International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.57-70
http://dx.doi.org/10.14257/ijsia.2014.8.1.06

An Improved Dominant Point Feature for Online Signature Verification

Darma Putra[1], Yogi Pratama[2], Oka Sudana[3] and Adi Purnawan[4]

[1,2.3.4]Department of Information Technology, Udayana University, Indonesia
[1]ikgdarmaputra@gmail.com, [2]yogipratama.ib@gmail.com,
[3]agungokas@unud.ac.id, [4]dosenadi@yahoo.com

Abstract

Among the biometric characteristic, signature forgery is the easiest way to do. Possibility of signature forgery similarity might be reached perfectly. This paper introduced a new technique to improve dominant point feature system based on its location for online signature verification. Dynamic Time Warping is used to match two signature features vector. The performance of system is tested by using 50 participants. Based on simulation result, system accuracy without presence of the simple and trained impostors is 99.65% with rejection error is 0% and acceptance error is 0.35%. While the current systems are faced with the simple and trained impostors, system accuracy became 91.04% with rejection error is 1.6% and an average of acceptance error is 7.36% with details as follows; acceptance error is 0.08%, acceptance error of simple impostors is 4.4%, and acceptance error of trained impostors is 17.6%.The improved feature within fusion is produce better accuracy significantly than dominant point feature. Accuracy of the improved feature within fusion is 91.04%, whereas system accuracy with just use the dominant point feature is 70.96%.

Keywords: *Verification, Dominant Point, Biometric, Signature, Location of Dominant Points*

1. Introduction

Research and development of the biometric verification of human beings especially the signatures has been widely applied. Several kinds of methods have been used to minimize the level of signature forgery because signature is the easiest to forge when it compares to the other biometric characteristics [1]. Possibility of signatures similarity might be reached perfectly. Few people realize that the possibility of the direction of motion of the signature is different for each person. It becomes the uniqueness of the signature itself, then for reasons such as to minimize the possibility that the signature to be forged [2].

Several methods have been applied to the biometrics(especially signatures) as identification or distinguishing between people with each other, they are dominant point [3], stroke matching [4], based on writing speed [5], angle detection [6, 7], support vector machine [8], mouse based signatures [9], time sequence[10], localized arc pattern [11],dynamic RBF networks and time series motifs [12],4 features (pen position, time, velocity, and pressure parameters) [13], local dominant orientation [14], etc.

Several studies have used dominant point as a research object or as an object feature extraction such as planar curves [15], digital curve [16], handwritten of some script [17, 19], and also signature detection. Recognition rate of the previous study that used dominant point as method for signature feature extraction in signature recognition is about 96% with 20

ISSN: 1738-9976 IJSIA

respondents [3], and the average recognition rate of several handwritten recognition systems using dominant point is above 90%.

This paper developed an online signature verification system using multi-matcher between dominant point feature that is motion direction based on chain code and the improved feature namely location of dominant points. The location of dominant points is obtained from coordinate values of dominant point that simplified using media division of the signature.

2. Research Method

Overview of the verification process in this paper could be seen in Figure1.

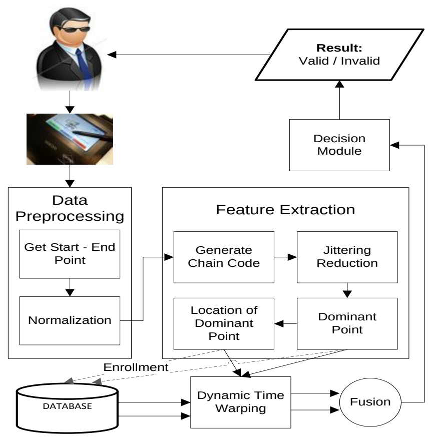


Figure 1. System Overview Diagram

2.1. Data Acquisition

Signature data is obtained using signature pad (Topaz Signature GemLCD1x5 USB). Each person was asked to write their signature on the signature pad, each person inserting 8signatures (3 of them are use as references and the other 5 are use as testers). Figure 2 shows the signature pad that used in this paper.

