Editor-in-Chief of the IJSIA Journal

Jemal. H. Abawajy,
Deakin University, Australia

Prof. Bharat Bhargava,
Professor in Department of Computer Science at Purdue, USA

General Information of IJSIA

Bibliographic Information

- ISSN: 1738-9976
- Publisher: SERSC

Science & Engineering Research
Support soCiety

Contact Information

Science & Engineering Research
Support soCiety

- Head Office: 20 Virginia Court, Sandy Bay, Tasmania, Australia
- Phone no.: +61-3-9016-9027
- Email: ijsia@sersc.org

Journal Topics

IJSIA aims to facilitate and support research related to security technology and the applications. The topics covered by IJSIA include the following:-

Basic Topics:

- Security technology
- Security products or systems
- Secure installation, generation and operation
- Security assurance
Applications using Security Engineering:

- Access Control
- Ad Hoc & Sensor Network Security
- Applied Cryptography
- Authentication and Non-repudiation
- Cryptographic Protocols
- Denial of Service
- E-Commerce Security
- Identity and Trust Management
- Information Hiding
- Insider Threats and Countermeasures
- Intrusion Detection & Prevention
- Network & Wireless Security
- Peer-to-Peer Security
- Privacy and Anonymity
- Security Analysis Methodologies
- Security in Software Outsourcing
- Systems and Data Security
- Ubiquitous Computing Security

Advisory/Editorial Board

- Ahmet Koltuksuz, Izmir Institute of Technology, Turkey
- Ajith Abraham, Norwegian University of Science and Technology, Norway
- Alessandro Piva, University of Florence, Italy
- Audun Josang, School of Software Engineering and Data Communications, Australia
- Beniamino Di Martino, Second University of Naples, Italy
- Binyang Zhou, Australian Catholic University, Australia
• Brian King, Indiana University Purdue University Indianapolis, USA
• Chin-Tser Huang, University of South Carolina, USA
• D P. Vakharia, S.V.N.I.T, India
• Damien Sauveron, XLIM Laboratory, France
• Debnath Bhattacharyya, Heritage Inst. of Technology, India
• Dharma P. Agrawal, University of Cincinnati, USA
• Dong Young Lee, Myoungji University, Korea
• Edgar Weippl, Vienna University of Technology, Austria
• Enrico Zio, Polytechnic of Milan, Italy
• Frank Piessens, Katholieke Universiteit Leuven, Belgium
• George Mohay, Queensland University of Technology, Australia
• Geyong Min, University of Bradford, UK
• Gildas Avoine, Massachusetts Institute of Technology, USA
• Giovanni Cagalaban, Hannam University, Korea
• Golden G. Richard III, University of New Orleans, USA
• Hai Jin, Huazhong University of Science and Technology, China
• Hua Liu, Xerox labs, USA
• Indrajit Ray, Colorado State University, USA
• Javier Garcia-Villalba, Complutense University of Madrid, Spain
• Javier Lopez, University of Malaga, Spain
• Jayaprakash Kar, Al Musanna College of Technology, Sultanate of Oman
• Jean-Jacques Quisquater, Universite catholique de Louvain, Belgium
• Jeng-Shyang Pan, National Kaohsiung University of Applied Sciences, Taiwan
• Jeno Bartalos, ICST, Europe
• Jianhua Ma, Hosei University, Japan
• Johnson Thomas, Oklahoma State University, USA
• Jordi Castell, University of Wisconsin, USA
• Jordi Forn, Technical University of Catalonia, Spain
• Jun Bi, Tsinghua University, China
• Kamaljit I. Lakhtaria, Atmiya Institute of Technology & Science, India
• Kamaljit I. Lakhtaria, Atmiya Institute of Technology and Science, India
• Karl Goeschka, Vienna University of Technology, Austria
• Katrin Franke, Fraunhofer Institute, Germany
• Kouich Sakurai, Kyushu University, Japan
• Kousalya G, Lealta Media, India
• Kyoungseok Kim, Chungbuk National University, Korea
• Laurence T. Yang, St. Francis Xavier University, Canada
• Maricel Balitanas-Salazar, University of San Agustin, Philippines
• Marjan Kuchaki Rafsanjani, University of Kerman, Iran
• N. Jaisankar, Manonmaniam Sundaranar University, India
• N.Jaisankar, SCS/VIT university, India
• R. Ravi, Kalasalingam University, India
• Randy Tolentino, Hannam University, Korea
• Rosslin John Robles, University of San Agustin, Philippines
• S.U. Hwang, Hongik University, Korea
• SeokSoo Kim, Hannam University, Korea
• Shiguo Lian, France Telecom R&D Beijing, China
• Suhas J Manangi, Microsoft India, India
• Sukumar Senthilkumar, Universiti Sains Malaysia, Malaysia
• Tao Gong, Donghua University, China
• Yang-sun Lee, Seokyung University, Korea
• Yu-Chen Hu, Providence University, Taiwan
• Yuh-Min Tseng, National Changhua University of Education, Taiwan
IJSIA is indexed by:

