TELKOMNIKA, Vol.11, No.4, December 2013, pp. 739~748
ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v11i4.1389

Time Series Based for Online Signature Verification

Pande Sutawan[1], Darma Putra*[2]
Department of Information Technology, Udayana University
Bukit Jimbaran, Badung, Bali, Indonesia, Telp. 03617853533
*Corresponding author, e-mail: sutawan.pande@gmail.com[1], ikgdarmaputra@gmail.com[2]

Abstrak

Sistem verifikasi tanda tangan merupakan proses pencocokan tanda tangan yang diuji dengan tanda tangan yang diklaim. Tulisan ini mengusulkan metode pengenalan ciri berbasis runtun waktu dan metode dynamic time warping untuk pencocokannya. Sistem yang dibuat menggunakan 900 data tanda tangan dari 50 partisipan yang teridiri atas 3 tanda tangan acuan untuk pengenalan ciri dan pencocokan menggunakan 5 tanda tangan dari masing-masing pengguna asli, simple imposters dan trained imposters. Pada pengujian ini diperoleh akurasi sistem tanpa pemalsu adalah 90,45 % di nilai ambang 44 dengan kesalahan penolakan (FNMR) adalah 5,2% dan kesalahan penerimaan (FMR) adalah 4,35 %, ketika dengan pemalsu akurasi sistem adalah 80,1% pada nilai ambang 27 dengan kesalahan penolakan (FNMR) adalah 15,6% dan kesalahan penerimaan (rata-rata FMR) adalah 4,26%, dengan rincian sebagai berikut: kesalahan penerimaan adalah 0,39 %, kesalahan penerimaan pemalsu sederhana adalah 3,2% dan kesalahan penerimaan pemalsu terlatih 9,2%.

Kata kunci: *verifikasi, biometrika, runtun waktu, tanda tangan online*

Abstract

Signature verification system is to match the tested signature with a claimed signature. This paper propose time series based for feature extraction method and dynamic time warping for match method. The system made by process of testing 900 signatures belong to 50 participants, 3 signatures for reference and 5 signatures from original user, simple imposters and trained imposters for signatures test. The final result system was tested with 50 participants with 3 references. This test obtained that system accuracy without imposters is 90,45 % at threshold 44 with rejection errors (FNMR) is 5,2% and acceptance errors (FMR) is 4,35 %, when with imposters system accuracy is 80,13 % at threshold 27 with error rejection (FNMR) is 15,6% and acceptance errors (average FMR) is 4,26 %, with details as follows: acceptance errors is 0,39%, acceptance errors simple imposters is 3,2% and acceptance errors trained imposters is 9,2%.

Keywords*: verification, biometric, time series, online signature*

1. Introduction

Information technology issues increasing rapidly making personalized recognition system automatically becomes something very important. There are two types of verification and identification for recognition system. Using a key or card have some weakness, such as: can be lost or stolen, can be used together, and easily duplicated. Same like use of user id, PIN, and passwords also have some problems, such as: don't remember (forgotten), can be used by other person, and passwords can be predicted. Biometric use unique characteristics of human physiological or behavioral. Biometrics may not be forgotten, is not easily lost, personal used only, and difficult to duplicate. This is cause biometrics widely used for automatic person recognition system for identification and verification systems. There are six common biometric use of for biometrics systems, such as fingerprint, iris, face, voice, hand geometry, and signature [1].

Signature a mean of personal identity authentication and verification. It is highly desirable to automate the process for the accurate identification of genuine handwritings and the detection of forged ones [2]. The handwritten signature is a biometric attribute [3]. Biometric signature is very common, and studies that have been published on the use of a signature verification system much especially offline signature. Offline signature has a low level of reliability due to the features of offline signature less than the signature line. Biometric signature

Received May 2, 2013; Revised July 8, 2013; Accepted July 24, 2013

verification systems that are based on the dynamic of a person's signature and not on its image (socalled online signature verification) are considerably better for a reliable authentication [4]. Online signature has more dimensions that are not in offline signature, so the signature line has a higher level of reliability than the offline signature.