Figure 2. Topaz SignatureGem LCD 1x5 USB

2.2. Signature Normalization

Normalization is a process to transform data in to the form of normal data in desired range. Normalization of signature scale is indispensable in signature verification system because the data signatures of the same user would not always be the same at each time (in this case is the signature scale), so with this normalization process, users can write their signature with different scale [1]. Process of normalization is shown by equation (1) and (2).

$$x_i = \frac{x_i^0 - x_{min}}{x_{max} - x_{min}} \qquad (1)$$

$$x_i = \frac{y_i^0 - y_{min}}{y_{max} - y_{min}} \qquad (2)$$

where (x_i, y_i) , (x_i^0, y_i^0) , (x_{min}, y_{min}) , (x_{max}, y_{max}) , W , H represent new coordinates pixel , old coordinates pixel, minimum coordinates, maximum coordinates, desired image width, and desired image height respectively.

Normalization process in this paper will change the signature size 250x250 pixels by moving each coordinate point (x, y) on the existing media in to a new pixel 250x250pixels sized according to the original size ratio signature pixel input on the new media. Normalization result of a signature sample is shown in Figure3.

a

b

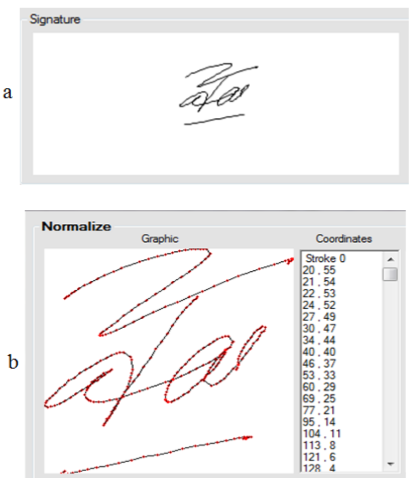


Figure 3. Signature (a) Before and (b) After Normalization Process

2.3. Feature Extraction

Features extraction is a module which is used to obtain the characteristics of a biometric. In this paper, feature extraction has four steps; Generate Chain Code, Jittering Reduction, Dominant Points Extraction, Dominant Points Location Determination.

2.3.1. Generate Chain Code: Generate chain code is a process to determine the motion direction of a signature based on chain code. Figure 4showsthe distribution of motion direction based on chain code [15, 21].

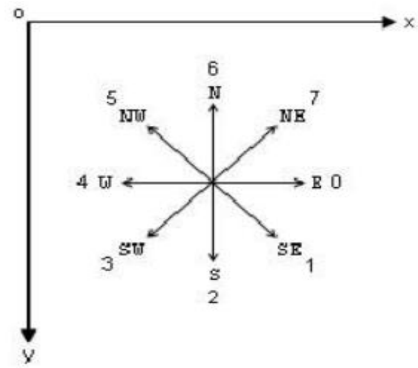


Figure 4. Distribution of Motion Direction

Angle from current point (x_1, y_1) to next point (x_2, y_2) can be calculated by equation (3).

$$\theta = tan^{-1}\left(\frac{y_2 - y_1}{x_2 - x_1}\right) \qquad (3)$$

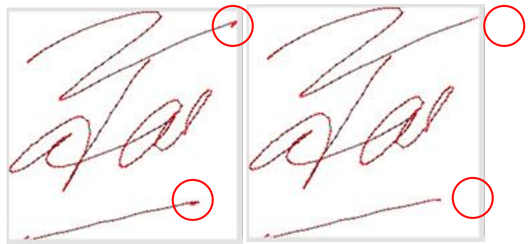
The angle will be converted into chain code. Angle to the chain code conversion in this paper is shown in Table1.

Table 1. Angle to Chain Code Conversion

If	Chain Code
θ> 337.5 or θ≤ 22.5	0
22.6 ≤ θ≤ 67.5	1
67.6≤ θ< 112.5	2
112.6 ≤ θ≤ 157.5	3
157.6≤ θ≤ 202.5	4
202.6 ≤ θ≤ 247.5	5
247.6≤ θ≤ 292.5	6
292.6 ≤ θ≤ 337.5	7

2.3.2. Jittering Reduction: Jittering reduction is used to ignore the chain code length less than or equal to the specified constant [3], so the signature looks more smooth and the results of feature extraction become more accurate.

