Biometric based Keystroke Dynamics Authentication - A Review

V. Chandrasekar*; Dr. S. Suresh Kumar**

*Department of Computer Science and Engineering,
Vivekanandha College of Technology for Women,
India.

**Department of Computer Science and Engineering,
Vivekanandha College of Technology for Women,
India.

Abstract

Over the past decade the technological achievements have resulted in improved network services. Because of electronic transactions are executed in these days, the security of computer access is relying important. Existing security techniques can be strengthen by behavioral biometrics such as keystroke dynamics which makes use of the typing cadence of an individual effectively and cheaply. There are numerous studies conducted in terms of data extraction, classification methods, experimental protocol and evaluations. The objective of this paper is to provide an insightful survey and comparison on keystroke dynamics biometrics and enhanced a new concept in classification and selection.

Keywords: Biometrics, Keystroke dynamics, statistical methods, pattern recognition, neural network, search heuristics.

1. Introduction

A ubiquitous part of the modern society has been the Computers. To store and process sensitive information, it has become all the more necessary to secure them from intruders since we depend so much on computers. So there is a need for simple, low-cost and unobtrusive device for user authentication and identification in computer based applications. The biometric is classified as physiological and behavioral biometrics. The example of physiological biometric includes finger print, etc., and behavioral biometric includes typing rhythm, etc. Reference [3] had given overview
of some biometric identification techniques (for both biometrics) and also References [108], [2] and [13] given the overview of behavioral biometric. Use of a behavioral biometric which makes use of the typing pattern of an individual can be obtained using existing systems such as standard keyboard, making it an inexpensive and extremely attractive technique. Using standard input device such as keyboard a user can attempts to access information stored on the computer or online. One of the major disadvantages of the biometric is that it is non-intrusive and can be applied covertly to augment existing cyber-security systems. Also Reference [137] had given a brief description of biometrics and its success factors and keystroke dynamics.

The user authentication process is classified as 1) Knowledge-based 2) Token-based 3) Biometric based. A biometric based system can be divided into two categories: authentication and identification. A strong authentication is referred to a combination of two or three of these processes. The process of associating the person with an identity is identification. There are two important error rates used to determine the performance of a biometric authentication system—False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR is used to measure the ability of the system to accept the unauthorized user. FRR is the number of genuine users rejected from using the system. Some researchers report the equal error rate (ERR) what is defined as the value of FAR/FRR. The lower the value of ERR, the better the system is. Reference [87] used Biometric menagerie and given the relation between the physiological and behavioral biometrics using some algorithms and shown the ERR. Therefore, in this paper we have clearly identified the works based on the type of application. Reference [107] stated that non English words are better than English words and used two classifiers.

2. Keystroke Dynamics

Keystroke dynamics is a behavioral biometrics and it aims to identify users based on the typing of the individuals or attributes such as duration of a keystroke or key hold time, latency of keystroke (inter-keystroke times), typing error, force of keystrokes etc. Human-computer interactions play an important role in keystroke dynamics. Reference [101], [16] gives the overview and applications of keystroke dynamics. Static keystroke analysis is performed on typing samples produced using predetermined text for all individuals under observation. Dynamic analysis implies a continuous or periodic monitoring of issued keystrokes. It is performed during the log-in session and continues after the session. The advantages are uniqueness, low implementation and deployment cost, continuous monitoring and authentication, increased password strength and lifespan. The disadvantages are lower accuracy, lower performance. Reference [148] address some research questions which are related to keystroke dynamics and mentioned some threats. Reference [55] based on keystroke sound proposed feature extraction and authentication algorithms and achieved EER of 25%. Also Reference [79] give the case study for keystroke dynamics and Reference [6] states that keystroke dynamics can be also used in internet banking.

3. Data Acquisition

Data acquisition is the preliminary and essential stage of keystroke dynamics research. Publicly available benchmark databases are limited due to the lower maturity compared with other established biometrics. Many researchers chose to generate in-house data set. Reference [110] study the factors involved during the data acquisition.
3.1 Data Size

Data size is collectively agreed that experiments include large number of subjects better signify the scalability of study. This is understandable due to various issues and difficulties encountered in data collection process (to be discussed in the following section). Regrettably most of the subjects performed involve only small number of subjects.