Several studies has used biometrics for online signature verification systems using a variety of methods for feature extraction include: using dynamic RBF network, time series to obtain the characteristic motifs [4], using algorithms based on time sequences to obtain the feature [5], using a support vector machine to acquire the feature [6], artificial neural networks [7], stroke matching, angular transformation for e-commerce services [8], etc. In this study, online signature characteristic is obtained by using the method of time series in the motion direction of a signature from start to the end writing on regular basis.

Details include a process of data collection, processing preparation, extraction process online signature traits using time series method, until the matching process through trial given quantitatively and qualitatively, and ends with the conclusions and suggestions of development.

2. Research Method

Signature verification system is the process signature matching tested with a signature that is claimed. The decision result is a signature authorized or unauthorized. Acquisition process characteristic signature plays an important role towards the success of the verification. In this research, the feature extraction of signatures obtained using time series method. While the process of matching using dynamic time warping method.

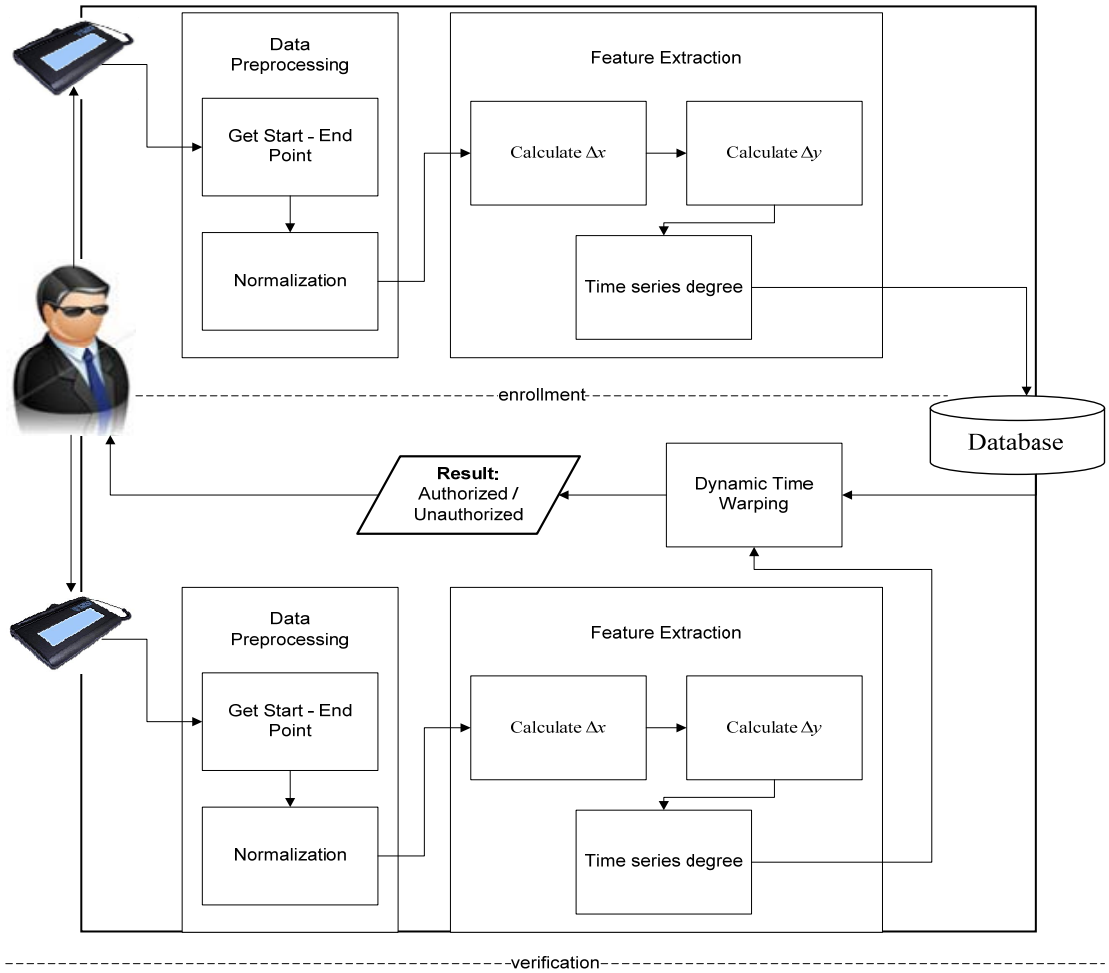

Figure 1. Overview System

2.1 Signature Online Acquisition

Online signature samples obtained input from Signature Gem LCD signature pad 1x5. Output generated signature pad are point coordinates *x* axis and *y* axis are sequentially starting from the beginning until the end autograph signatures periodically.

(a) (b)