Jittering reduction with constant = 2 required in this paper to adjust the tool that used to input the signature (signature pad Topaz Signature Gem LCD 1 x 5 USB) had a high accuracy in getting the points on each stroke. Figure 5shows the difference of signature without and with jittering reduction.



a b

Figure 5.Signature (a) Without and (b) with Jittering Reduction Process

Red dots mark in Figure 5(a, b) shows the different parts of the signature without and with jittering reduction. Chain code with length less than or equal to 2 is considered as noise on the input process.

2.3.3. Dominant Points Extraction: Dominant point extraction process is used to obtain the coordinates which are regarded as an important coordinate on every stroke. Dominant point is a collection of point coordinates that is the starting point, end point, local extreme, and the midpoint.

Start and end coordinates of the stroke could be found by accessing the array at start and end index of each stroke [3], but for local extrema can't be detected with extrema equation because signature is an abstract curve which is not be made based on any equation [20].

Local extrema in signatures obtained through detection of chain code that performed vertically and horizontally with the addition of local extrema detection conditions to obtain the midpoint value [3]. In this paper, local extrema and the midpoint obtained through the change of motion direction or the change of chain code values. For example, there is a signature with its coordinates as follows:

{P_1(25, 25), P_2(26, 24), P_3(27, 23), P_4(28, 22), P_5(29, 21), P_6(30, 20), P_7(31, 19), P_8(32, 18), P_9(32, 17), P_{10}(32, 16), P_{11}(32, 15), P_{12}(32, 14), P_{13}(32, 13), P_{14}(32, 12), P_{15}(32, 11), P_{16}(32, 10), P_{17}(31, 11), P_{18}(30, 12), P_{19}(29, 13), P_{20}(28, 14), P_{21}(27, 15), P_{22}(26, 16), P_{23}(25, 17), P_{24}(24, 16), P_{25}(23, 15), P_{26}(22, 14), P_{27}(21, 13)}

The conversion of these points into the chain code is as follows:

77777776666666633333335555

The dominant point can be obtained by taking the coordinates which is just before the change of motion direction is occurs.

7777777666666663333333555**5** = **7 6 3 5**
{P_1, P_8,P_{16}, P_{23}, P_{27}} → Dominant Points

2.3.4. Dominant Points Location Determination: This is the proposed technique in this paper. Location of dominant points method developed based on dominant point. Coordinate of each dominant point will be placed on the media that has been divided into several parts, and then the value of each coordinate will be simplified based on media division. Figure 6 shows the illustration of location of dominant point process.

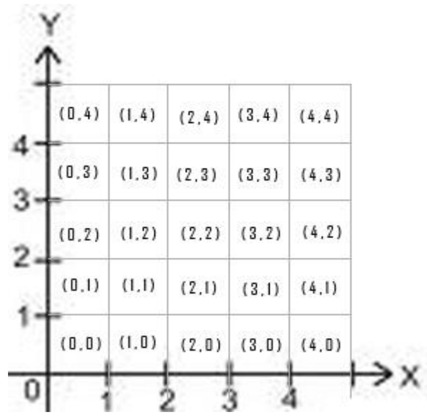


Figure 6. Illustration of Location of Dominant Point Process

Location of dominant point process only could be extracted after get a feature of dominant points. In this paper, the simplification is done in 250 x 250 pixels with 10x10 sections of media division. Table 2 shows the simplification of the coordinate values on location of dominant point process.

Table 2. Simplification of the Coordinate Values

If	Value
$0 \leq (x \text{ or } y) \leq 25$	0
$25 < (x \text{ or } y) \leq 50$	1
$50 < (x \text{ or } y) \leq 75$	2
$75 < (x \text{ or } y) \leq 100$	3
$100 < (x \text{ or } y) \leq 125$	4
$125 < (x \text{ or } y) \leq 150$	5
$150 < (x \text{ or } y) \leq 175$	6
$175 < (x \text{ or } y) \leq 200$	7
$200 < (x \text{ or } y) \leq 225$	8
$225 < (x \text{ or } y) \leq 250$	9

For example, there is a signature with its coordinates of dominant points as follows:

$$\{P_1(20,55), P_2(95,9), P_3(162,0), P_4(55,96), P_5(61,95), P_6(241,13), P_7(250,11), P_8(244,16)\}$$

The location of dominant points above is converted as follows:

$$\{P_1(0,2), P_2(3,0), P_3(6,0), P_4(2,3), P_5(2,3), P_6(9,0), P_7(9,0), P_8(9,0)\}$$

2.3.5. Signature Feature Fusion: The type of multi modal biometric in this paper uses the combination of 2 features of the same biometric (multi matchers) and fusion on level score.