3.2 Data Type

In general, experimental subjects are required to either provide character-based text or purely numerical inputs. The majority of research works are with character-based inputs. The input type can be further subdivided into long or short term. Short term inputs normally consist of username, password while long inputs are usually referred to paragraphs of text enclosing 100 words or more.

3.3 Genuine and Impostor Samples

Data collected will eventually be used for performance evaluation. The most common way of performance measurement is the degree of accuracy of a system’s ability to distinguish genuine and impostor. The user sample data is divided into two subsets. The first subset is used in training while the remaining in testing sample.

4. Feature Selection

Keystroke dynamics biometrics is rich with distinctive feature information that can be used for recognition purposes. Some of the features are listed in Table 1. Among the easiest and common feature harvested by researches is the timing measurement of individuals keystroke inputs. The timing feature includes:

1) **Di-graph:** Timing information of two consecutive keystrokes, known as digraph. Reference [135] proven that digraphs are good for free text keystroke dynamics. It is categorized as dwell time and flight time.
   - Dwell time refers to the amount of time between pressing and releasing a single key (i.e.) how long a key was hold pressing down.
   - Flight time refers to the amount of time pressing and releasing two successive keys and also called as latency.

2) **N-graph:** N-graph refers to the timing measurement between three or more consecutive keystroke events. Reference [138] used clustering “similar” n-graphs algorithm for continuous authentication and achieved FAR of 3.47% and FRR of 0%.

The feature also includes P-P (Press-Press), P-R (Press-Release), R-P (Release-Press), and R-R (Release- Release).

Also Reference [57] use the press time and release time and used Weighted and non-weighted Norm (k) and demonstrated the other features clearly. Reference [26] proposed
continuous monitoring of the users typing pattern which used latency as their feature and Markov chain which models the mean and variance of the delay between two keystrokes.

5. Methodology

Many classification methods have been applied in keystroke dynamics study over the last decades. Keystroke dynamics recognition can be perceived as a pattern recognition problem and most of the popularly and commonly deployed methods can be broadly categorized as statistical, machine learning approaches and other.

5.1 Statistical Approach

The popularity is directly related to the simplicity, ease of implementation and low overhead. Among the common generic statistical measures include mean, median, standard deviation, statistical t-test and k-nearest neighbor. Using linear statistical approaches may not provide good result and lacking during the training state are some of the disadvantages. References [49], [32] used the Euclidean distance. They achieved a false acceptance rate (FAR) of 0% and false reject rate (FRR) of 4%. Recently Reference [5] used absolute distance and achieved the equal error rate of 0.0445%. Reference [112] used the distance measure for feature selection. Reference [63] achieved an error rate of 0.032 using TKI, TKP. Reference [31] used cosine correlation for online examination continuous authentication. Reference [146] used Mahalanobis distance, Manhattan distance and fusion of both distance and classifier as Nearest Neighbor and achieved ERR of 8.7% for fusion of distances. Reference [52] used traditional static authentication mechanism for continuous authentication and provided a secure, reliable, inexpensive and non-intrusive technique. Reference [7] used S.D and gave the alert levels and achieved ERR of 3%. Reference [28] used statistical measure and overview of keys, their experimental results and advantages, disadvantages of keystroke dynamics. Reference [136] used graphical based password keystroke dynamics for touch screen devices and proposed pressure features (mean, S.D) and achieved ERR of 6.9%. Reference [58] used Relative Entropy, Euclidian distance and K-NN classifier and achieved ERR of 77% (Euclidian distance) and 55% (Relative Entropy). Table 2 list some of the statistical approach used in the past decades.

Also References [133], [47] (FRR of 1%) used the statistical measure and Reference [143] used Discrete Wavelet Transform (DWT) and achieved FAR and FRR of 1.95% for feature selection. Reference [117] used dwell time, flight time as feature extraction and performed test statistic on those values. Reference [104] used Gaussian probability density function, Direction Similarity Measure and achieved 6.36% of ERR. Reference [85] used Euclidean, Manhattan distance for banking transaction systems. Reference [84] used distance- to- median and compared anomaly detection algorithm with other algorithm results.

