

Accuracy Analysis in Fingerprint Authentication Using the Fractional Fourier Transform without Misalignment Correction of Scanned Images

Reiko Iwai, Hiroyuki Yoshimura

Graduate School of Engineering, Chiba University, Chiba, Japan Email: reiko@tu.chiba-u.ac.jp, yoshimura@faculty.chiba-u.jp

Received December 26, 2011; revised January 17, 2012; accepted February 27, 2012

ABSTRACT

In many fingerprint authentication devices, a frame to insert the fingertip or a hollow to put the fingertip is used to avoid the position or rotation misalignment of a newly scanned genuine fingerprint image, when the fingerprint authentication is conducted. Moreover, the misalignment correction by the numerical calculation is indispensable for the fingerprint authentication devices to achieve the high accuracy. In this study, we investigated the effects of misalignment of the scanned genuine fingerprint image with the one used for generating the template on the accuracy in our fingerprint authentication method using the fractional Fourier transform (FRT). As a result, it was found that our method can achieve high authentication accuracy under the condition that the position-misalignment ratio is 17.6% or less and the rotation misalignment (rotation angle) is 28 degrees or less, even if the misalignment correction is not conducted.

Keywords: Fractional Fourier Transform; Fingerprint Authentication; Biometrics; Personal Information Protection

1. Introduction

The authentication of personal identities by fingerprints has been much researched until now. In particular, it has recently been paid attention to because of ease, cheap price and being used everywhere, such as ATMs in a bank, diligence and indolence management in an office, etc. It is also widely being installed in cell phones, notebook PCs because of its downsizing. In our previous studies [1-4], we have proposed a new data processing method using the FRT [5-9] to generate the secured fingerprint templates. In these studies, we assumed the fingerprint authentication devices for personal possessions such as cell phones, where other authentication measures such as an IC card, a key, etc., are not needed. As a result, we made clear that the authentication accuracy in our method has extremely high compared with that in the marketed compact fingerprint authentication products, even if dirt, sebum, etc., are attached to the fingertip and there are scratches. In addition, it was found that clearer impostor authentication can be achieved by use of other authentication measures and clearer genuine authentication can be achieved in our method even if fingertips have large cuts [10].

In many fingerprint authentication devices, a frame to insert the fingertip or a hollow to put the fingertip is used to avoid the position or rotation misalignment of a newly

oid the position or rotation misalignment of

scanned genuine fingerprint image, when the fingerprint authentication is conducted. Moreover, the misalignment correction by the numerical calculation is indispensable for the fingerprint authentication devices to achieve the high accuracy, and the researches on the misalignment correction have been conducted [11-16]. In these studies, the purpose was only the corrections of position-misalignment and distortion of the original images and the corrections were achieved by various methods. However, in these studies, the evaluation of the authentication accuracy using the fingerprint images before and after the corrections was not performed. Therefore, in this study, we clearly demonstrate the misalignment ranges in our method to perform the fingerprint authentication with the same or higher authentication accuracy in comparison with that in the compact marketed fingerprint authentication devices using the misalignment corrections. By this study, it will be made clear that the fingerprint authentication of high accuracy without misalignment corrections would be possible in our method based on processing the fingerprint images using the FRT. Moreover, we could easily guess that the fingerprint authentication with high accuracy would be possible in our method especially when the misalignment corrections are conducted. In this study, we investigate the effects of misalignment of a newly scanned genuine fingerprint image on the accuracy in our fingerprint authentication method using the template generated by the FRT. Noteworthy is that the our method can realize the high authentication accuracy without misalignment correction. Specifically, we would clear the upper limits of position and rotation misalignments of the scanned genuine fingerprint image, which satisfy the specifications of the authentication accuracy in the marketed products based on the frequency analysis method.

