Proceedings of "The 6th SEAMS-UGM Conference 2011"
Computer, Graph and Combinatorics, pp.601–614.

A Comparison Framework for Fingerprint Recognition Methods

Ary Noviyanto and Reza Pulungan

Abstract. Many fingerprint recognition methods have been proposed and the need arises for a methodology to compare these methods, in order to be able to decide whether a particular method is better than another. In this paper, we report on our effort to develop a methodology to compare the robustness of fingerprint recognition methods. As a case study, we apply this methodology to compare two recent fingerprint recognition algorithms proposed by Chikkerur (2005) and Wibowo (2006). We are able to conclude that, overall, Chikkerur's algorithm performs better than Wibowo's.

Keywords and Phrases: Fingerprint recognition methods, comparison framework.

1. INTRODUCTION

The needs for biometrics that can be used to recognize people based on their bodily characteristics have existed long. Biometric recognition is associated with identification ("Who is X?") and verification ("Is this X?") [13]. Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, conceived an idea that body measurements can be used to identify criminals; and this has changed major law enforcement departments in the mid-19th century [3].

Not all body measurements can be eligible to be a biometric. Human fingerprint, which has been used for authentication purposes for more than 100 years [3, 4, 7], is one of the most well-known biometrics. Fingerprints can be a biometric because they have characteristics that are feasible to measure, distinct, permanent, accurate, reliable, and acceptable [7]. There are three levels of fingerprints' features that can be used in recognition processes [5]:

(1) Global level: the ridge flows of fingerprints create particular patterns, such as shown in Figure 1.

2010 Mathematics Subject Classification: 68T10

(2) Local level: there are 150 different patterns or forms of ridges in fingerprints. These patterns are called minutiae (see Figure 2). The most popular minutiae are *ridge endings* and *ridge bifurcations*.
(3) Very-fine level: at this level, we look at the deeper levels of detail in the ridges. The most important feature is *finger sweet pore*, which can be observed using a high resolution sensor (1000 dpi) (see Figure 2).

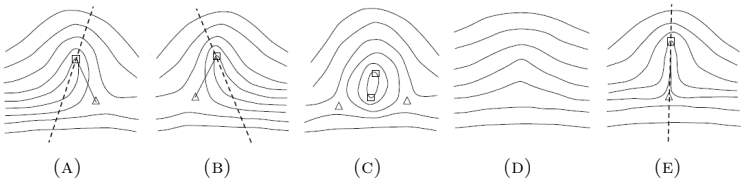


FIGURE 1. Global level of fingerprints' features [5]: (A) Left-loop, (B) Right-loop, (C) Whorl, (D) Arch, and (E) Tented-arch

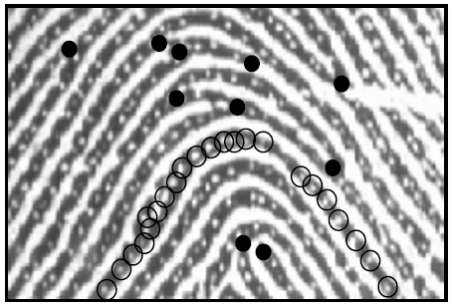


FIGURE 2. Black solid circles are *minutiae* and circles with hole are *sweat pore* [5]

Several researchers have attempted to propose fingerprint recognition methods (FRM), such as Chikkerur [1] and Wibowo [12]. Methodologies and techniques to compare those FRMs are required. In this paper, we are going to report on our effort to build a comparison framework for FRMs, that considers the minutiae as the distinguishing features. The comparison framework measures the quality of the methods based on their robustness. An FRM is robust if it can distinguish every input properly. The robustness of an FRM can also be analyzed from the robustness of each phase involved in FRM. If each phase of the fingerprint recognition method is robust, we can then confidently take a conclusion that the FRM itself is robust.

2. PRELIMINARIES

2.1. **Failures in Biometric System.** There are two possible errors in biometric systems [2], namely:

(1) *α-error*, which is a failure occurring when comparison results reject or conclude as different, things which are the same. Hence, this is also called a *false non-match*. The ratio of this failure is called *false non-match rate* (FNMR) or *false reject rate* (FRR).
(2) *β-error*, which is a failure occurring when comparison results accept or conclude as the same, things which are different. Hence, this is also called a *false match*. The ratio of this failure is called *false match rate* (FMR) or *false accept rate* (FAR).