5.2 Machine Learning Approach

The machine learning approach is widely used in the pattern recognition domain. It is a technique to automatically improve algorithms by extracting information from existing data. The core idea is the ability to identify and classify pattern and make correct decision based on data provided. Sub domain under this category includes but not restricted to neural networks, fuzzy logic and
evolutionary computing. The machine learning techniques such as Decision tree, Naive Bayesian, Instance Based Learning, Decision Table, One Rule, Random Tree and K-Star are used [145] and stated that Decision Tree is accurate. Reference [89] incorporates shift key and used Random Forest algorithm and achieved FAR of 1%, FRR of 14% and ERR of 5%. Reference [113] used Random forest which are based on numbers and achieved FAR of 1.51% and accuracy of 99.97%. Reference [144] used Nearest neighbor classifier, Gaussian model, One-class SVM for database of Beihang.

5.2.1 Neural Networks

Neural Networks (NN) are adaptive non-linear statistical data modeling tools which have been inspired by biological interconnection of neurons. References [122], [12] used NN for their classification. There are two ways in which the weights can be assigned-supervised learning and unsupervised learning. One of the most popular methods in supervised learning is backpropagation. Marcus and Samuel use the Artificial Neural Networks for investigation and achieved results as shown in Table 3. Recently reference [119] used Probabilistic Neural Network (PNN) and achieved ERR as 0%. References [105], [19] used Perceptron (NN). Reference [128] used Z-score, BPNN, PNN, and CFNN and stated that PNN was the best. Reference [1] used Adaline NN and BPNN. Reference [65] used GA based wrapper approach and fitness function. Reference [21] used ARTMAP-FD neural network and compared it with other methods and stated that it has the lowest ERR of 14.94%.

5.2.2 Pattern Recognition and Learning based Algorithms

Pattern recognition is the act of using patterns or objects and classifying them into different categories based on certain algorithms. It includes Bayes classifier, Fisher linear discriminant (FLD), Support Vector Machine (SVM), etc. Reference [18] used Bayer classifier, FLD and minimum distance classifier for classification and achieved FAR of 2% and References [127], [33] used fuzzy set. Other achievements are listed in Table 4.

Also Reference [22] used Bayesian classifier, Discrimination function. Reference [94] used Learning algorithm and achieved 2.5% of ERR Reference [66] used SVM for classification for Chinese character and achieved 100% accuracy except one character due to the small size of its font. Reference [62] used 14- anomaly detection algorithms and achieved ERR from 9.6% to 10.2%. Reference [111] proved the fusion 2D faces (Eigen face algorithm and association between key points) and Keystroke dynamics (SVM) which resulted as ERR of 2.22% for fusion, 8.77% for SVM and 6.38% for Eigen face algorithm and association between key points. Reference [8] used Decision Fusion Center which applies Chair- Varshney Fusion algorithm for multi modal authentication.

5.2.3 Search Heuristics and Combination of Algorithms

Search heuristics such as Genetic Algorithm (GA) are used to find an optimum solution. They are a part of evolutionary algorithms. Ant Colony Optimization (ACO) is an example where GA is used. They also find application in areas such as bioinformatics. Reference [20] used PAM as classification and Reference [30] used SVM, GA and achieved FRR of 3.54%. Reference [126] used Virtual Key Force (VKF) and resulted that ACO reduces 46.51% of total features. Reference [4] used GA, PSO, BPNN and achieved FAR of 0.01% and ERR of 0.063%. Reference [37]
proposed PSO and compared it with GA. Reference [98] used NN, Fuzzy, Statistical classifier. Reference [147] used GMM-UBM, DBN and achieved 0.055 and 0.035 of ERR respectively. Reference [39] states different algorithms (such as Novel joining method, etc.,) with their results, tools and techniques for behavioral biometrics. Refer Table 5 for further achievements in these algorithms.