- EBSCO
- ProQuest
- ULRICH
- DOAJ
- OpenJ-Gate
- SCOPUS
- Cabell
- EI Compendex

Editorial Secretary

- Ronnie D. Caytiles
## Table of Contents

**An Improved Reconstruction methods of Compressive Sensing Data Recovery in Wireless Sensor Networks**

Sai Ji, Liping Huang, Jin Wang, Jian Shen and Jeong-Uk Kim

**Influence of HRM Practices on Privacy Policy Compliance Intention: A Study among Bank Employees in Korea**

Youngkeun Choi and Taejong

**Modeling and Analysis of SMER Constraints Violation in IRBAC 2000 Model Based on Colored Petri Nets**

Meng Liu and Xuan Wang

**Efficient Data Memory Usages of 3GPP Authentication and Key Agreement Protocol**

Minha Park, Yeog Kim and Okyeon Yi

**A TPSAC Model and Its Application to Mechanical Cloud Simulation**

Changyu Liu, Shoubin Dong, Huiling Li, Bin Lu and Alex Hauptmann

**An Improved Dominant Point Feature for Online Signature Verification**

Darma Putra, Yogi Pratama, Oka Sudana and Adi Purnawan

**Development of Object-Oriented Analysis and Design Methodology for Secure Web Applications**

Kyung-Soo Joo and Jung-Woong Woo
Freshness Consideration of Hierarchical Key Agreement Protocol in WSNs  
81

Sung-Woon Lee and Hyunsung Kim

A Novel Approach to Design the Fast Pedestrian Detection for Video Surveillance System  
93

Shuoping Wang, Zhike Han, Li Zhu and Qi Chen

Securing E-Governance Services through Biometrics  
103

Madhavi Gudavalli, Dr. D. Srinivasa Kumar and Dr. S. Viswanadha Raju

113

Chang-Su Moon and Sun-Hyung Kim

A Reliable File Protection System Based on Transparent Encryption  
123

Jun Liu, ShuYu Chen, MingWei Lin and Han Liu

Sensitive Semantics-Aware Personality Cloaking on Road-Network Environment  
133

Min Li, Zhiguang Qin and Cong Wang

Secured Session Key Agreement Protocol for Iris Cryptosystem Using Customized Elliptic Curve Cryptography  
147

Usha. S and Kuppuswami. S
Towards an Efficient and Secure Online Digital Rights Management Scheme in Cloud Computing  