We prepare three kinds of real fingerprint images: the genuine fingerprint images; the genuine fingerprint images with position misalignment; the genuine fingerprint images with rotation misalignment, and focus on the peak value of the two-dimensional (2D) normalized cross-correlation function (NCF) between the intensity distributions of the FRTs (*i.e.*, the intensity FRTs). The intensity FRT is obtained by extracting 256×256 pixels at the center part of the 2D original fingerprint image and conducting the FRTs with the random FRT's orders in the different lines of the extracted image. Specifically, we obtain the peak values of the NCFs in the following: 1) the intensity FRT of the extracted genuine fingerprint image is registered (we call it the fingerprint template); 2) the intensity FRT of a newly scanned and extracted fingerprint image with position or rotation misalignment is obtained (we call it the intensity FRT with position or rotation misalignment); 3) the genuine distribution for the mean and the standard deviation of the peak value of the NCF derived from 1) and 2) is obtained. As for the impostor distribution, the mean 0.287 and the standard deviation 0.0484 of the 5995 peak values of the NCFs derived in our previous study [10] are used. Finally, we obtain the minimum error rate (MER) by a value satisfied with the condition the false acceptance rate (FAR) and the false rejection rate (FRR) take the same value [17]. The authentication threshold is also decided.

In Section 2, the generation method of the fingerprint templates is explained in brief. In Section 3, we obtain the properties of the peak values of the NCFs for genuine authentication between the fingerprint templates and the intensity FRTs with position misalignment. In Section 4, we obtain the properties of the peak values of the NCFs for genuine authentication between the fingerprint templates and the intensity FRTs with rotation misalignment. In Section 5, we evaluate the authentication accuracy based on the MER derived from the results obtained in Sections 3 and 4 in this study and in our previous study [10]. Finally, in Section 6, conclusions in our study and future study are described.

2. Generation Method of the Fingerprint Templates

In this section, the generation method of the fingerprint templates is explained. Fingerprint images provided by the Biometric System Laboratory [18] were used as original fingerprint images. The provided fingerprint images were 880 from 110 fingertips. For each fingertip, there were 8 fingerprint images. We selected one fingerprint image for each fingertip. Therefore, we used 110 original fingerprint images which were not affected by abrasion and distortion. As an example, **Figure 1** visualizes the data in the TIF format with 480 vertical and 640 horizontal pixels. In our previous study, it was clear that the fingerprint authentication accuracy is scarcely affected by extracted size [3]. Therefore in this study, as

fected by extracted size [3]. Therefore, in this study, as depicted in **Figure 2**, we analyzed using the fingerprint images with 256 vertical and 256 horizontal pixels extracted from the center of **Figure 1**. We call this image the genuine fingerprint image. The real size corresponds to 13.0 mm by 13.0 mm. In this study, as shown in **Figure 2**, height and width of the images are called line and column, respectively.

The FRT is the generalization of a conventional Fourier transform (FT). The FRT of the one-dimensional input data u(x) is defined as [19,20].



Figure 1. An example of the original fingerprint image.



Figure 2. Genuine fingerprint image with 256 lines and 256 columns extracted from the center of the image shown in Figure 1.

 $\times 10^{5}$ 12

$$u_{p}(x_{p}) = \int u(x) \exp\left[i\pi(x_{p}^{2} + x^{2})/s^{2} \tan\phi\right]$$

$$\times \exp\left[-2i\pi x_{p}x/s^{2} \sin\phi\right] dx,$$
 (1)

where $\phi = p\pi/2$, p = FRT's order, $s = \sqrt{\lambda f_s} = con$ stant (in the optical FRT, s is called a scale factor), $\lambda =$ wavelength and f_{e} = arbitrarily fixed focal length. In this study, the value of s was fixed at 1.0. In particular, p takes a value of 4n + 1, n being any integer, the FRT corresponds to the conventional FT. The intensity FRT, $I_p(x_p)$, is obtained by calculating $|u_p(x_p)|^2$.