2.2. **False Non-Match (FNM) and False Match (FM).** In order to define FNM and FM, we first define feature extraction, matching and the process of making conclusions. We define a sample of biometrics as S_{ik}; where i is the individual that the biometric sample belongs to and k denotes the index of the successful acquisition process (different samples of biometrics can be acquired from the same individual). The features of every biometric sample S_{ik}, denoted by X_{ik}, is then extracted. The result of matching, denoted by $Y_{ik,i'k'}$, is obtained from matching biometric samples S_{ik} and $S_{i'k'}$. The next process is to decide whether the two biometric samples represent the same biometric. Given a threshold τ, two biometrics are not similar if $Y_{ik,i'k'} > \tau$ and two biometrics are similar if $Y_{ik,i'k'} \leq \tau$.

We define $D_{ii'j}$, a binary function that represent the j-th conclusion taken from comparing the biometrics of the i-th and i'-th individuals. If the value of $D_{ii'j}$ is one, then the sistem has made a mistake and if the value of $D_{ii'l}$ is zero, then the sistem was right. $D_{ii'l}$ is defined as follows:

$$D_{ii'j} = \begin{cases} 1 & \text{jika } i = i' \text{ and } Y_{ik,ik'} > \tau, \\ 0 & \text{jika } i = i' \text{ and } Y_{ik,ik'} \leq \tau, \\ 0 & \text{jika } i \neq i' \text{ and } Y_{ik,i'k'} > \tau, \\ 1 & \text{jika } i \neq i' \text{ and } Y_{ik,i'k'} \leq \tau. \end{cases} \tag{1}$$

From $D_{ii'k}$ we can compute False Non-Match Rate (FNMR) dan False Non-Match Rate (FMR) as follows:

$$\text{FMR} = \frac{\sum_i \sum_{i' \neq i} \sum_j D_{ii'j}}{\sum_i \sum_{i' \neq i} n_{ii'}}, \text{ and,} \tag{2}$$

$$\text{FNMR} = \frac{\sum_i \sum_j D_{iij}}{\sum_i n_{ii}}, \tag{3}$$

where $n_{ii'}$ is the number of comparisons between two individuals, and n_{ii} is the number of time an individual is compared with himself. If $i = i'$ then the comparison is called *genuine matching* and if $i \neq i'$ then the comparison is called *imposter matching*.

2.3. **Sensitivity and Specificity.** *Sensitivity* and *specificity* are used to measure the success of an algorithm in detecting *minutiae* [8]. They are defined as follows:

$$\text{Sensitivity} = 1 - \frac{\text{missedminutiae}}{\text{groundtruth}}, \text{ and} \tag{4}$$

$$\text{Specificity} = 1 - \frac{\text{falseminutiae}}{\text{groundtruth}}, \tag{5}$$

where missedminutiae is the number of genuine *minutiae* that are not detected, falseminutiae is the number of false *minutiae* that are detected, and groundtruth is number of *minutiae* that are defined by fingerprint experts.

2.4. **Equal Error Rate (ERR).** *Equal Error Rate* (ERR) is an objective evaluating criteria for classifier performance testings. It is objective in the sense that the rejection threshold is selected independently. Equal Error Rate defines the intersection point between FNMR and FMR curves as the function of the rejection threshold [6]. In other words, ERR is a value where FNMR is equal to FMR, as shown in Figure 3.

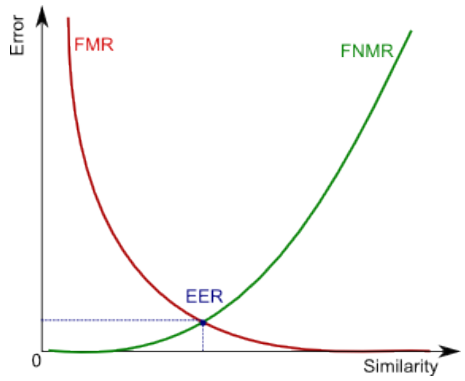


FIGURE 3. The Relationship between FNMR, FMR and ERR

2.5. **Mean and Standard Deviation.** *Mean* is used to assert the common value from a collection of values. The mean of N data X_i, denoted by $\bar{X}$, is defined by [9]:

$$\bar{X} = \frac{\sum_{i=1}^{N} X_i}{N}. \tag{6}$$

Beside mean, we need a way to measure the spread of the collection of values from its means. *Standard deviation* of N data X_i, denoted by s, is defined by [9]:

$$s = \sqrt{\frac{\sum_{i=1}^{N}(X_i - \bar{X})^2}{N-1}}. \tag{7}$$

3. THE COMPARISON FRAMEWORK

We divide the whole fingerprint recognition process into three parts, namely enhancement process, feature extraction process and matching process. To get a complete view of the quality of two fingerprint recognition methods or more, we need to compare the three parts separately. The results of the partial comparisons will inform us about the relative quality of the given fingerprint recognition methods. We therefore define a comparison framework that contains testings for each part, namely enhancement testing, feature extraction testing, and matching testing.

