New Physiological Biometrics Based on Human Cognitive Factors

Omar Hamdy and Issa Traoré
Department of Electrical and Computer Engineering
University of Victoria
Victoria, BC, Canada
Omar@uvic.ca and Itraore@ece.uvic.ca

Abstract

Modeling and quantifying different human factors continue to be one of the major challenges in introducing new biometric systems. For example, drivers of some of our behavior differences are still mysteries, and hence cannot be modeled.

In this paper, we propose a novel biometric system; it introduces the visual search and short-term memory human factors to the world of biometrics. This homogeneous system uses only the standard mouse as an input sensor for the two biometric factors.

Experimental evaluation was performed using mass enrollment of 275 participants, and Neural Network for classification. Results showed an Equal Error Rate (EER) of 3.88%.

1. Introduction

A physical or behavioral attribute needs to have certain characteristics in order to qualify as a good candidate in biometric systems. Nevertheless, not all good candidates are practical to use. Many other integrant components affect building any new such system. Drivers of some of our behavior differences are still mysteries, and hence cannot be modeled; for example, how visual distortions correspond to behavioral errors. Some other behaviors are possible to quantify only through high caliber equipments. For example, measuring some of the brain activities in response to different stimulus. Data sensor precision is another factor that shapes the effectiveness of a biometric system. Therefore, introducing a new biometric means a success in all of these areas, and not only in modeling a certain physiological or behavioral attribute.

In this paper we introduce a novel biometric system that is based on human cognitive factors, which overcomes these mentioned limitations and difficulties. Studies in areas related to human perception and cognition are usually directed toward studying collective human behaviors and phenomenons for psychology research [5, 11, 22, 12, 7]. In other research, these attributes are studied to engineer better gadgets and systems for human use and interactions [8, 23]. The novelty in this research is that for the first time, two such human attributes are used for discriminative purpose between humans. The first modeled attribute is the visual scan & detection; this biometric depends on the human visual system (physiological), as well as the developed search skills each one has developed over the years (behavioral). The second attribute is the short-term memory, which has unique characteristics that made it possible for us to model and use in the proposed biometric system.

The system provides a testing framework that studies and records the effect of these human factors in an experiment designed for that purpose. Another notable contribution is that standard mouse is the only data input used for the two cognitive factors. This simplicity of data collection, in addition to the achieved performance make it potential to use this system as authentication mechanism at login time; the fact that no additional or special hardware is required allows using it for authentication on the INTERNET.

It is important to note however, that this work is fundamentally different from other work that used mouse dynamics for as biometrics, such as [2, 16]. In mouse dynamics, the biometrics are based primarily on the mouse movement style and habits of users; in this work however, the mouse movement style is continually changing in response to the cognitive factors stimulation. Hence, the biometric in this research depends on measuring these mouse movement changes and references them to the cognitive factors.

In Section 2, characteristics of the visual scan & detection, and short-term memory cognitive factors are
highlighted. Section 3 details how the visual scan &
detection and the short-term memory were successfully
modeled; this includes the proposed system framework,
and the extracted features. Section 4 details the ex-
periment procedure, biometric analysis, and the per-
formance evaluation. Finally, future directions for that
research are discussed in Section 5.

2. Biometric System Components

The philosophy of this research is that under abnor-
mal circumstance, biometric differences are more dis-
tinct. For examples, people who are walking in downtown on a busy street, and athletes who are competing in 100 m champion marathon. In the first case, dif-
fences are not well visible, because the action falls within most people’s normal capability. In the sec-
ond case, however, the action performed is pushing to the limits, and that is where more obvious differ-
ces could be distinguished from one another. The proposed biometric system therefore, tries to put the
users in very visual distracting environment in an at-
tempt to push their capabilities to the limit.

In this section we explain the introduced visual scan &
detection, and short term memory cognitive fac-
tors. In the following section, we propose a frame-
work to model them.