In this study, the grayscale distribution in one line of a genuine fingerprint image shown in Figure 2 could be regarded as a wave pattern. The FRT was performed using Equation (1) in each line of the image by changing the FRT's order randomly and the intensity FRT distributions with the different FRT's orders in different lines were obtained. In Figure 2, the FRT's orders are expressed in terms of p_1, p_2, \dots, p_{256} and take values from 0.1 to 1.9 because this range has been thought to be the best performance in our processing method [4].

Figure 3 shows the intensity FRT of the genuine fingerprint image shown in Figure 2. In this study, this image is called the fingerprint template. The peak value of the fingerprint template is 1.18×10^6 . We prepared 110 fingerprint templates.

3. Properties of the Peak Values of the NCFs between the Fingerprint Templates and the Intensity FRTs with Position Misalignment

In this Section, we calculate the mean values and the standard deviations of the peak values of the NCFs between the fingerprint templates and the intensity FRTs with position misalignment. Figure 4 shows an example of the original genuine fingerprint image. It is a 256 \times 256 scanned image and used for generating the fingerprint template. Figure 5 shows eight 256×256 scanned genuine fingerprint images having position misalignments with Figure 4. The position-misalignment ratio in Figure 5 is 17.6%, *i.e.*, 46 pixels shift to different eight directions of Figure 4. The directions are 1) lower 46 lines; 2) upper 46 lines; 3) right 46 columns; 4) left 46 columns; 5) lower left 23 lines & 23 columns; 6) upper left 23 lines & 23 columns; 7) lower right 23 lines & 23 columns and 8) upper right 23 lines & 23 columns. The shift quantity was changed from 2 pixels to 46 pixels by 2 pixels. We prepared 110 fingerprint templates. For each fingerprint template, we prepared eight intensity FRTs of the fingerprint images with position misalignments. Therefore, 880 peak values of the NCFs between the fingerprint templates and the intensity FRTs with position misalignment were obtained for each shift quantity. The variation range of FRT's order p was from 0.1



image shown in Figure 2.



Figure 4. An example of the original genuine fingerprint image.

to 1.9.

The position-misalignment ratio (shift quantity) was calculated as follows. The whole number of pixels in a scanned fingerprint image is $256 \times 256 = 65536$. In the case of the position misalignment with 46 pixels in the lower, upper, right or left direction as shown in Figure 5 (a), (b), (c) or (d), the misalignment ratio becomes $256 \times$ $46/65536 \times 100 \approx 18.0\%$. On the other hand, in the case of that the position misalignment with 46 pixels in the oblique direction as shown in Figure 5(e), (f), (g) or (h), the misalignment ratio becomes $(256 \times 23 \times 2 - 23 \times 2)$ 23)/65536 \times 100 \approx 17.2%. By averaging these values, *i.e.*, (18.0 + 17.2)/2 = 17.6%, we decided the position-misalignment ratio with 46 pixels shift quantity.

As an example, Figure 6(a) denotes the fingerprint template obtained from Figures 4, 6(b) and (c) denote the intensity FRTs with 17.6% position-misalignment ratio (46 pixels shift quantity) in the directions of lower left and upper right, respectively. The peak values are 1) 6.51×10^{6} , 2) 4.74×10^{6} and 3) 5.99×10^{6} . Figure 7 shows the NCFs between the fingerprint template shown in Figure 6(a) and the intensity FRTs with position

300



Figure 5. Eight examples of the scanned genuine fingerprint images having 17.6% position-misalignment ratio (46 pixels shift quantity) with Figure 4, when the misalignment directions are (a) Lower; (b) Upper; (c) Right; (d) Left; (e) Lower left; (f) Upper left; (g) Lower right and (h) Upper right.

Figure 6. (a) The fingerprint template obtained from Figure 4. The intensity FRTs with 17.6% position-misalignment ratio (46 pixels shift quantity) in cases of (b) Lower left and (c) Upper right directions.



182

Figure 7. NCFs between the fingerprint template and the intensity FRT with position misalignment. (a) NCF between Figures 6(a) and (b); and (b) NCF between Figures 6(a) and (c).

misalignments shown in **Figures 6(b)** and **(c)**. The peak values are 1) 0.814 and 2) 0.870.