3.1. **Enhancement Testing.** The enhancement testing is a testing that compares *only* the enhancement process of fingerprint recognition methods. The aim of this testing is to compare the success rate of each enhancement process. Figure 4 shows how enhancement testings are carried out. To fairly compare the quality of enhancement processes, we use third party softwares that do not contain any enhancement process whatsoever. We use MINDTCT [11] as feature extraction software and BOZORTH3 [10] as matcher software to perform verification. The quality of each enhancement process is then represented by its FNMR and FMR.

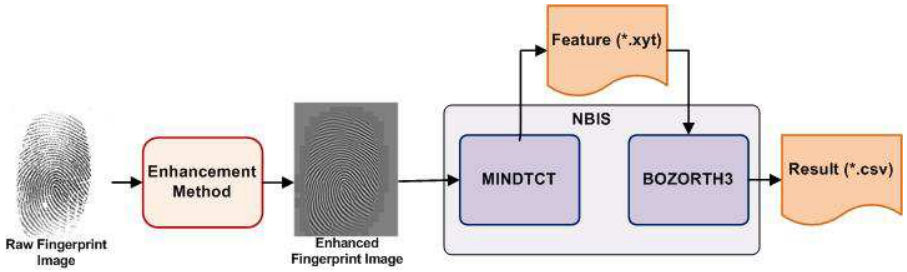


FIGURE 4. The Flow Diagram of the Enhancement Testing

3.2. **Feature Extraction Testing.** The feature extraction testing is a testing that compares *only* the feature extraction process of fingerprint recognition methods. The difficulty of this testing lies in that a particular feature extraction method might be linked with a particular enhancement method during analysis. Therefore, we need to pass all necessary parameters from the enhancement process to the feature extraction process, if any. We have to make sure that the image is not changed after the enhancement process. Figure 5 shows that the enhancement process is retained in the testing, but filtering process that modifies the raw image is removed. With this scheme, parameters that are required during the feature extraction process can be passed on without changing the input image, and hence the input images before and after the enhancement process are the same.

The result as shown in Figure 5 is a fingerprint image with additional feature points. We then compute the values of *sensitivity* and *specificity* to determine the performance of the feature extraction process. Ideally we need fingerprint experts to

create a standard template of the genuine fingerprint features, so that we can compute the values of *sensitivity* and *specificity* precisely.

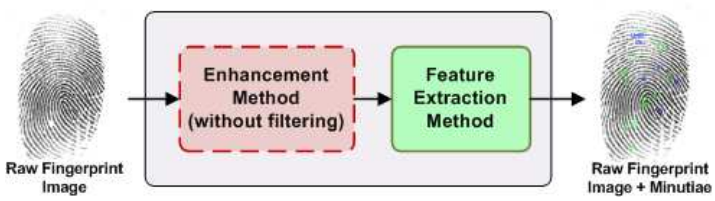


FIGURE 5. The Flow Diagram of the Feature Extraction Testing

3.3. **Matching Testing.** The matching testing is a testing that compares *only* the matching process of fingerprint recognition methods. The difficulty of this testing lies in the differences of features' representation. A particular matcher might be related with a particular features' representation. Therefore, features' representations are converted to a particular format that conforms with the matchers. To compare fairly, we have to make sure that the features are the same although they might have different representations.

In this testing, we compute mean and standard deviation of matched feature points (*minutiae*) in *genuine matching* and *imposter matching*. Using the combination of the values of mean and standard deviation of matched minutiae, the performance of matcher to determine fingerprint images through its features can be observed. The distance of the mean ± standard deviation between *genuine matching* and *imposter matching* is required to determine the threshold. The greater the distance, the easier it is to determine the threshold. An overlap of the mean ± standard deviation between *genuine matching* and *imposter matching*—i.e., their mean ± standard deviation intersect each other—means that there must have been mistakes or failures in the matching process. If such overlap exists, the threshold cannot be determined precisely.