6. Future Work

In the previous search work, the various algorithms for identification and verification of a user are discussed. We believe that the selection of a suitable algorithm will help us to achieve high accuracy and reliable biometric system. Our work is to select an appropriate algorithm for these methods. The algorithms as used to be are Hausdroff distance for feature extraction and Memetic algorithms (MA), Stochastic Diffusion Search (SDS) for feature selection and Adaptive Resonance Theory (ART), Radial Basis Function Network (RBFN) for classification techniques respectively. A brief discussion and the previous work of both the algorithms are discussed.

Felix Hausdroff was the first to build up the Hausdroff distance. It includes the Euclidean distance and has some other calculations. The Hausdroff distance between the poly lines and the usage of the areas are discussed [42], between curves [17] and between two point sets [120]. Reference [95] they provide the algorithm for minimum summed Hausdroff distance under translation and problems related to minimize the Hausdroff distance between points, disks and balls. The Hausdroff distance between set of plane parametric curves and the proposed the algorithm for computation and calculated the accuracy of the system by [68]. Reference [80] computes the linear time algorithm between convex polygons and reference [81] computes the Hausdroff distance between the models at interactive rates and calculated the depth and both described some lemmas.

Memetic algorithms are a class of stochastic global search heuristics in which Evolutionary algorithms based approaches are combined with the problem solvers. Reference [86] the various algorithms used in Neural Networks and they proposed the MA and stated that MA are the best and reference [88], [102] used for travelling salesman problem and reference [51] used MA for optimization with some case studies and reference [44] used for vehicle transportation. MAs are utilized in medicine, economics, mathematics, oceanography, etc.

Stochastic Diffusion Search (SDS) is a multi-agent population based global search and optimization algorithm which is simple and robust. SDS is used for solving best-fit pattern recognition and matching problems. It is a search technique in the Swarm Intelligence family. References [123], [129] used SDS for pattern recognition and reference [64] shown that it can be applicable to stochastic and dynamic optimization problems. Reference [90] proposed SDMS using SDS which is the formation of an advertising network consisting of a population of independent agents/websites. Reference [82] given an overview of SDS and Reference [46] used SDS and proposed SDS-PSO technique to solve the knapsack problem.

Grossberg introduced the Adaptive Resonance Theory (ART) to overcome the stability and plasticity. It encompasses a wide variety of Neural Networks. It is classified as ART1 and ART2 based on their input patterns. Reference [77] used ART1 to produce stable and clear
recognition even beyond the originally stored template and reference [103] the use of unsupervised ART2 neural network for recognizing patterns in statistical process control charts and shown that these networks are plastic and stable without erasing currently stored information. Reference [11] achieved 97% accuracy in protein classification using ART2 neural networks. FuzzyARTMAP which is supervised ART used in applications such as analytical chemical process and environment [27], [141] and for analog pattern categorization and learning [38] and to retrieve the content based text and image [10].

Radial Basis Function Network (RBFN) is a linear model which is defined as functions with responses decreasing or increasing monotonically with the distance from a central point. RBFN in reference [106] used as neural network for face recognition and achieved better recognition rate of 98.6% and acceptance ratio of 85%. Reference [74] combined RBFN and Gaussian and proposed GRBF which is used for learning strategies and reference [76] they analyzed mathematically and proven some theorem relating RBFN and reference [96] used it for universal approximation.

7. Conclusions

In this survey, an extensive survey of research conducted in the field of keystroke dynamics over the past decades is listed. In order to make an effective biometrics there are a few challenges to be overcome. Certain features are more useful from others which we seen from the existing literature. However, the above given algorithms can be used in the enhancement of our future work. A large variability in the stored template and current template is the typing behavior of an individual changes. Since keystroke dynamics is non-intrusive and cost effective biometric, it has tremendous potential to grow in the area of cyber security and remote monitoring.

References


Akila M, Suresh Kumar S “Improving Feature Extraction in Keystroke Dynamics using Optimization Techniques and Neural Network” in SEISCON 2011.


Alex Andersen and Simen Hagen “Using alert levels to enhance keystroke dynamic authentication” in NIK conference, 2007.


Dawn Song, Peter Venable and Adrian Perrig “User recognition by keystroke latency pattern analysis” in 1997.