Multi matchers means the system uses two different algorithms in the feature extraction or matching process at the same biometric. Fusion at level score means the system combines the scores which are produced by these two features (dominant point and location of dominant point) after the matching process [1]. Figure 7 shows the scheme of fusion signature feature fusion.

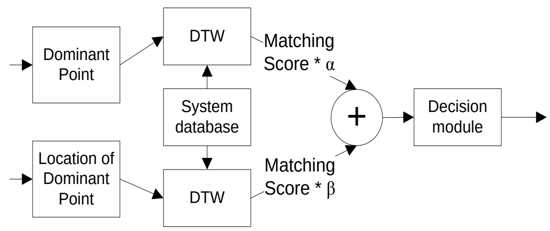


Figure 7. Scheme of Signature Feature Fusion

Each matching scores will be multiplied by α and β (according to Figure 7) where α + β = 1, and then the multiplied matching scores will be summed to obtain the fusion score.

2.3.6. Matching: Dynamic Time Warping (DTW) matching method is used because the length of two signature feature vectors tends to be different. The DTW calculation technique can be seen in [21].

3. Result and Analysis

The performance of this system is tested by using 50 data participants, each participant entering 8 data of their signatures, 3 of them as references and the other 5 as testers. This test is also uses 10 data impostors signature as testers, 5 for simple impostors and 5 for trained impostors. Simple impostors are the people who forged the others signature with just one look at that signature, and the trained impostors is a person who forged the other signature with some practice process .Each of testing phase will be faced with two different database types: database without simple and trained impostors and database with simple and trained impostors. Accuracy of the system could be calculated by equation (4):

$$Accuracy = 100 - (FNMR + FMR) \quad (4)$$

where FNMR, FMR represents false non-match rate and false match rate.

3.1. Determining Fusion Weight

This test is needed to obtain the best fusion weight (α, β) of the two methods that used in this system. These weights will be used in the next tests [1]. This testing uses database size in 50 participants with 3 references for each participant. Tables 3 and 4 shows the result of the testing.

Average FMR in Table 4 is computed from the average of False Match Rate, False Match Rate with simple impostors, and False Match Rate with trained impostors.

Row number 11 (α=1, β=0) from Table 3 and 4 means the system only uses dominant point feature. The receiver of operating curve with only uses dominant point is shown in Figure 8

Table 3. α , β Testing without Simple and Trained Impostors

No	α	β	T	FNMR (%)	FMR (%)	Accuracy (%)
1	0	1	64	0.4	0.92	98.68
2	0.1	0.9	64.5	0.4	0.69	98.91
3	0.2	0.8	63.7	0	0.63	99.37
4	0.3	0.7	65.1	0	0.35	99.65
5	0.4	0.6	64.4	0	0.38	99.62
6	0.5	0.5	63.6	0	0.40	99.60
7	0.6	0.4	62.7	0	0.57	99.43
8	0.7	0.3	60.1	0	1.39	98.61
9	0.8	0.2	60.7	1.2	2.05	96.75
10	0.9	0.1	62.5	3.2	2.84	93.96
11	1	0	64.6	5.6	6.05	88.35

Table 4. α , β Testing with Simple and Trained Impostors

No	A	B	T	FNMR (%)	Average FMR (%)	Accuracy (%)
1	0	1	67.2	2.4	10.31	87.29
2	0.1	0.9	68.5	2.4	9.03	88.57
3	0.2	0.8	68.3	1.2	8.45	90.35
4	0.3	0.7	69.4	1.6	7.36	91.04
5	0.4	0.6	67.9	1.2	8.30	90.50
6	0.5	0.5	68.9	2.8	7.49	89.71
7	0.6	0.4	67.6	3.2	9.10	87.70
8	0.7	0.3	67.7	5.2	9.24	85.56
9	0.8	0.2	67	5.6	12.25	82.15
10	0.9	0.1	66.1	5.6	15.73	78.67
11	1	0	65.4	7.6	21.44	70.96

