. H. Connell and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2007, vol. 29, pp. 561-572.

[7] C. Lee, J. –Y. Choi, K. –A. Toh, S. Lee and J. Kim, "Alignment-free cancelable fingerprint templates based on local minutiae information," *IEEE Transactions on Systems, Man, and Cybernetics. Part B: Cybernetics*, 2007, vol. 37, pp. 980-992.

[8] H. Yang, X. Jiang and A. C. Kot, "Generating secure cancelable fingerprint templates using local and global features," *Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology, 2009 (ICCSIT 2009)*, 2009, pp. 645-649.

[9] B. Yang, C. Busch, P. Bours and D. Gafurov, "Non invertible geometrical transformation for fingerprint minutiae template protection," *Proceedings of the First International Workshop on Information Forensics and Security, 2009 (WIFS 2009)*, 2009, pp. 81-85.

[10] Z. Jin, A. B. J. Teoh, T. S. Ong and C. Tee, "Generating revocable fingerprint template using minutiae pair representation," *Proceedings of 2010 2nd International Conference on Education Technology and Computer (ICETC)*, 2010, vol. 5, pp. V5-251-V5-255.

[11] H. Yoshimura and Reiko Iwai, “New encryption method of 2D image by use of the fractional Fourier transform,” *Proceedings of ICSP'08 (The 9th International Conference on Signal Processing, IEEE)*, 2008, vol.3, pp.2182-2184.

[12] H. Yoshimura, “Fingerprint templates with high recognition accuracy and high security generated by discrete fractional sine transform,” *Proceedings of the sixth International Conference for Internet Technology and Secured Transactions (ICITST-2011, IEEE)*, 2011, pp.185-190.

[13] H. Yoshimura, “Recognition accuracy and robustness of fingerprint templates generated by discrete fractional sine transform,” *International Journal for Information Security Research*, 2012, vol. 2, pp. 266-273.

[14] H. Yoshimura, “Fingerprint templates generated by the fractional Fourier, cosine and sine transforms and comparison of recognition accuracy and robustness,” *Proceedings of SPIE*, 2014, vol.9234, 92340B.

[15] http://www.neurotechnology.com/verifinger.html

[16] T. Mansfield, G. Kelly, D. Chandler and J. Kane, “Biometric Product Testing Final Report, Issue 1.0,” CESG/BWG Biometric Test Programme, Centre for Mathematics and Scientific Computing, National Physical Laboratory, 2001.

[17] H. M. Ozaktas, Z. Zalevsky and M. A. Kutay, *The Fractional Fourier Transform*, John Wiley & Sons., New York, 2001.

[18] F. J. Marinho L. M. Bernardo, “Numerical calculation of fractional Fourier transforms with a single fast-Fourier-transform algorithm,” *Journal of the Optical Society of America*, 1998, vol. 15, pp. 2111-2116.

[19] S. –C. Pei and M. –H. Yeh, “The discrete fractional cosine and sine transform,” *IEEE Transactions on Signal Processing*, 2011, vol. 49, pp. 1198-1207.

Acknowledgements

This research was supported by JSPS KAKENHI Grant Number 24560039.