Fabin Monrose, Michael K. Reiter, Susanne Wetzel “Password Hardening Based on Keystroke Dynamics” in ACM, 1999.


Nandini Chourasia “Authentication of the user by keystroke dynamics for banking transaction system” in Proceedings of International Conference on Advances in Engineering and Technology, pp. 41-45, 2014.


Nick Bartlow and Bojan Cukic “Evaluating the reliability of credential hardening through keystroke dynamics” in IEEE, 2006.


Sergio Tenreiro de Magalhaes, Kenneth Revett and Hanrique M.D.Santos “Password Secured Sites- Stepping Forward with keystroke dynamics” in IEEE, 2005.


Yilin Li, Baochang Zhang, Yao Cao, Sanqiang Zhao, Yongsheng Gao, Jianzhuang Liu “Study of the BeiHang keystroke dynamics Database” in International Joint Conference on Biometric Compendium (IJCB), IEEE, pp. 1-5, 2011.


Table 1: Features of Keystroke Dynamics

<table>
<thead>
<tr>
<th>Study</th>
<th>Features</th>
<th>Text Type</th>
<th>Users</th>
<th>Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>[35]</td>
<td>Trigraph</td>
<td>S</td>
<td>44</td>
<td>220</td>
</tr>
<tr>
<td>[118]</td>
<td>Key hold time</td>
<td>S</td>
<td>53</td>
<td>10000</td>
</tr>
<tr>
<td>[45]</td>
<td>N-graph</td>
<td>S</td>
<td>19</td>
<td>95</td>
</tr>
<tr>
<td>[60]</td>
<td>Digraph</td>
<td>S</td>
<td>50</td>
<td>500</td>
</tr>
<tr>
<td>[97]</td>
<td>Latency</td>
<td>D</td>
<td>25</td>
<td></td>
</tr>
</tbody>
</table>

S-Static, D- Dynamic
**Table 2: Listing the Statistical Approach**

<table>
<thead>
<tr>
<th>Study</th>
<th>Features</th>
<th>Classification</th>
<th>Users</th>
<th>Samples</th>
<th>FAR</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>[131]</td>
<td>Latency</td>
<td>Statistical classifier</td>
<td>6</td>
<td>36</td>
<td>0%</td>
<td>4%</td>
</tr>
<tr>
<td>[24]</td>
<td>Latency</td>
<td>Mean</td>
<td>17</td>
<td>34</td>
<td>6%</td>
<td>12%</td>
</tr>
<tr>
<td>[54]</td>
<td>Digraph</td>
<td>Mahalanobis distance</td>
<td></td>
<td>0.0001</td>
<td>0.5</td>
<td></td>
</tr>
<tr>
<td>[109]</td>
<td>Latency</td>
<td>Mean, S.D</td>
<td>33</td>
<td>429</td>
<td>0.25%</td>
<td>16.36%</td>
</tr>
<tr>
<td>[125]</td>
<td>Digraph, Latency</td>
<td>Mean, Median, S.D</td>
<td></td>
<td>0%</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>[53]</td>
<td>Duration</td>
<td>Statistical classifier</td>
<td></td>
<td>9%</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>[23]</td>
<td>Digraph, Trigraph</td>
<td>Distance measure</td>
<td>205</td>
<td>0.0456%</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td>[100]</td>
<td>Latency, duration</td>
<td>Statistical fusion</td>
<td></td>
<td>1.035%</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>[9]</td>
<td>Latency</td>
<td>Hungarian matching</td>
<td>783</td>
<td>0.88%</td>
<td>9.62%</td>
<td></td>
</tr>
<tr>
<td>[15]</td>
<td>Free text</td>
<td>Statistical measure</td>
<td>30</td>
<td>450</td>
<td>3.23%</td>
<td>1.61%</td>
</tr>
<tr>
<td>[139]</td>
<td>Latency</td>
<td>Statistical measure, Random Distribution function</td>
<td>20</td>
<td>4.38%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>[67]</td>
<td>Latency, Duration</td>
<td>Statistical measure</td>
<td></td>
<td>1.89%</td>
<td>1.45%</td>
<td></td>
</tr>
<tr>
<td>[134]</td>
<td>Latency, Duration</td>
<td>Statistical method, Measure of disorder, Time discretization method and Fusion of these three methods</td>
<td>38</td>
<td>1.7%</td>
<td>2.1%</td>
<td></td>
</tr>
<tr>
<td>[78]</td>
<td>Digraph, Trigraph</td>
<td>Typing path</td>
<td>18</td>
<td>0%</td>
<td>0% to 55%</td>
<td></td>
</tr>
<tr>
<td>[59]</td>
<td>Digraph, Dwell time, Trigraph</td>
<td>Position Specific Scoring Matrices(motif) and multiple sequence algorithm</td>
<td>20</td>
<td>0.6%</td>
<td>0.4%</td>
<td></td>
</tr>
<tr>
<td>[99]</td>
<td>Latency, Duration</td>
<td>Linear Discriminant Analysis</td>
<td></td>
<td>4.23%</td>
<td>18.36%</td>
<td></td>
</tr>
<tr>
<td>[40]</td>
<td>Duration, Latency</td>
<td>Mean, S.D, Distance pattern</td>
<td></td>
<td>0%</td>
<td>3.83%</td>
<td></td>
</tr>
</tbody>
</table>