This test obtained that system accuracy without presence of the simple and trained impostors is 88.35% with FNMR is 5.6% and FMR is 6.05% at threshold (T) = 64.6. While the systems are faced with the simple and trained impostors, the system accuracy became 70.96% 4 with FNMR is 7.6% and an average of Average FMR is 21.44% at the threshold (T) = 65.4 with details as follows: FMR is 5.12%, FMR with simple impostors is 24.4%, and FMR with trained impostors (FMR TI) is 34.6%.

Row number 1 (α=0,β=1) from Table 3 and 4 shows the system only uses the location of dominant point method. The receiver of operating curve with only uses the location of dominant point is shown in Figure 9.

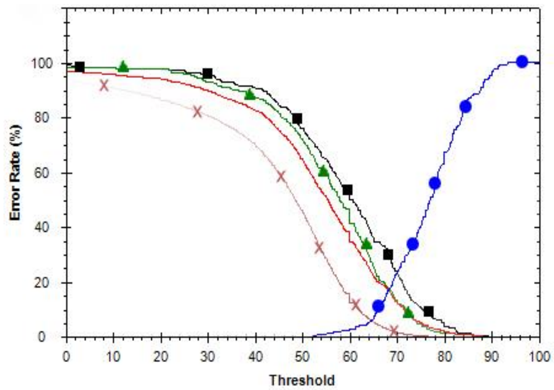


Figure 8. The Receiver Operating Curve with α=1, β=0. Sign Dot, Cross, Triangle, and Rectangle Represents FNMR, FMR, FMR with Simple Impostors, FMR with Trained Impostors Respectively, and the Line without Mark Represents Average FMR

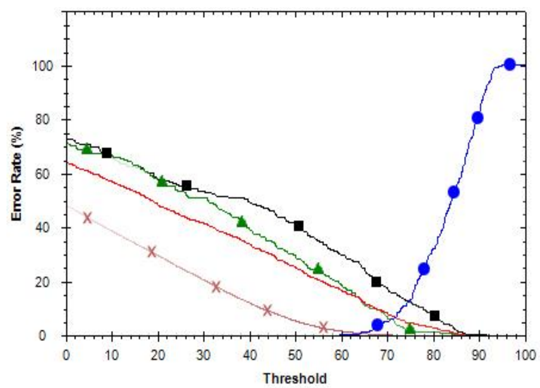


Figure 9. The Receiver Operating Curve with α=0, β=1. Sign Dot, Cross, Triangle, and Rectangle Represents FNMR, FMR, FMR with Simple Impostors, FMR with Trained Impostors Respectively, and the Line without Mark Represents Average FMR

This test obtained that system accuracy without presence of the simple and trained impostors is 98.68% at T 64with FNMR is 0.4%and FMR is 0.92%.While the systems are faced with the simple and trained impostors, system's accuracy became 87.29% with FNMR is 2.4% and Average FMR is 10.31% at T = 67.2 with details as follows: FMR is 0.53%, FMR with simple impostors is 10%, and FMR with trained impostors is 20.4%.

The other rows in the tables show the fusion of dominant point and location of dominant point feature performance. The best fusion occurs on row number 4 with α=0.3 and β=0.7 where the system accuracy without presence of the simple and trained impostors is 99.65% with FNMR is 0% and FMR is 0.35% at T = 65.1.While the systems are faced with the simple and trained impostors, system's accuracy became 91.04% with FNMR is 1.6% and Average FMR is7.36% at T = 69.4with details as follows: FMR is 0.08%, FMR SI is 4.4%, and FMR TI is 17.6%. The receiver of operating curve of fusion scheme is shown in Figure 10.