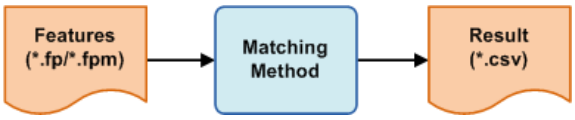


FIGURE 6. The Flow Diagram of the Matching Testing

3.4. **Overall Testing.** Beside the partial testings (i.e., enhancement testing, feature extraction testing and matching testing), we also perform an overall testing that compares the whole process of fingerprint recognition methods. This testing is used to compare the evaluation results of the fingerprint recognition methods.

EER is used as an evaluating measure for this overall testing . EER provides information of the best performance of the FRM, namely when its value is the same as that of FNMR.

4. EXPERIMENTAL DATA

We collect our data set using a 500 dpi resolution fingerprint sensor that can produce images of size 280 × 360 pixels. Figure 7 shows several examples of the obtained fingerprint images. We also have a particular naming scheme: each fingerprint image is named according to format: *name.fingerprint-code.index-of-acquisition.bmp*.

(A) (B) (C) (D) (E)

FIGURE 7. Several fingerprint images in 500 dpi resolution: (A) agung.0.03.bmp, (B) ata.1.06.bmp (C) kartika.2.01.bmp, (D) christ.3.03.bmp, and (E) illy.4.01.bmp

From 16 volunteers, a total of 640 fingerprint images have been collected. From each volunteer we took 40 images; eight different images for each finger.

5. EXPERIMENTAL RESULTS

To demonstrate the use of the framework, we will use and compare the implementations of two fingerprint recognition methods based on Chikkerur's [1] and Wibowo's [12].

5.1. **Enhancement Testing Result.** In this phase, we compare two enhancement methods: *STFT analysis method* [1] and *Gabor filter method* [12]. The result of the enhancement testing is shown in Table 1 and Table 2. Table 1 shows the comparison of FNMR and FMR of both Chikkerur's and Wibowo's methods for each data set. The values of the mean and the corresponding standard deviation of data in Table 1 are presented in Table 2.

The values of FNMR and FMR from Table 1 are also depicted in Figure 8. From Figure 8a, we can observe that Chikkerur's method performs better than Wibowo's method; Chikkerur's values of FNMR are less than Wibowo's. In Figure 8b, Wibowo's method performs better than Chikkerur's. However, as can be observed, the y-axis of the graph in Figure 8b ranges only between 0 and 1 (while the y-axis of the graph in Figure 8a ranges between 0 and 16); hence the difference in the FMR results is not

TABLE 1. Enhancement Testing Result

Data set	**Comparison**	**Method** (%)	
		Chikkerur's	**Wibowo's**
1	FNMR	3.57	10.71
	FMR	0.03	0.07
2	FNMR	0.36	0.36
	FMR	0.00	0.00
3	FNMR	5.54	7.14
	FMR	0.87	0.83
4	FNMR	1.07	5.54
	FMR	0.00	0.00
5	FNMR	2.14	7.14
	FMR	0.00	0.00
6	FNMR	7.86	15.36
	FMR	0.16	0.00
7	FNMR	0.36	0.36
	FMR	0.05	0.00
8	FNMR	3.04	10.71
	FMR	0.54	0.07

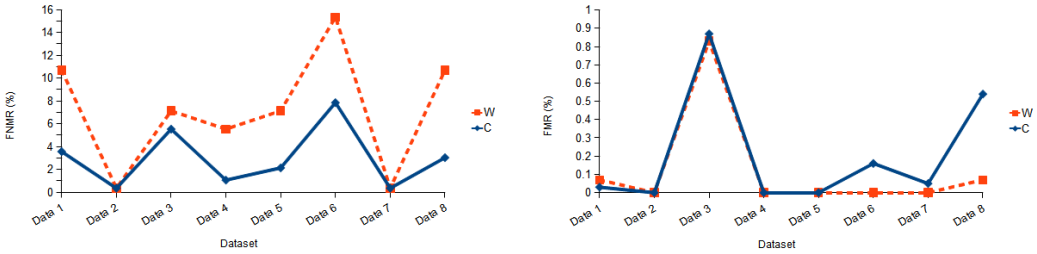
TABLE 2. Mean and STD of FNMR and FMR from Table 1

Parameter Comparison	**Method** (%)	
	Chikkerur's	**Wibowo's**
Mean FNMR	2.99	7.17
STD FNMR	2.64	5.18
Mean FMR	0.21	0.12
STD FMR	0.32	0.29

as significant as that of FNMR results. Overall, we can conclude that Chikkerur's enhancement method performs better than Wibowo's enhancement method.