**Statistical Approach using Identification Rate**

<table>
<thead>
<tr>
<th>Study rate</th>
<th>Features</th>
<th>Classification</th>
<th>Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>[29]</td>
<td>n-graph</td>
<td>Statistical classifier</td>
<td>100% accuracy</td>
</tr>
<tr>
<td>[14]</td>
<td>Latency</td>
<td>BP, Euclidean</td>
<td>Acceptance-84 to 85%</td>
</tr>
<tr>
<td>[75]</td>
<td>Latency, duration</td>
<td>Manhattan distance</td>
<td>Correct classification-73%</td>
</tr>
</tbody>
</table>
### Table 3: Lists the Neural Networks Classification

<table>
<thead>
<tr>
<th>Study</th>
<th>Features</th>
<th>Classification</th>
<th>Users</th>
<th>Samples</th>
<th>FAR</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>[70]</td>
<td>Duration, Latency</td>
<td>ANN, Distance measure, SLP, MLP</td>
<td>46</td>
<td>1840</td>
<td>0%</td>
<td>14.9%  17.4% 11.5%</td>
</tr>
<tr>
<td>[92]</td>
<td>Latency</td>
<td>Potential function, Bayes decision rule</td>
<td></td>
<td></td>
<td>0.7%  0.8%</td>
<td>1.9%  2.1%</td>
</tr>
<tr>
<td>[132]</td>
<td>Latency, Duration</td>
<td>ANN</td>
<td>21</td>
<td>275</td>
<td>0.0</td>
<td>0 to 1.0%</td>
</tr>
<tr>
<td>[72]</td>
<td>Latency, Duration</td>
<td>BPNN, GA, PSO, ACO</td>
<td>27</td>
<td>2700</td>
<td>0.078% 0.063% 0.059%</td>
<td></td>
</tr>
<tr>
<td>[69]</td>
<td>Latency, Duration</td>
<td>MLPN, RBNF</td>
<td>U-21 A-165</td>
<td></td>
<td>3.47% 0%</td>
<td></td>
</tr>
<tr>
<td>[25]</td>
<td>Latency</td>
<td>3-layered BPNN</td>
<td></td>
<td></td>
<td>1.1%  0%</td>
<td></td>
</tr>
<tr>
<td>[130]</td>
<td>Latency, Duration, Digraph</td>
<td>Statistical method, MLP</td>
<td></td>
<td></td>
<td>1.80% 1.35%</td>
<td></td>
</tr>
<tr>
<td>[43]</td>
<td>Finger pressure</td>
<td>k-NN analytical</td>
<td></td>
<td></td>
<td>Accuracy- 99%</td>
<td></td>
</tr>
<tr>
<td>[48]</td>
<td>Latency, Duration, Digraph</td>
<td>Bayesian fusion</td>
<td>24</td>
<td></td>
<td>ERR- 8.21%</td>
<td></td>
</tr>
</tbody>
</table>