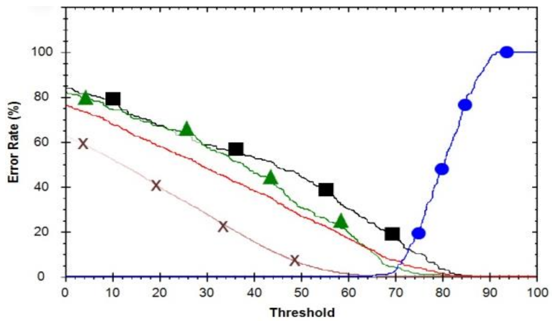


Figure 10. The Receiver Operating Curve with α=0.3, β=0.7. Sign Dot, Cross, Triangle, and Rectangle Represents FNMR, FMR, FMR with Simple Impostors, FMR with Trained Impostors Respectively, and the Line without Mark Represents Average FMR

The experiment results show that the proposed feature in this paper produce better accuracy significantly than the dominant point feature. Finally, the best accuracy is obtained by combine those two feature with $\alpha = 0.3$ and $\beta = 0.7$.

3.2. Number of Reference Test

This test is used to analyze accuracy of the system against the number of references that used in this system. Database size that used in this test is 50 participants with fusion weight $\alpha = 0.3$ and $\beta = 0.7$. Table 5 and 6 shows the result of this test.

Table 5. Number of Reference Test without Simple and Trained Impostors

Number of Reference(s)	T	FNMR (%)	FMR (%)	Accuracy (%)
1	51.3	2	3.49	94.51
2	59.1	1.2	1.15	97.65
3	65.1	0	0.35	99.65

Table 6. Number of Reference Test with Simple and Trained Impostors

Number of Reference(s)	T	FNMR (%)	Average FMR (%)	Accuracy (%)
1	54.5	4.4	18.44	77.16
2	60.7	2.4	14.27	83.33
3	69.4	1.6	7.36	91.04

Table 5 and table 6 show that the system accuracy increases along with the number of references in the database.

4. Conclusion

The proposed method in this paper has successfully improves the dominant point feature. This method can increase the performance of the online signature verification system significantly whether without and with simple and trained impostors. In the testing with simple and trained impostors, the system can increase the accuracy more than 17 %, while without simple and trained impostors can increase the accuracy more than 10 %. The online signature verification system in this paper is very feasible to be developed and applied for authentication applications. For future work, we would develop mobile signature authentication system