5.2. **Feature Extraction Testing Result.** In the second testing, we compare two feature extraction methods: *chain code* based method [1] and *templating* based method [12]. The result of feature extraction testing is shown in Table 3. The columns of Table 3 are as follows:

(1) *File Name* is name of the file of the fingerprint image.
(2) *Ground truth* is the number of the genuine minutiae based on benchmark.
(3) *Total* is the total number of minutiae that can be extracted.
(4) *Missed* is the number of genuine minutiae that cannot be extracted.
(5) *False* is the number of minutiae that are extracted but not genuine.
(6) *Match* is the number of minutiae that are extracted and genuine.

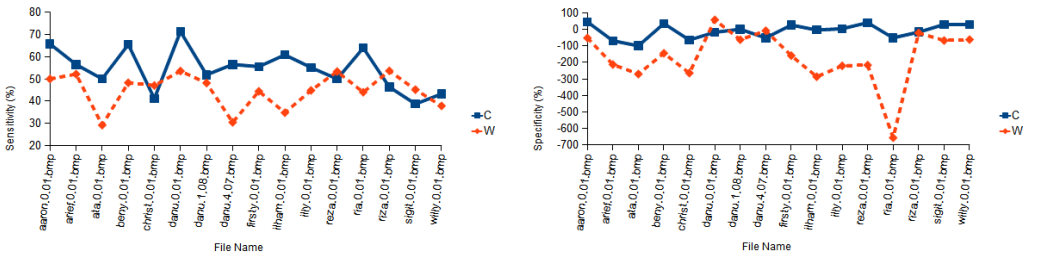


(A) FNMR (B) FMR

FIGURE 8. Enhancement testing result: (A) the values of FNMR for each data set, and (B) the values of FMR for each data set. The continuous line represents Chikkerur's enhancement method while the dashed line Wibowo's

(7) *Sens.* and *Spec.* are the values of sensitivity and specificity, respectively.

The associated sensitivity and specificity of the two methods from Table 3 are shown in Figure 9. From Figure 9, we observe that both sensitivity and specificity of Chikkerur's method are higher than those of Wibowo's. This means that Chikkerur's feature extraction method performs better than Wibowo's features extraction method.



(A) Sensitivity (B) Specificity

FIGURE 9. Feature extraction result: (A) the values of sensitivity, and (B) the values of specificity. The continuous line represents Chikkerur's enhancement method, while the dashed line represents Wibowo's

5.3. **Matching Testing Result.** In this testing, we compare two matching methods: *graph-based* [1] and *point pattern matching based on alignment* methods [12]. The result

Table 3. Feature Extraction Testing Result

No	File Name	Ground truth	Total		Missed		False		Match		Sens. (%)		Spec. (%)	
			C	W	C	W	C	W	C	W	C	W	C	W
1	aaron.0.01.bmp	38	46	77	13	19	21	58	25	19	65.79	50.00	44.74	-52.63
2	arief.0.01.bmp	23	52	84	10	11	39	72	13	12	56.52	52.17	-69.57	-213.04
3	ata.0.01.bmp	24	60	96	12	17	48	89	12	7	50.00	29.17	-100.00	-270.83
4	beny.0.01.bmp	29	38	85	10	15	19	71	19	14	65.52	48.28	34.48	-144.83
5	christ.0.01.bmp	17	35	70	10	9	28	62	7	8	41.18	47.06	-64.71	-264.71
6	danu.0.01.bmp	28	53	27	8	13	33	12	20	15	71.43	53.57	-17.86	57.14
7	danu.1.08.bmp	27	41	57	13	14	27	44	14	13	51.85	48.15	0.00	-62.96
8	danu.4.07.bmp	23	48	32	10	16	35	25	13	7	56.52	30.43	-52.17	-8.70
9	firsty.0.01.bmp	27	35	82	12	15	20	70	15	12	55.56	44.44	25.93	-159.26
10	ilham.0.01.bmp	23	38	97	9	15	24	89	14	8	60.87	34.78	-4.35	-286.96
11	illy.0.01.bmp	29	44	106	13	16	28	93	16	13	55.17	44.83	3.45	-220.69
12	reza.0.01.bmp	30	33	111	15	14	18	95	15	16	50.00	53.33	40.00	-216.67
13	ria.0.01.bmp	25	54	200	9	14	38	189	16	11	64.00	44.00	-52.00	-656.00
14	riza.0.01.bmp	41	67	72	22	19	48	50	19	22	46.34	53.66	-17.07	-21.95
15	sigit.0.01.bmp	31	34	66	19	17	22	52	12	14	38.71	45.16	29.03	-67.74
16	willy.0.01.bmp	37	43	74	21	23	27	60	16	14	43.24	37.84	27.03	-62.16
Average		**28.25**	**45.06**	**83.50**	**12.88**	**15.44**	**29.69**	**70.69**	15.38	12.81	**54.54**	**44.80**	**-10.82**	**-165.75**
STD		**6.26**	**9.99**	**38.71**	**4.32**	**3.29**	**9.65**	**39.27**	**4.08**	**4.17**	**9.46**	**7.91**	**44.91**	**167.91**