Figure 2. Signature online acquisition (a) signature pad, (b) signature online

2.2 Preprocessing

Preprocessing aims to equalize the signature input, so not dependent on scale (small large signature), rotation (tilt signature) and translational (position to coordinate 0,0 signature field). Preprocessing also aims to align the center of the signature. Equation for the set consistent scale:

$$x_i = \frac{x_{\mathrm{i}}^{O} - x_{\min}}{x_{\max} - x_{\min}} W \quad (1)$$

$$y_i = \frac{y_{\mathrm{i}}^{O} - y_{\min}}{y_{\max} - y_{\min}} H \quad (2)$$

Points $(x_{\mathrm{i}}^{O}, y_{\mathrm{i}}^{O})$ are points for normalize, points (x_i, y_i) are result from normalize, $x_{\min} = \min\{x_{\mathrm{i}}^{o}\}$, $y_{\min} = \min\{y_{\mathrm{i}}^{o}\}$, $x_{\max} = \max\{x_{\mathrm{i}}^{o}\}$, $y_{\max} = \max\{y_{\mathrm{i}}^{o}\}$,*W* and *H* are the width and heigth, in this research *W* and *H* are 300. Result from normalized Figure 2 (b) is show in Figure 3.

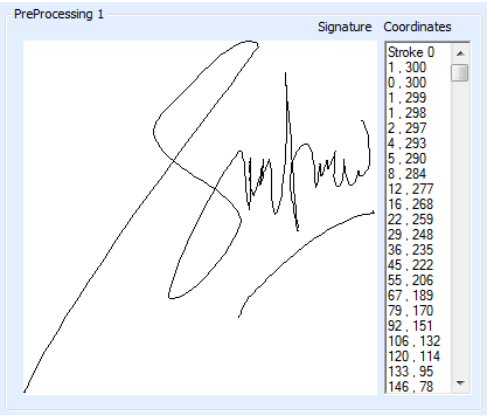

Figure 3. Signature Online Preprocessing

2.3 Feature Extraction

Signatures that have been processed in the preprocessing stage will then be processed further to get the features that reflect the characteristics of the signature. Feature often used in signature verification system, among others:

1. Total time spent to create a signature

2. Values of velocity signature changes based on the *x* axis and *y* axis
3. The length of time the pen is pressed or lifted
4. The overall length of the signature line
5. Motion direction

Feature extraction in this system using signature feature of motion direction. The process feature extraction is done by processing the points that have been obtained from the results preprocessing.