Huang Qinlong, Ma Zhaofeng, Fu Jingyi, Yang Yixian and Niu Xinxin

Security Assessment for Key Management in Mobile Ad Hoc Networks  

Reham Abdellatif Abouhogail

Evading Anti-debugging Techniques with Binary Substitution  

JaeKeun Lee, BooJoong Kang and Eul Gyu Im

Knowledge Based Secure Data Streaming in Virtual Environment  

Anand. R and Dr. S. Saraswathi

A Study of Security Requirement Demand Survey Analysis on Manufacturing Industry  

Hangbae Chang

Fault Diagnosis Research of Submarine Casing Cutting Robot for Abandoned Oil Wellhead  

Xiaojie Tian, Yonghong Liu, Yunwei Zhang, Rongju Lin and Yuanyuan Xi

Study on Accurate Calculating the Risk of the SCADA  

YoungIn You and KyuongHo lee

Android Mobile Application System Call Event Pattern Analysis for Determination of Malicious Attack  

You Joung Ham, Daeyeol Moon, Hyung-Woo Lee, Jae Deok Lim and Jeong Nyeo Kim
A survey of Cyber Attack Detection Strategies 247

Jamal Raiyn

Secure Data Management Scheme using One-Time Trapdoor on Cloud Storage Environment 257

Sun-Ho Lee and Im-Yeong Lee

Performance of Converged Secure Socket Layer and CMVP Cryptographic Modules 273

Okyeon Yi, Seunghwan Yun, Myungseo Park, Nuri Hwang, Taeyean Kwon and Chaewon Yun

Crowdsourcing Fraud Detection Algorithm Based on Ebbinghaus Forgetting Curve 283

Li Peng, Yu Xiao-yang, Liu Yang and Zhang Ting-ting

Risk Prediction of Malicious Code-Infected Websites by Mining Vulnerability Features 291

Taek Lee, Dohoon Kim, Hyunchol Jeong and Hoh Peter In

The Design and Implementation of Collaboration Service Integration Platform Based on Context-Aware Role Based Access Model 295

Shu-Ping Lu, Kuei-Kai Shao, Yu-Nung Chao, Kuo-Shu Luo and Chi-Hua Chen

New Construction of Even-variable Rotation Symmetric Boolean Functions with Optimum Algebraic Immunity 307

Yindong Chen, Hongyan Xiang and Ya-nan Zhang
Dynamic Multi-keyword Top-k Ranked Search over Encrypted Cloud Data  
Xingming Sun, Xinhui Wang, Zhihua Xia, Zhangjie Fu and Tao Li  

A Study on the Optimization Method for the Rule Checker in the Secure Coding  
JaeHyun Kim and YangSun Lee  

Efficient Image Scrambling based on any Chaotic Map  
Cao Guanghui, Hu Kai and Zhou Jun  

Comparison of Secure Development Frameworks for Korean e-Government Systems  
Dongsu Seo  

Network Security Situation Assessment Ecurity Based on the Associated Diffusion Analysis  
Xiangdong Cai, Yuran Wang, Fushuai Zhang and Yangjing yi  

Security Vulnerabilities Tests Generation from SysML and Event-B Models for EMV Cards  
Noura Ouerdi, Mostafa Azizi, M’Hammed Ziane, Abdelmalek Azizi, Jean-louis Lanet and Aymerick Savary  

Lossless Data Hiding Technique using Reversible Function  
Sang-Ho Shin and Jun-Cheol Jeon
Sinkhole Vulnerabilities in Wireless Sensor Networks 401

Junaid Ahsenali Chaudhry, Usman Tariq, Mohammed Arif Amin and Robert G. Rittenhouse

New Construction of Efficient Certificateless Aggregate Signatures 411

He Liu, Sijia Wang, Mangui Liang and Yongqian Chen

How to Formally Model Features of Network Security Protocols 423

Gyesik Lee
An Improved Dominant Point Feature for Online Signature Verification

Darma Putra¹, Yogi Pratama², Oka Sudana³ and Adi Purnawan⁴

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

![Figure 1. System Overview Diagram](image)

2.1. Data Acquisition

Signature data is obtained using signature pad (Topaz Signature GemLCD 1x5 USB). Each person was asked to write their signature on the signature pad, each person inserting 8 signatures (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](image)