References

[1] D. Putra, "Biometric System", Yogyakarta: ANDI Offset, Indonesia, **(2009)**.
[2] Z. Riha and V. Matyas, "Biometric Authectication Systems", FI MU Report Series, **(2000)**.
[3] F. Soedjianto, K. Lukas Dwi and R. Adipranata, "Signature Recognition with Dominant Point Method", Petra Christian University Siwalankerto, Indonesia, **(2006)**, pp. 121-131.
[4] H. Kai and Y. Hong, "On-Line Signature Verification Based on Stroke Matching", Electrical and Information Engineering University of Sydney, Australia, **(2006)**.
[5] J. Anil, D. G. Friederike and S. D. Connell, "On-line Signature Verification", Department of Computer Science and Engineering, Michigan State University.
[6] A. Rosenfeld and E. Johnston, "Angle Detection on Digital Curves", IEEE Trans. Comput., vol. C-22, **(1973)** September, pp. 509-522.
[7] A. Rosenfeld and J. S. Weszka, "An Improved Method of Angle Detection on Digital Curves", IEEE Trans.Comput., vol. C-24, **(1975)** September, pp. 940-941.
[8] C. Gruber, T. Gruber and B. Sick, "Online Signature Verification with New Time Series Kernels for Support Vector Machines", LNCS, vol. 3832. Springer, **(2006)**, pp. 500-508.
[9] L. Hansheng, P. Srinivas and G. Venu, "Mouse Based Signature Verification for Secure Internet Transactions", State University of New York at Buffalo USA.
[10] L. Fangjun, M. Shiliang, C. Kaidong and X. Xianfeng, "On-Line Handwritten Signature Verification Algorithm Based On Time Sequence", Institute for Scientific Computing And Information, **(2005)**.
[11] A. A. K. Oka Sudana, "Signature Image Verification System with Localized Arc Pattern Method", Faculty of Engineering, Udayana University, Bali, Indonesia, **(2000)**.
[12] G. Christian, "Signature Verification with Dynamic RBF Network and Time Series Motifs", University of Passau, Germany.
[13] M. Mailah and L. Boon, "Biometric Signature Verification Using Pen Position, Time, Velocity And Pressure Parameters", UniversitiTeknologi Malaysia, **(2008)**.
[14] J. Choi, W. Kim, H. Kong and C. Kim, "Real-Time Vanishing Point Detection Using The Local Dominant Orientation Signature", 3DTV Conference: The True Vision - Capture, Transmission and Display of 3D Video (3DTV-CON), **(2011)**, pp. 1-4.
[15] C. Di Ruberto and A. Morgera, "A New Iterative Approach for Dominant Point Extraction in Planar Curves", WSEAS Transactions on Computers, vol. 8, no. 3, **(2009)** March, pp. 482-493.
[16] C. H. The and R. T. Chin, "On the Detection of Dominant Points on Digital Curves", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 11, no. 8, (1989) August, pp. 859-872.
[17] Y. Su and D. Guozhong, "Detecting Dominant Points on On-line Scripts with a simple Approach", Proceedings of the Eighth International Workshop on Frontiers in Handwriting Recognition (IWFHR'02) IEEE, pp. 351-356.
[18] X. Li, and D.-Y. Yeung, "On-Line Handwritten Alphanumeric Character Recognition Using Dominant Point In Stroke", DBLP Pattern Recognition, vol. 30, no. 1, **(1997)** January, pp. 31-44.
[19] P. Tewari, "Use of Dominant Point Detection Feature for Recognition of Online Handwritten Devanagari Script", Thesis in Computer Science and Engineering Department, Thapar University, Patiala, **(2012)** June.
[20] H. W. H. Leung, "Feature Extraction, Matching and Relevance Feedback for Sketch Retrieval", Carnegie Mellon University, Electrical and Computer Engineering, **(2003)** June.
[21] I. Ketut Gede Darma Putra and M. Ari Sentosa, "Hand Geometry Verification Based-on Chain Code and Dynamic Time Warping", International Journal of Computer Application, vol. 38, no. 12, **(2012)**, pp. 17-22.

Authors

I Ketut Gede Darma Putra, is a lecturer in Department of Electrical Engineering and Information Technology, Udayana University Bali, Indonesia. He received his S.Kom degree in Informatics Engineering from Institute of Sepuluh November Technology Surabaya, Indonesia on 1997. His received his Master Degree on Informatics and Computer Engineering from Electrical Engineering Department, Gadjah Mada University, Indonesia on 2000 and achieved his Doctorate Degree on Informatics and Computer Engineering from Electrical Engineering Department, Gadjah Mada University, Indonesia on 2006. His research interests are Biometrics, Image Processing, Data Mining, and Soft computing.

Yogi Pratama, has graduated from Department of Information Technology, Udayana University on 2013. His research interests are Image Processing and Programming.

A. A. Kompiang Oka Sudana, received his S.Kom degree in Informatics Engineering from Institut Teknologi Sepuluh Nopember University in 1997, and his MT. degree in Informatics and Computer System from Gajah Mada University in 2001. He was Technical Manager at PT. INFOS Teknologi Indonesia (Software Developer) during April 2008–Sept. 2008, Information Technology Leader–Human Resources and General Affair Division at PT JAS Catering International Airport Ngurah Rai Bali during April 2003–July 2006, Person in Charge of Technological and Professional Skills Development Sector Project (TPSDP)–Asian Development Bank (ADB) Loan, Batch II in Electrical Engineering Study Program during 2002-2006, and now he is lecturer at Magisterial Program of Electrical Engineering Department of Udayana University, lecturer at Electrical Engineering Department (major in Computer System and Informatics) of Udayana University, lecturer at Information Technology Department of Udayana University, and member of Development Project Team of Academic Management Information System and Networking Implementation of Udayana University. His research experiences are in Analysis and Design of Information Systems and Biometric Identification and Recognition.

Adi Purnawan, has finished his study in Information Technology on 2006 at Universitas Pembangunan Nasional "Veteran" Yogyakarta and finished his Master Degree on 2008 at Gadjah Mada University Yogyakarta in Eletrical Engineering. His research focus is on Image Processing.