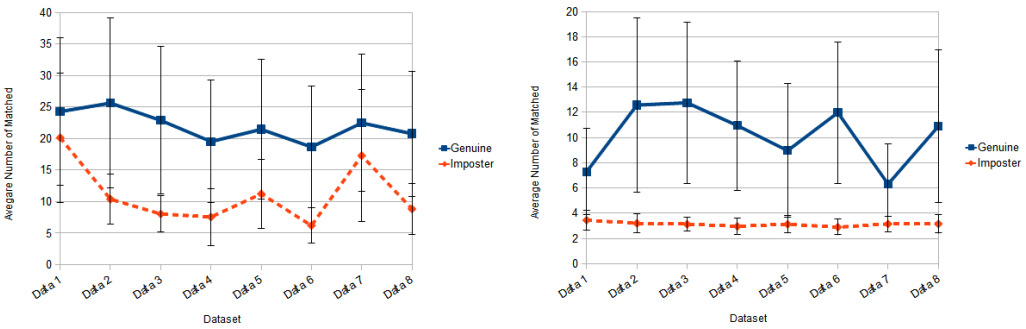
Table 4. Matching Testing Result

Data set	Method							
	Chikkerur's				Wibowo's			
	Mean Genuine	STD Genuine	Mean Imposter	STD Imposter	Mean Genuine	STD Genuine	Mean Imposter	STD Imposter
1	7.29	3.43	3.45	0.79	24.28	11.73	20.14	10.30
2	12.58	6.94	3.20	0.73	25.63	13.47	10.40	3.95
3	12.76	6.39	3.13	0.55	22.90	11.73	8.05	2.87
4	10.95	5.15	2.96	0.63	19.53	9.69	7.57	4.51
5	8.97	5.32	3.13	0.69	21.47	11.12	11.23	5.44
6	11.98	5.62	2.90	0.61	18.68	9.60	6.22	2.76
7	6.32	3.15	3.15	0.60	22.49	10.83	17.31	10.45
8	10.90	6.03	3.16	0.74	20.78	9.93	8.84	4.03
Avg.	**10.22**	**5.25**	**3.14**	**0.67**	**21.97**	**11.01**	**11.22**	**5.54**

Table 5. The Overall Testing Result

Data set	Method											
	Chikkerur's						Wibowo's					
	EER (%)	FNMR/ FMR	Mean Gen. (%)	STD Gen. (%)	Mean Imp. (%)	STD Imp. (%)	EER (%)	FNMR/ FMR	Mean Gen. (%)	STD Gen. (%)	Mean Imp. (%)	STD Imp. (%)
1	7.60	0.20	18.54	12.65	6.48	3.26	19.51	0.43	22.74	9.84	18.24	7.42
2	10.00	0.10	28.08	15.20	7.64	1.79	19.10	0.23	38.07	18.70	15.45	5.20
3	11.30	0.05	27.91	12.90	7.95	1.87	17.60	0.18	38.83	18.13	13.66	4.51
4	14.50	0.04	38.61	14.64	9.48	2.46	18.70	0.20	37.74	17.77	13.83	6.16
5	9.60	0.14	21.40	12.77	7.60	1.86	19.77	0.30	33.42	18.17	16.27	6.73
6	13.55	0.05	32.09	13.81	9.31	2.48	17.20	0.20	40.15	19.28	13.30	5.13
7	6.95	0.28	21.47	18.08	6.26	2.27	21.38	0.40	25.62	10.86	18.39	8.46
8	12.20	0.09	31.35	16.02	8.64	2.52	18.50	0.24	36.53	18.50	14.64	5.75
Avg.	**10.71**	**0.12**	**27.43**	**14.51**	**7.92**	**2.31**	**18.97**	**0.27**	**34.14**	**16.41**	**15.47**	**6.17**
STD	**2.69**	**0.08**					**1.31**	**0.10**				