Figure 4 show an illustration of time series at feature extraction. Points normalized results calculated by the equation (3), (4) and (5) from start until end points.

$$\Delta x = x_i - x_p \quad (3)$$

$$\Delta y = y_i - y_p \quad (4)$$

$$\theta_i = tan^{-1}\left(\frac{\Delta y}{\Delta x}\right) \quad (5)$$

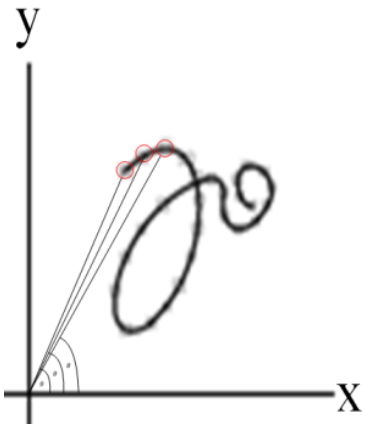

Figure 4. Time series illustration

Points x_i, y_i are points result from normalized, points x_p, y_p are the central points. Equation (3) used to determine the Δx value, meaning that the value of *x* results preprocessing reduced the central point value *x*. Equation (4) used to determine the Δy value, meaning the value of *y* results preprocessing reduced the center point *y* value. Equation (5) is used to determine the value of $\theta_i, \ldots, \theta_n$ of all points. Theta value is the result feature extraction are stored in the database and used in the match process. Result feature extraction are time series degree values. The example feature extraction result Figure 4 as shown below:

909090909089898888878583817975706559514436282116120806040302020101010000000000102040710141721252830313334353637383839393938383838383838383839393940424345474950535456575859606060606059585755525047444239373433313029282727272727272829303132333435353636373737373636353433323129292828272828282930303132333333343434343433323230292828272626262627282829303030313131313131303029282827272626262627282829303030313131313131303029282827262626262627282829303031323233343435343435343433323129282624222018161412100908080807070707080910121416182023252729303233343435353535343433333231313029282727262525242322222121202020202021212223232425252626262727262626252524232323232232232323232324242424242424242423232222222121212121212222222223232323222222221212121202020201919192020202122222323242425252525242424232322222121202020212121222223232424252525252424242323222221212020202119181717161515141414131352525251515050494847464443413938363433313029292828272727272626262626262626262626

Each value of feature extraction is represented by two characters in sequence from beginning to end, so length of the value is 462. Results of feature extraction from time series is

very detailed, long rows of time series values could reach thousands depending from length and the short signature.

2.4 Matching Similarity

Signature verification process is comparing signature with the reference signature contained in the system. Signature entered into the system typically ranges from 3 to 10 signatures. Signature tested with a reference signature has been found in the system, and using a particular threshold value to determine whether the signature authorized or unauthorized. Dynamic time warping is a method for calculating the distance between time series data. DTW advantage of other distance method is able to calculate the distance of two vectors of data with different lengths. DTW distance between two vectors is computed from the bending line optimal (optimal warping path) of the second vector. To calculate the most reliable DTW is a dynamic programming method. DTW distance can be calculated by the equation [6-8]:

$$D(UV) = \gamma(m,n) \tag{6}$$

$$\gamma(m,n) = d_{base}(u_j, v_j) + \min[\gamma(i-1,j), \gamma(i-1,j-1), \gamma(i,j-1)] \tag{7}$$

$$\gamma(0,0) = 0, \gamma(0,\infty) = 0, \gamma(\infty,0) = \infty \tag{8}$$

2.5 Perfomance Evaluation

Evaluate accuracy of the signature verification system is calculated from the error value False Non Match Rate (FNMR) with False Match Rate (FMR) of the genuine user and value False Non Match Rate (FNMR) genuine user with average False Match Rate (FMR) of the original user's, simple imposter, trained imposter. Simple imposter is the signature forger who only saw once and immediately forged signatures. Trained imposter is the signature forger who forged signature with the training process.

Verification system test using 900 signatures belong to 50 participants, each participant representing 3 reference signature and test signature 5 signatures original participants. Simple imposters and trained imposters each represent 5 signatures. Perfomance test of the system is done by calculating the value of FNMR with FMR and FNMR with average FMR (genuine user, simple imposters, trained imposters). FNMR stated probability sample of users does not match the other references given same user, FMR stated probability sample of users matched with references drawn at random belong to different users while the EER (Equal Error Rate) stated error rate when FNMR = FMR. FNMR and FMR values are very dependent on the threshold value T is used. Different T values produce FNMR, FMR and the EER is very small at a certain threshold value. Score is obtained by unauthorized users match test signature with a reference signature of the same person, while unauthorized users score is obtained by comparing test signature with a reference signature belongs to people who are not the same.