2.2. Signature Normalization

Normalization is a process to transform data into 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).
\[ x_{i} = \frac{x_{i}^{0} - x_{\text{min}}}{x_{\text{max}} - x_{\text{min}}} \]  

\[ y_{i} = \frac{y_{i}^{0} - y_{\text{min}}}{y_{\text{max}} - y_{\text{min}}} \]  

where \((x_{i}, y_{i})\), \((x_{i}^{0}, y_{i}^{0})\), \((x_{\text{min}}, y_{\text{min}})\), \((x_{\text{max}}, y_{\text{max}})\), \(W\), \(H\) 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 into a new pixel 250x250 pixels sized according to the original size ratio. Signature pixel input on the new media. Normalization result of a signature sample is shown in Figure 3.

![Figure 3. Signature (a) Before and (b) After Normalization Process](image)

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 4 shows the distribution of motion direction based on chain code [15, 21].

Copyright © 2014 SERSC
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).

\[
\theta = \tan^{-1}\left(\frac{y_2-y_1}{x_2-x_1}\right)
\]  

(3)

The angle will be converted into chain code. Angle to the chain code conversion in this paper is shown in Table 1.

<table>
<thead>
<tr>
<th>Table 1. Angle to Chain Code Conversion</th>
</tr>
</thead>
<tbody>
<tr>
<td>If (\theta)</td>
</tr>
<tr>
<td>(\theta &gt; 337.5) or (\theta \leq 22.5)</td>
</tr>
<tr>
<td>(22.6 \leq \theta \leq 67.5)</td>
</tr>
<tr>
<td>(67.6 \leq \theta &lt; 112.5)</td>
</tr>
<tr>
<td>(112.6 \leq \theta \leq 157.5)</td>
</tr>
<tr>
<td>(157.6 \leq \theta \leq 202.5)</td>
</tr>
<tr>
<td>(202.6 \leq \theta \leq 247.5)</td>
</tr>
<tr>
<td>(247.6 \leq \theta \leq 292.5)</td>
</tr>
<tr>
<td>(292.6 \leq \theta \leq 337.5)</td>
</tr>
</tbody>
</table>

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 5 shows the difference of signature without and with jittering reduction.
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:

777777666666663333335555

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

777777666666663333335555 = 7 6 3 5
\{P_1, P_8, P_{16}, P_{23}, P_{27}\} \rightarrow \text{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

<table>
<thead>
<tr>
<th>If</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 ≤ (x or y) ≤ 25</td>
<td>0</td>
</tr>
<tr>
<td>25 &lt; (x or y) ≤ 50</td>
<td>1</td>
</tr>
<tr>
<td>50 &lt; (x or y) ≤ 75</td>
<td>2</td>
</tr>
<tr>
<td>75 &lt; (x or y) ≤ 100</td>
<td>3</td>
</tr>
<tr>
<td>100 &lt; (x or y) ≤ 125</td>
<td>4</td>
</tr>
<tr>
<td>125 &lt; (x or y) ≤ 150</td>
<td>5</td>
</tr>
<tr>
<td>150 &lt; (x or y) ≤ 175</td>
<td>6</td>
</tr>
<tr>
<td>175 &lt; (x or y) ≤ 200</td>
<td>7</td>
</tr>
<tr>
<td>200 &lt; (x or y) ≤ 225</td>
<td>8</td>
</tr>
<tr>
<td>225 &lt; (x or y) ≤ 250</td>
<td>9</td>
</tr>
</tbody>
</table>

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](image)

Each matching scores will be multiplied by $\alpha$ and $\beta$ (according to Figure 7) where $\alpha + \beta = 1$, 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):

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

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 ($\alpha$, $\beta$) 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 ($\alpha=1, \beta=0$) 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. \(\alpha, \beta\) Testing without Simple and Trained Impostors