of the matching testing is shown in Tabel 4. Tabel 4 shows comparison of the mean and the standard deviation of genuine and imposter matchings. The values of the mean and the standard deviation of both genuine and imposter matchings of both methods are plotted in Figure 10.



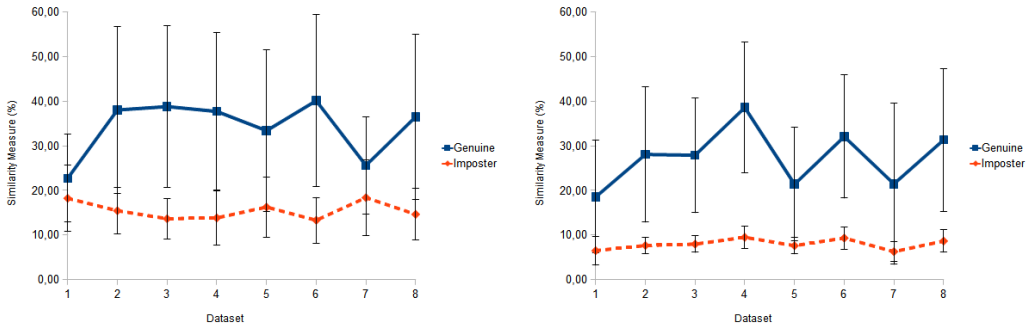
(A) Wibowo's (B) Chikkerur's

FIGURE 10. Matching testing result: (A) Wibowo's matching method, and (B) Chikkerur's matching method. The continuous line represents genuine matching, while the dashed line represents imposter matching

From Figure 10, we observe that Wibowo's method produces more overlaps than Chikkerur's method (seven overlaps compared to three). This means that Chikkerur's matcher has better ability in distinguishing fingerprint images based on their features than Wibowo's matcher.

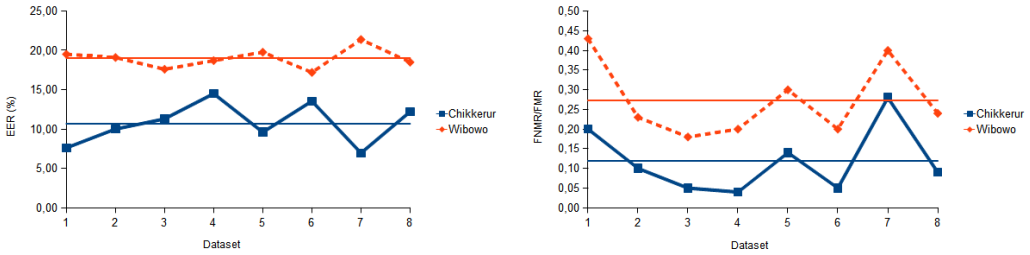
5.4. **Overall Testing Result.** The overall testing result is shown in Table 5. Table 5 shows the comparison of EER with the corresponding FNMR/FMR and also the comparison of the mean and the standard deviation of both genuine and imposter matchings (Mean Gen., STD Gen., Mean Imp. and STD Imp.). The values of the mean and the standard deviation of both genuine and imposter matchings are the measure of the similarity between two fingerprint images. The comparison of the mean and the standard deviation of both genuine and imposter matchings is depicted in Figure 11 and the comparison of EER with the corresponding FNMR/FMR is depicted in Figure 12.

From Figure 11, we observe that Chikkerur' method produces greater gaps between genuine matching and imposter matching than Wibowo's method. This means that Chikkerur's method is able to distinguish fingerprint images better than Wibowo's. This result can also be confirmed in Figure 12: Chikkerur's method produces higher values of FNMR/FMR than Wibowo's method.