3. Results and Analysis

Testing online signature verification using time series method done in 2 stages:

1. Determaining the best reference
2. Database size test

3.1 Determaining The Best Reference

This test is used to analyze accuracy of the system againts the number of references that used in this system. Size of database that used in thih test is 50 participants. Table 1 and 2 shows the result of this test.

Table 1. Reference without imposters

Reference	T	FNMR	FMR	Accuracy
1	64	8,4	12,38367	79,21632653
2	47	9,6	5,257143	85,14285714
3	44	5,2	4,35102	90,44897959

Table 2. Reference with imposters

Reference	T	FNMR	Avg FMR	Accuracy
1	51	16,8	14,6	68,53
2	26	16,1	6,95	76,95
3	27	15,6	4,26	80,14

Table 1 and Table 2 can be presented with a chart as shows in Figure 5.

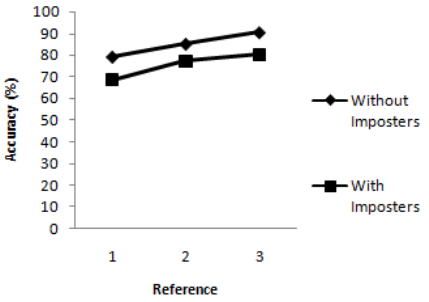

Figure 5. Graph Reference

Figure 5 shows that the system accuracy increases along with the number of references in database.

3.2 Database size test

This test is used to analyze stability of the system against the number / size of database that used in this system. Maximum size of database that used in this test is 50 participants. The test will be performed with 3 references. Result of this test is shown in graphical as shown as Figure 6-11 with the following note: False non match rate is shown by a line with dot mark; False match rate is shown by a line with “x” mark; False match rate of simple imposters is shown by a line with triangle mark; False match rate of trained imposters is shown by a line with rectangle mark; Average of false match rate is shown by a line without any mark.

1. Test with 15 participants database number 1

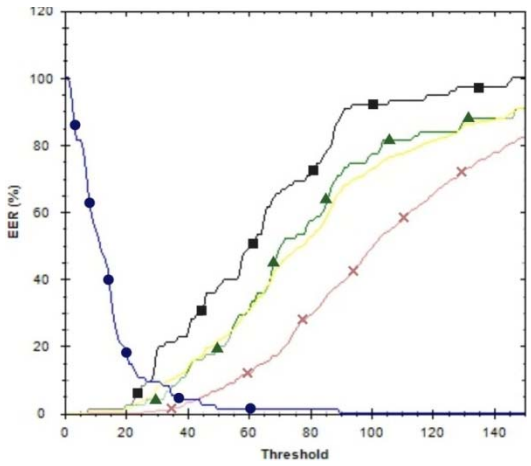

Figure 6. Graph 15 participants database number 1

This test obtained that system accuracy without imposters is 94,19048% at threshold 37 with rejection errors (FNMR) is 4% and acceptance errors (FMR) is 1,809524%, when with imposters system accuracy is 83,52381% at threshold 22 with error rejection (FNMR) is 14,66667% and acceptance errors (average FMR) is 1,809524%, with details as follows: acceptance errors is 0,095238%, acceptance errors simple imposters is 2,666667% and acceptance errors trained imposters is 2,666667%.

2. Test with 15 participants database number 2

This test obtained that system accuracy without imposters is 88,09524% at threshold 46 with rejection errors (FNMR) is 4% and acceptance errors (FMR) is 7,904762%, when with imposters system accuracy is 83,11111% at threshold 37 with error rejection (FNMR) is 10,66667% and acceptance errors (average FMR) is 6,222222%, with details as follows: acceptance errors is 4%, acceptance errors simple imposters is 6,666667% and acceptance errors trained imposters is 8%.