The mean values and the standard deviations for several position-misalignment ratios are summarized in Ta**ble 1**. In the table, misalignment ratios are 0.781% (2) pixels shift quantity), 3.89% (10 pixels shift quantity), 7.74% (20 pixels shift quantity), 11.6% (30 pixels shift quantity), 14.6% (38 pixels shift quantity) and 17.6% (46 pixels shift quantity). Then, the mean values take values from 0.844 to 0.968 and the standard deviations take values from 0.0276 to 0.0895. We can understand from the mean values in Table 1 that the authentication accuracy judged as a genuine person becomes worse with an increase in the position-misalignment ratio. However, it is found that there is no problem in the authentication between a genuine person and an impostor person, because the mean value for every position-misalignment ratios is fully higher than 0.287 which is the result of the

4. Properties of the Peak Values of the NCFs between the Fingerprint Templates and the Intensity FRTs with Rotation Misalignment

In this Section, we calculate the mean values and the standard deviations of the peak values of the NCFs between the fingerprint templates and the intensity FRTs with rotation misalignment. **Figure 8** shows two examples of the scanned genuine fingerprint images having rotation misalignments with **Figure 4**. The values of rotation angle are 1) 5 degrees and 2) 28 degrees. In our analysis, the values of rotation angle were changed from 1 to 28 degrees by 1 degree. We used the 110 fingerprint templates which are the same ones used in Section 3. Therefore, 110 peak values of the NCFs between the fingerprint templates and the intensity FRTs with rotation misalignment were obtained for each value of rotation angle. The variation range of FRT's order *p* was from 0.1 to 1.9.

Figure 9 denotes the intensity FRTs with the rotation misalignment having 1) 5 degrees and 2) 28 degrees rotation angles. The peak values are 1) 3.09×10^6 and 2) 8.34×10^6 . **Figure 10** shows the NCFs between the fingerprint template shown in **Figure 6(a)** and the intensity FRTs with rotation misalignments shown in **Figures 9(a)** and **(b)**. The peak values are 1) 0.860 and 2) 0.850.

The mean values and the standard deviations for several rotation angles are summarized in **Table 2**. In the table, rotation angles are 1 degree, 5 degrees, 10 degrees, 15 degrees, 25 degrees, 26 degrees and 28 degrees. Then, the mean values take values from 0.846 to 0.965 and the standard deviations take values from 0.0196 to 0.0770. We can understand from the mean values in **Table 2** that the authentication accuracy judged as a genuine person becomes worse with an increase in the rotation angle.



Figure 8. Two examples of the scanned genuine fingerprint images having the rotation misalignment with Figure 4, when the rotation angles are (a) 5 degrees and (b) 28 degrees.



Table 1. Mean values and standard deviations for various position-misalignment ratios.

Figure 9. The intensity FRTs with rotation misalignment in cases of (a) 5 degrees and (b) 28 degrees rotation angles.

(b)

Figure 10. NCFs between the fingerprint template and the intensity FRT with rotation misalignment. (a) NCF between Figures 6(a), 9(a) and (b) NCF between Figures 6(a) and 9(b).

600

However, it is found that there is no problem in the authentication between a genuine person and an impostor person, because the mean value for every rotation angle is fully higher than 0.287 which is the result of the impostor authentication [10].

5. Comparison of Authentication Accuracy between Our Method and the Conventional Fingerprint Authentication Device

5.1. In Case of the Position Misalignment

In this subsection, we evaluate the authentication accuracy based on the MER, considering the position misalignment. **Figure 11** is the result showing a set of genuine and impostor distributions of the peak values of the NCFs obtained from the genuine authentication of Section 3 in this study and the impostor authentication with the mean value 0.287 and the standard deviation 0.0484 in our previous study [10], respectively. In **Figure 11**, the left side one corresponds to the impostor distribution and the right side one was obtained in the case that the position-misalignment ratio is 17.6% in Section 3. In **Figure 11**, the MER is 0.00175 and the authentication threshold is 0.474.