(A) Wibowo's (B) Chikkerur's

FIGURE 11. Overall testing result: the similarity value of (A) Wibowo's method, and (B) Chikkerur's method. The continuous line represents genuine matching, while the dashed line represents imposter matching



(A) EER (B) FNMR/FMR

FIGURE 12. Overall testing result: the value of (A) EER, and (B) FNMR/FMR. The continuous line represents Chikkerur's FRM, while the dashed line represents Wibowo's FRM

6. CONCLUDING REMARKS

Our experiment shows that, overall, Chikkerur's FRM is better then Wibowo's FRM. This conclusion is based on the partial comparison results. The result is that Chikkerur's enhancement method performs better than Wibowo's, which is shown by the fact that Chikkerur's method has smaller false non-match rate in accuracy testing. The Chikkerur's feature extraction method also performs better than Wibowo's, which is shown by its higher values of sensitivity and specificity. For matching method,

Chikkerur's method can distinguish features format better than Wibowo's method. In addition, we estimate the classification accuracy of the whole FRM in the overall testing. In this testing, Chikkerur's method has a higher accuracy than Wibowo's. Hence, the partial testings and the overall testing bring us to the same conclusion: Chikkerur's method is better than Wibowo's.

In this paper, we have developed a framework that can be used to compare fingerprint recognition methods. We have also demonstrated the use of the proposed framework by comparing two recent methods. The experiments showed that the comparison framework performs well in measuring the relative quality of the two fingerprint recognition methods. Since a fingerprint recognition method can usually be divided into the three processes—i.e., enhancement, feature extraction and matching processes—the proposed comparison framework provides specific and detailed information in each process. The comparison results of each process enable us to investigate the performance of a fingerprint recognition method in a more detail way. This framework provides a basis to compare other fingerprint recognition methods.

References

[1] Chikkerur, S.S.: Online Fingerprint Verification System. Master's thesis, State University of New York at Buffalo, Buffalo, New York, June 2005.
[2] Dunstone, T., Yager, N.: Biometric System and Data Analysis Design, Evaluation, and Data Mining. Springer, 2009.
[3] Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20, 2004, http://dx.doi.org/10.1109/TCSVT.2003.818349.
[4] Komarinski, P.: Automated Fingerprint Identification Systems (AFIS). Academic Press, 2004.
[5] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer Publishing Company, Incorporated, 2009.
[6] Poh, N., Bengio, S.: Evidences of equal error rate reduction in biometric authentication fusion. Idiap-RR Idiap-RR-43-2004, IDIAP, 2004.
[7] Ravi, J., Raja, K.B., Venugopal, K.R.: Fingerprint Recognition Using Minutia Score Matching. CoRR abs/1001.4186, 2010.
[8] Sherlock, B., Monro, D., Millard, K.: Fingerprint enhancement by directional Fourier filtering. IEEE Proceedings - Vision, Image, and Signal Processing, 141(2), 87–94, 1994, http://link.aip.org/link/?IVI/141/87/1.
[9] Stockburger, D.W.: Introductory statistics: Concepts, models and applications 1998, http://business.clayton.edu/arjomand/book/sbk00.html.
[10] Watson, C.I., Garris, M.D., Tabassi, E., Wilson, C.L., Mccabe, R.M., Janet, S., Ko, K.: User's Guide to Export Controlled Distribution of NIST Biometric Image Software (NBIS-EC), 2007.
[11] Watson, C.I., Garris, M.D., Tabassi, E., Wilson, C.L., Mccabe, R.M., Janet, S., Ko, K.: User's Guide to NIST Biometric Image Software (NBIS), 2007.
[12] Wibowo, M.E.: Sistem Identifikasi Sidik Jari Berdasarkan Minutiae. Master's thesis, Universitas Gadjah Mada, Yogyakarta, Indonesia, Oktober 2006.
[13] Woodward, J.D., Orlans, N.M.: Biometrics. McGraw-Hill, Inc., New York, NY, USA 2002.

Ary Noviyanto
Faculty of Computer Science, Universitas Indonesia, Indonesia
e-mail: ary.noviyanto@ui.ac.id

Most of this work was done when the first author was with Universitas Gadjah Mada

REZA PULUNGAN
Department of Computer Science and Electronics
Faculty of Mathematics and Natural Sciences, Universitas Gadjah Mada, Indonesia
e-mail: pulungan@ugm.ac.id