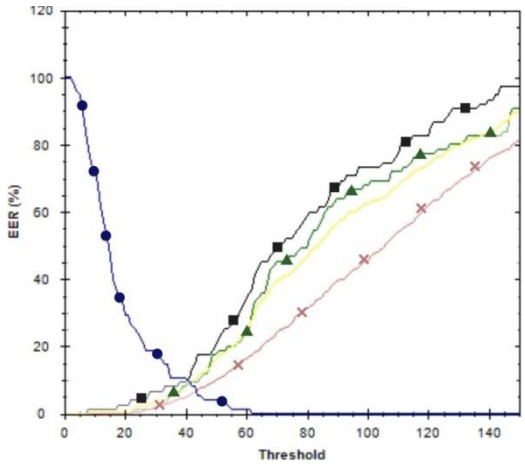

Figure 7. Graph 15 participants database number 2

3. Test with 15 participants database number 3

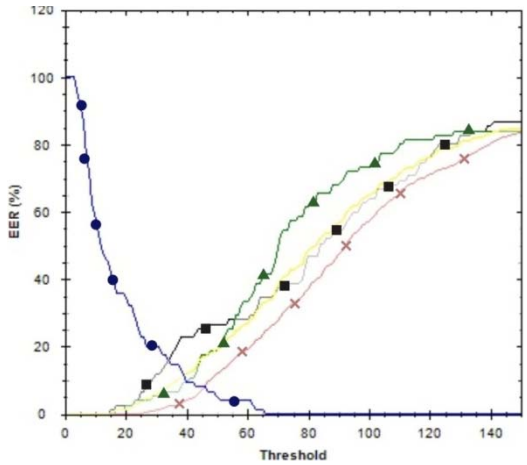

Figure 8. Graph 15 participants database number 3

This test obtained that system accuracy without imposters is 86,66667% at threshold 40 with rejection errors (FNMR) is 9,333333% and acceptance errors (FMR) is 4%, when with

imposters system accuracy is 73,65079% at threshold 26 with error rejection (FNMR) is 22,66667% and acceptance errors (average FMR) is 3,68254%, with details as follows: acceptance errors is 0,380952%, acceptance errors simple imposters is 4% and acceptance errors trained imposters is 6,666667%.

4. Test with 25 participants database number 1

This test obtained that system accuracy without imposters is 91% at threshold 37 with rejection errors (FNMR) is 7,2% and acceptance errors (FMR) is 1,8%, when with imposters system accuracy is 81,74444% at threshold 27 with error rejection (FNMR) is 14,4% and acceptance errors (average FMR) is 3,855556%, with details as follows: acceptance errors is 0,36667%, acceptance errors simple imposters is 3,2% and acceptance errors trained imposters is 8%.