MERs for various position-misalignment ratios are summarized in **Table 3**. In the table, the MERs take values from 4.30×10^{-19} to 0.00175 and the thresholds take values from 0.474 to 0.709. The data indicated by red letters correspond to the result obtained from **Figure 11**. For comparison, the most recent specifications of FARs and FRRs of the marketed products based on the frequency analysis method are indicated in **Table 4** [21]. In **Table 4**, the authentication accuracy is approximately less than from 0.0001% to 0.01% in the FAR and less than 0.1% in the FRR. The FAR and the FRR take different values, because the marketed products focus on the FAR. In this paper, however, we directly compare the MERs for various position-misalignment ratios in **Table 3** with the FARs in **Table 4**.

As a result, we found that our method has higher authentication accuracy in comparison with those shown in the recent available specification sheet of major fingerprint authentication systems in the market. This fact means that our method can sufficiently achieve the authentication accuracy with the normal security level shown in **Table 4** when the genuine fingerprint images have approximately less than 17.6% position-misalignment ratio as understood from **Table 3**. In addition, our method is equivalent to the authentication accuracy with the high security level when the genuine fingerprint images have approximately less than 14.6% position-misalignment ratio. Also the other smaller position-misalignment ratios are satisfied with the authentication accuracy with the high security level. Moreover, in our previous study [3], the mean value of the MERs of the variously extracted fingerprint images was about 1.10×10^{-3} . Therefore, it was also found that the authentication accuracy is considerably improved when the position-misalignment ratio is 14.6% or less as understood from **Table 3**.

5.2. In Case of the Rotation Misalignment

In this subsection, we evaluate the authentication accuracy based on the MER, considering the rotation misalignment. **Figure 12** is the result showing a set of genuine and impostor distributions of the peak values of the NCFs obtained from the genuine authentication of Section 4 in this study and the impostor authentication in our previous study [10], respectively. In **Figure 12**, the left side one corresponds to the impostor distribution. In particular, the right side one was obtained in the case that the rotation angle was 28 degrees in Section 4. In **Figure 12**, the MER is 0.00116 and the authentication threshold is 0.492.

MERs for various rotation misalignments are summarized in **Table 5**. In the table, the MERs take values from 2.82×10^{-24} to 0.00116 and the thresholds take values from 0.492 to 0.758. The data indicated by red letters correspond to the result obtained from **Figure 12**. We directly compare the MERs for various rotation misalignments (rotation angles) in **Table 5** with the FARs in **Table 4**.



Figure 11. The red curve is the genuine distribution obtained from the results in Section 3 when the position-misalignment ratio is 17.6%. The blue curve is the impostor distribution obtained from the results in our previous study [10].

Table 3. MERs for various position-misalignment ratios.

Position-misalignment ratio (%)	0.781	3.89	7.74	11.6	14.6	17.6
MER (%)	4.30×10^{-19}	3.58×10^{-6}	1.26×10^{-6}	3.23×10^{-5}	0.000193	0.00175
Threshold	0.709	0.530	0.538	0.512	0.495	0.474

Table 4. Specifications of the marketed products based on the frequency analysis method.

Security level	FAR (%)	FRR (%)
Low	< 0.01	N/A
Normal	< 0.001	< 0.1
High	< 0.0001	N/A

Table 5. MERs for various rotation misalignments (rotation angles).

Rotation angle (degree)	1	5	10	15	25	26	28
MER (%)	2.82×10^{-24}	1.40×10^{-7}	3.67×10^{7}	3.98×10^{-6}	7.62×10^{-5}	0.000102	0.00116
Threshold	0.758	0.550	0.542	0.524	0.498	0.517	0.492



Figure 12. The red curve is the genuine distribution obtained from the results in Section 4 when the rotation angle is 28 degrees. The blue curve is the impostor distribution obtained from the results in our previous study [10].