### Table 4: Lists the various Pattern Recognition and Learning Based Algorithms

<table>
<thead>
<tr>
<th>Study</th>
<th>Features</th>
<th>Classification</th>
<th>FAR</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>[115]</td>
<td>Latency</td>
<td>Bayes algorithm</td>
<td>2.8%</td>
<td>8.1%</td>
</tr>
<tr>
<td>[93]</td>
<td>Latency</td>
<td>Pattern recognition</td>
<td>0.7%</td>
<td>1.9%</td>
</tr>
<tr>
<td>[142]</td>
<td>Latency</td>
<td>Fuzzy logic</td>
<td>7.4%</td>
<td>2.8%</td>
</tr>
<tr>
<td>[140]</td>
<td>Pressure exerted, Latency</td>
<td>SVM</td>
<td>0.95%</td>
<td>5.6%</td>
</tr>
<tr>
<td>[83]</td>
<td>Digraph</td>
<td>SVM, KRR</td>
<td>0.055</td>
<td>0.007</td>
</tr>
<tr>
<td>[50]</td>
<td>Duration, Latency</td>
<td>sEMG</td>
<td>Identification rate- 99.375%</td>
<td></td>
</tr>
<tr>
<td>[116]</td>
<td>Duration, Latency</td>
<td>Minimum distance classifier, Classification error 13%</td>
<td>3-means algorithm, Neighborhood algorithm 56%</td>
<td></td>
</tr>
</tbody>
</table>

sEMG- Surface Electromyography which is based on Wavelet Transformation and SVM.
**Table 5: List the various Search Heuristics and Combination of Algorithms**

<table>
<thead>
<tr>
<th>Study</th>
<th>Features</th>
<th>Classification</th>
<th>FAR</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>[36]</td>
<td>Duration</td>
<td>GA, PSO</td>
<td>0.76%</td>
<td>0.81%</td>
</tr>
<tr>
<td>[73]</td>
<td>Duration</td>
<td>Mean, S.D, ACO</td>
<td>0%</td>
<td>3.83%</td>
</tr>
<tr>
<td>[71]</td>
<td>Duration</td>
<td>GA, PSO</td>
<td>0.81%</td>
<td>0.76%</td>
</tr>
<tr>
<td>[124]</td>
<td>Duration, Latency, Digraph, Trigraph</td>
<td>GA, PSO, ACO with ELM</td>
<td>&lt;20%</td>
<td>0%</td>
</tr>
<tr>
<td>[114]</td>
<td>Duration, Latency, Digraph</td>
<td>Fuzzylogic, NN, Statistical, Fuzzy and NN, Fuzzy and Statistical, NN and Statistical, Fuzzy and NN and Statistical</td>
<td>0.19</td>
<td>0.11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.22</td>
<td>0.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.13</td>
<td>0.02</td>
</tr>
<tr>
<td>[34]</td>
<td>Latency</td>
<td>ANN, KNN</td>
<td>29%</td>
<td>1.03%</td>
</tr>
<tr>
<td>[41]</td>
<td>Latency, Duration</td>
<td>Manhattan distance</td>
<td>10.1%</td>
<td>21%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Random forest</td>
<td>1.4%</td>
<td>33.0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GDA</td>
<td>1.9%</td>
<td>20.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SVM (Linear)</td>
<td>0.9%</td>
<td>20.9%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SVM</td>
<td>5.6%</td>
<td>7.6%</td>
</tr>
<tr>
<td>[91] and [121]</td>
<td>Latency, Duration, Digraph</td>
<td>Mean, Median, S.D, PSO, Average Accuracy rate</td>
<td>89.23%</td>
<td>87.54%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GA</td>
<td>87.54%</td>
<td>92.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACO</td>
<td>92.8%</td>
<td>93.5%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RABCO</td>
<td>93.5%</td>
<td></td>
</tr>
<tr>
<td>[61]</td>
<td>Digraph</td>
<td>GA</td>
<td>95%</td>
<td></td>
</tr>
<tr>
<td>[56]</td>
<td>KD, fingerprint, palmprint</td>
<td>BFOA, SVM</td>
<td>92.8%</td>
<td></td>
</tr>
</tbody>
</table>