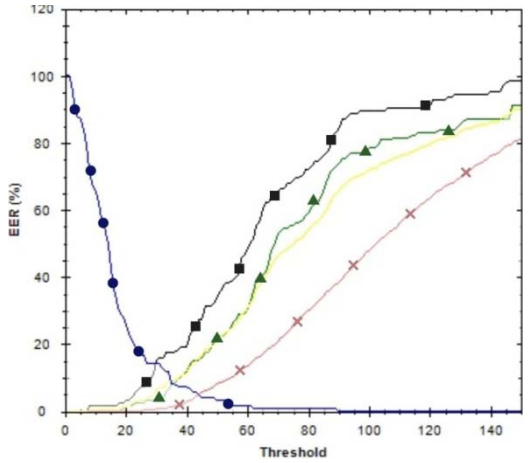

Figure 9. Graph 25 participants database number 1

5. Testwith 25 participants database number 2

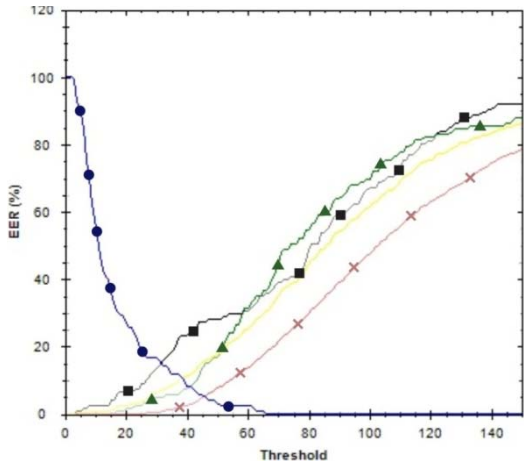

Figure 10. Graph 25 participants database number 2

This test obtained that system accuracy without imposters is 90,1% at threshold 44 with rejection errors (FNMR) is 5,6% and acceptance errors (FMR) is 4,3%, when with imposters

system accuracy is 77,54444% at threshold 26 with error rejection (FNMR) is 18,4% and acceptance errors (average FMR) is 4,055556%, with details as follows: acceptance errors is 0,166667%, acceptance errors simple imposters is 3,2% and acceptance errors trained imposters is 8,8%.

6. Test with 50 participants

This test obtained that system accuracy without imposters is 90,44897959% at threshold 44 with rejection errors (FNMR) is 5,2% and acceptance errors (FMR) is 4,35102%, when with imposters system accuracy is 80,1361% at threshold 27 with error rejection (FNMR) is 15,6% and acceptance errors (average FMR) is 4,263946%, with details as follows: acceptance errors is 0,391837%, acceptance errors simple imposters is 3,2% and acceptance errors trained imposters is 9,2%.

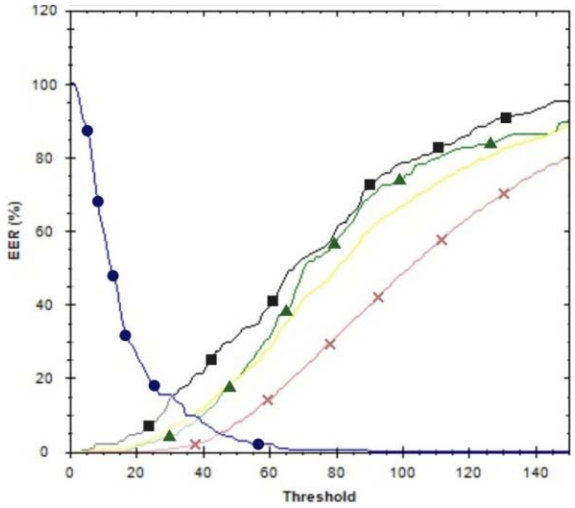

Figure 11. Graph 50 participants

3.3 Stability Test

This stability test can be presented with a chart as shows in Figure 12.

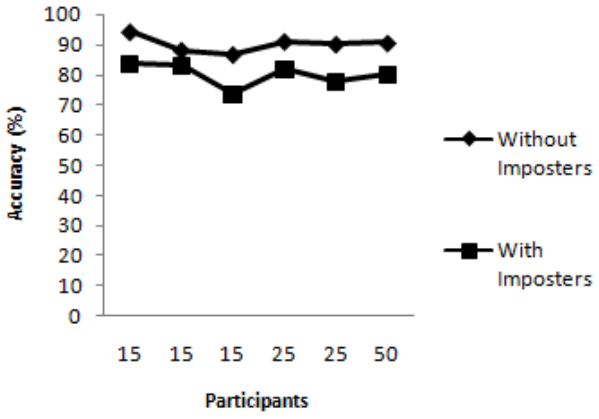

Figure 12. Graph Stability level

Based on Figure 12, the system is stable enough, its mean that system is not affected by size database or number of participants.