As a result, we found that our method has higher authentication accuracy in comparison with those shown in the recent available specification sheet of major fingerprint authentication systems in the market. This fact means that our method can sufficiently achieve the authentication accuracy with the normal security level shown in **Table 4** when the genuine fingerprint images have approximately less than 28 degrees rotation angle as understood from **Table 5**. In addition, our method is equivalent to the authentication accuracy with the high security level when the genuine fingerprint images have approximately less than 26 degrees rotation angle. Also the other smaller rotation misalignments are satisfied with the authentication accuracy with the high security level. Moreover, the mean value of the MERs of the variously extracted fingerprint images was about 1.10×10^{-3} [3]. Therefore, it was also found that the authentication accuracy is considerably improved when 26 degrees or less rotation angle as understood from **Table 5**.

6. Conclusion

The misalignment correction of a newly scanned genuine fingerprint image is indispensable for achieving the high authentication accuracy in many fingerprint authentication devices. In this study, we investigated the effects of the misalignment on the accuracy in our fingerprint authentication method using the template generated by the FRT. As a result, it was found that our method can achieve high authentication accuracy under the condition that the position-misalignment ratio is 17.6% or less and the rotation misalignment (rotation angle) is 28 degrees or less, even if the misalignment correction is not conducted. Therefore, the speeding up of the fingerprint authentication process and higher authentication accuracy can be strongly expected by use of our method. As a further study, the accuracy in our fingerprint authentication method should be evaluated by use of its prototype.

REFERENCES

[1] R. Iwai and H. Yoshimura, "A New Method for Improv-

ing Robustness of Registered Fingerprint Data Using the Fractional Fourier Transform," *International Journal of Communications, Network and System Sciences*, Vol. 3, No. 9, 2010, pp. 722-729. doi:10.4236/ijcns.2010.39096

- [2] R. Iwai and H. Yoshimura, "Matching Accuracy Analysis of Fingerprint Templates Generated by Data Processing Method Using the Fractional Fourier Transform," *International Journal of Communications, Network and System Sciences*, Vol. 4, No. 1, 2011, pp. 24-32. doi:10.4236/ijcns.2011.41003
- [3] R. Iwai and H. Yoshimura, "New Method for Increasing Matching Accuracy and Reducing Process Time of Fingerprint Data by the Fractional Fourier Transform," *Proceedings of* 2010 *IEEE* 17th International Conference on Image Processing, Hong Kong, Vol. 3, 26-29 September 2010, pp. 3061-3064. <u>doi:10.1109/ICIP.2010.5654171</u>
- [4] R. Iwai and H. Yoshimura, "High-Accuracy and High-Security Individual Authentication by the Fingerprint Template Generated Using the Fractional Fourier Transform," In: G. Nikolic, Ed., Fourier Transforms—Approach to Scientific Principles, Chapter 15, 2011, pp. 281-294.
- [5] D. Mendlovic and H. M. Ozatkas, "Fractional Fourier Transforms and Their Optical Implementation: I," *Journal of the Optical Society of America A*, Vol. 10, No. 9, 1993, pp. 1875-1881. <u>doi:10.1364/JOSAA.10.001875</u>
- [6] H. M. Ozatkas and D. Mendlovic, "Fractional Fourier Transforms and Their Optical Implementation: II," *Journal of the Optical Society of America A*, Vol. 10, No. 12, 1993, pp. 2522-2531. doi:10.1364/JOSAA.10.002522
- [7] F. J. Marinho and L. M. Bernardo, "Numerical Calculation of Fractional Fourier Transforms with a Single Fast-Fourier-Transform Algorithm," *Journal of the Optical Society of America A*, Vol. 15, No. 8, 1998, pp. 2111-2116. doi:10.1364/JOSAA.15.002111
- [8] H. M. Ozaktas, Z. Zalevsky and M. A. Kutay, "The Fractional Fourier Transform," John Wiley & Sons, Upper Saddle River, 2001.
- [9] X. Yang, Q. Tan, X. Wei, Y. Xiang, Y. Yan and G. Jin, "Improved Fast Fractional-Fourier-Transforms Algorithm," *Journal of the Optical Society of America A*, Vol. 21, No. 9, 2004, pp. 1677-1681. doi:10.1364/JOSAA.21.001677
- [10] R. Iwai and H. Yoshimura, "Improved Authentication Accuracy by Individually Set Orders of the Fractional Fourier Transform and Effects of Damage of Fingerprint Image on Authentication Accuracy," *International Journal of Communications, Network and System Sciences*, Vol. 4, No. 12A, 2011, pp. 770-777. doi:10.4236/ijcns.2011.432095
- [11] C. Gang, Z, Yao and N. Rongrong, "Forensic Estimation