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

Table 4. \(\alpha, \beta\) Testing with Simple and Trained Impostors

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

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% 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 \((\alpha=0, \beta=1)\) 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.
This test obtained that system accuracy without presence of the simple and trained impostors is 98.68% at $T = 64$ with 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 $\alpha = 0.3$ and $\beta = 0.7$ 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 is 7.36% at $T = 69.4$ with 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 $\alpha=0.3$, $\beta=0.7$. 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

<table>
<thead>
<tr>
<th>Number of Reference(s)</th>
<th>T</th>
<th>FNMR (%)</th>
<th>FMR (%)</th>
<th>Accuracy (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>51.3</td>
<td>2</td>
<td>3.49</td>
<td>94.51</td>
</tr>
<tr>
<td>2</td>
<td>59.1</td>
<td>1.2</td>
<td>1.15</td>
<td>97.65</td>
</tr>
<tr>
<td>3</td>
<td>65.1</td>
<td>0</td>
<td>0.35</td>
<td>99.65</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Number of Reference(s)</th>
<th>T</th>
<th>FNMR (%)</th>
<th>Average FMR (%)</th>
<th>Accuracy (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>54.5</td>
<td>4.4</td>
<td>18.44</td>
<td>77.16</td>
</tr>
<tr>
<td>2</td>
<td>60.7</td>
<td>2.4</td>
<td>14.27</td>
<td>83.33</td>
</tr>
<tr>
<td>3</td>
<td>69.4</td>
<td>1.6</td>
<td>7.36</td>
<td>91.04</td>
</tr>
</tbody>
</table>

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

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 Electrical Engineering. His research focus is on Image Processing.
International Journal of Security and its Applications

Country: South Korea

Subject Area: Computer Science

Subject Category: Computer Science (miscellaneous)

Publisher: Science and Engineering Research Support Society. Publication type: Journals. ISSN: 17389976

Coverage: 2007-2012

H Index: 4

Indicators

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SJR</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
<td>0.010</td>
<td>0.102</td>
<td>0.122</td>
<td>0.139</td>
<td>0.157</td>
</tr>
<tr>
<td>Total Documents</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>18</td>
<td>38</td>
<td>24</td>
<td>20</td>
<td>29</td>
<td>106</td>
<td></td>
</tr>
<tr>
<td>Total Docs. (3years)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>18</td>
<td>56</td>
<td>80</td>
<td>82</td>
<td>73</td>
<td></td>
</tr>
<tr>
<td>Total References</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>267</td>
<td>626</td>
<td>419</td>
<td>392</td>
<td>604</td>
<td>1,222</td>
</tr>
<tr>
<td>Total Cites (3years)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1,222</td>
</tr>
<tr>
<td>Self Cites (3years)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Citable Docs. (3years)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>18</td>
<td>56</td>
<td>80</td>
<td>82</td>
<td>73</td>
</tr>
<tr>
<td>Cites / Doc. (4years)</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.06</td>
<td>0.09</td>
<td>0.09</td>
<td>0.28</td>
<td>0.28</td>
<td>0.52</td>
</tr>
<tr>
<td>Cites / Doc. (3years)</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.06</td>
<td>0.09</td>
<td>0.28</td>
<td>0.32</td>
<td>0.53</td>
</tr>
<tr>
<td>Cites / Doc. (2years)</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.06</td>
<td>0.09</td>
<td>0.27</td>
<td>0.43</td>
<td>0.67</td>
</tr>
<tr>
<td>References / Doc.</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>14.83</td>
<td>16.47</td>
<td>17.46</td>
<td>19.60</td>
<td>20.83</td>
</tr>
<tr>
<td>Cited Docs.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>19</td>
<td>17</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Uncited Docs.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>51</td>
<td>61</td>
<td>65</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td>% International Collaboration</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

How to cite this website?

Follow us:

Twitter

SJR is developed by:

Scimago Lab, Copyright 2007-2014. Data Source: Scopus®