4. Conclusion

Based on the test results, biometric signature verification system has high performance. The accuracy of system increases along with the number of references in the database. The system is stable, its mean the system is not affected by size database or number of participants.

The final result system was tested with 50 participants with 3 references. This test obtained that system accuracy without imposters is 90,44897959% at threshold 44 with rejection errors (FNMR) is 5,2% and acceptance errors (FMR) is 4,35102%, when with imposters system accuracy is 80,1361% at threshold 27 with error rejection (FNMR) is 15,6% and acceptance errors (average FMR) is 4,263946%, with details as follows: acceptance errors is 0,391837%, acceptance errors simple imposters is 3,2% and acceptance errors trained imposters is 9,2%.

The verification system is very feasible to developed and applied towards mobile systems for specific application fields, such as attendance systems applications.

References

[1] Riha Z, Vaclav M. Biometric Authentication System. FI MU Report Series. 2000.
[2] Plamondon R, Srihari N. On-line and Off-line handwriting recognition: a comprehensive survey. *IEEE Transactions on Pattern Analysis Machine Intelligence*. 2000; 22(1): 63-84.
[3] Anil J, Freidereke D G, Connell S D. On-line Signature Verification. Department of Computer Science and Engineering. Michigan State University.
[4] Christian G. Signature Verification with Dynamic RBF Network and Time Series Motifs. University of Passau Germany.
[5] Fangjun L, Shiliang M, Kaidong C, Xianfeng X. On-Line Handwritten Signature Verification Algorithm Based On Time Sequence. Institute for Scientific Computing and Information. 2005.
[6] Gruber C, Gruber T, Sick B. Online Signature Verification with New Time Series Kernels for Support Vector Machines. *Proceeding of ICB*. Hongkong. 2006; 3832: 500–508.
[7] Milton H, Fernando O. Handwritten Signature Authentication using Artificial Neural Networks.
[8] Uthansakul, Peerapong, Uthansakul. Online Signature Verification Using Angular Transformation for e-Commerce Services. Word Academy of Science, Engineering and Technology, 2010.
[9] Jayadevan R, Satish R K, Pradeep M P. Dynamic Time Warping Based Static Hand Printed Signature Verification. *Journal of Pattern Recognition Research*, 2009; pp. 52-65.
[10] Hansheng L, Srinivas P, Venu G. Mouse Based Signature Verification for Secure Internet Transactions. State University of New York USA.
[11] Kai H, Hong Y. On-Line Signature Verification Based on Stroke Matching. Electrical and Information Engineering University of Sydney Australia. 2006.
[12] Alan M, Trevathan J, Read W, "Neural Network-based Handwritten Signature Verification", School of Mathematics, Physics and Information Technology, James Cook University Australia, 2008.
[13] Payman M and Amirhassan M S. Dynamic Online Signatures Recognition System Using a Novel Signature-Based Normalized Features String and MLP Neural Network. 2007.
[14] Mailah M, Boon L. Biometric Signature Verification Using Pen Position, Time, Velocity and Pressure Parameters. University Technology. Malaysia. 2008.
[15] Pranav P, Keogh E, Lin J, Lonardi S. Mining Motifs in Massive Time Series Databases. *Proceeding of the ICDM*. 2002; 2: 370–377.
[16] Li W, Eamonn K. Semi-Supervised Time Series Classification. University of California.
[17] Pratikakis Z K, Comelis I J, Nyssen E. Using Landmarks to Establish a Point-to-Point Correspondence between Signatures. Vrije University Brussel Belgium. 2000.
[18] Zhifeng Y, Futai Z, Wenjie Y. Cryptanalysis to a Certificateless Threshold Signature Scheme. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(6): 1496-1502.
[19] Lizhen M. More Efficient VLR Group Signature Based on DTDH Assumption. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(6): 1470-1476.
[20] Dongqing Z, Yubing H, Xueyu T. Nonlinier/Non-Gaussian Time Series Prediction Based on RBF-HMM-GMM Model. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(6): 1214-1226.