of Gamma Correction in Digital Images," *Proceedings of* 2010 *IEEE* 17th International Conference on Image Processing, Hong Kong, 26-29 September 2010, pp. 2097-2110. doi:10.1109/ICIP.2010.5652701

- [12] A. Ross and R. Nadgir, "A Thin-Plate Spline Calibration Model for Fingerprint Sensor Interoperability," *IEEE Transaction on Knowledge and Data Engineering*, Vol. 20, No. 8, 2008, pp. 1097-1110. doi:10.1109/TKDE.2007.190696
- [13] H. Morimura, S. Shigematsu, T. Shimamura, K. Machida and H. Kyuragi, "A Pixel-Level Automatic Calibration Circuit Scheme for Capacitive Fingerprint Sensor LSIs," *IEEE Journal of Solid-State Circuits*, Vol. 37, No. 10, 2002, pp. 1300-1306. <u>doi:10.1109/JSSC.2002.803022</u>
- [14] A. A. K. Surya, A. S. Nugroho and C. Lim, "Evaluation of Fingerprint Orientation Field Correction Methods," *Proceedings of 2011 International Conference on Ad*vanced Computer Science and Information System, Jakarta, 2 August 2011, pp. 353-358.
- [15] Q. Zhao, A. Jain and G. Abramovich, "3D to 2D Fingerprints: Unrolling and Distortion Correction," *Proceedings* of 2011 International Joint Conference on Biometrics, Washington, DC, 11-13 October 2011, pp. 1-8. doi:10.1109/IJCB.2011.6117585
- [16] C. Cork, L. Depre and J. Tyminski, "Proximity Correction of IC Layouts Using Scanner Fingerprints," *Proceedings of 2007 IEEE/SEMI Advanced Semiconductor Manufacturing Conference*, Stresa, 11-12 June 2007, pp. 18-23. doi:10.1109/ASMC.2007.375073
- [17] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, "Handbook of Fingerprint Recognition," Springer, New York, 2003.
- [18] D. Maltoni and D. Maio, "Download Page of FVC2004," Biometric System Laboratory, University of Bologna, Bologna, 2004. http://bias.csr.unibo.it/fvc2004/ download.asp
- [19] H. M. Ozaktas, O. Arikan and M. A. Kutay, "Digital Computation of the Fractional Fourier Transform," *IEEE Transactions on Signal Processing*, Vol. 44, No. 9, 1996, pp. 2141-2150. <u>doi:10.1109/78.536672</u>
- [20] A. Bultheel and H. E. M. Sulbaran, "Computation of the Fractional Fourier Transform," *Applied Computational Harmonic Analysis*, Vol. 16, No. 3, 2004, pp. 182-202. doi:10.1016/j.acha.2004.02.001
- [21] DDS Co., Ltd., "Hybrid Biometric Authentication Device, Hybrid Biometric Authentication Method, and Computer-Readable Storage Medium Where Computer Program for Hybrid Biometric Authentication Is Stored," WO 2009/ 096475 A1, 2009 http://www.freepatentsonline.com/WO2009096475.pdf