2.1. Visual Scan & Detection

Visual scan is a frequent process in our daily life.
We search for road signs, we visually search for a piece of
information of interest on a website, or we search for certain food brand in a grocery store. Visual scan
and detection could be defined as the task of discrimi-
inating a target of interest from surrounding distracters [21].
The eye’s fovea has the highest concentration of pho-
toreceptor cells (cones). Therefore, when we perform
a visual search, object images that fall on the fovea
are the ones that are examined, as they can be identi-
ﬁed in details [22]. Special quick and short eye move-
ments called saccades and ﬁxation help changing the
eye location to locate stimuli of potential interest dur-
ing the visual search [22].
The average time estimate needed to search for an ob-
ject among \( N \) objects in a spatial ﬁeld can be expressed by the following [23]:

\[
T = \frac{N \times I}{2}
\]  

(1)

Where \( I \) is the average time one user takes to in-
spect an object during the visual search. The idea is to
proportionately design a process that can measure the aver-
age inspection time \( I \) of an individual, and use that as biometric data. Two main design factors should be con-
sidered to isolate \( I \) from other inﬂuences:

1. Visual search has to be guided by bottom-up model [8], in which cognitive factors, which are the
top-down model, do not inﬂuence the search. For
example, searching for a name in an unsorted list
will require a sequential search in across the entire
list until the desired name is found (bottom-up);
however, searching for the same name in a sorted
list, is inﬂuenced by the cognitive skills to perform
more efﬁcient search (top-down).

2. Experiment should maximize the visual distortion
in order to better differentiate between subjects’ visual search capabilities.

2.2. Short Term Memory

Short-term memory is the human sensory input storage. It receives visual snapshots transferred
from the eye by the visual cortex. Input from the vi-
sual cortex is shortly stored there to give a chance
to the perceptual part of the brain to go through all
the temporarily stored visual snapshots, ﬁlter out all
that are not important or do not worth the atten-
tion, and pass to the working memory visual informa-
tion that are of high importance. Short-term memory
is characterized by two properties: size, and de-
cay. For visual information, the short-term memory is
estimated to have a size of about 17 letters, and an av-
erage decay time of 200 ms [1]. Different researches
have studied the retrieval capacity and capabil-
ity from the short-term memory [13]. It was found
that information retrieval capability from short-term
and working memory is different from one per-
son to the other.

To introduce the short-term memory information re-
trieval as a biometric, the experiment is modiﬁed to
measure that capability. Random text associated with
a shufﬂed keyboard is customized to include some char-
acters that are repeated at certain points of the ran-
dom text. Collected data is later carefully analyzed to
study the retrieval from short-term memory impact.

3. Modeling System

Despite the complexity of the new introduced phys-
iological biometrics, the proposed modeling system
maintains its simplicity by using the standard com-
puter mouse as the only data reader for both biomet-
rics. This means that we are introducing a homoge-
neous biometric system, in which no separate sensors are needed to read each biometric’s data.

3.1. System Framework

The proposed architecture provides an integrated solution suite with tools needed at the different data processing stages. The system main components are presented in Fig. 1. It includes the following main components:

3.1.1. User Cognitive Sensor Module This module provides a configurable test environment. It can design and deploy different tests which targets one or both the human cognitive factors identified. It is composed of the following sub-components:

- **VISUAL DISPLAYS** to generate all the visual QWERTY and Shuffled keyboards displays.
- **TEST GENERATOR** to build the keyboard codes and the random phrases that go with them.
- **SHUFFLER ENGINE** to provide multiple shuffling mechanisms suitable for the different test types.
- **MOUSE TRACKER** to record specific mouse activities.

3.1.2. Feature Extractor Module This module processes user raw data collected from the sensor module, and produces user feature vector. This passes through different data processing stages:

- **USER LOG READER** to read and load all the user recorded data from the testing sessions.
- **FEATURE EXTRACTION** to process the user raw data loaded, and extract the identified features.

3.2. Test Design

The experiment idea is to expose the subjects to sequence of specially designed interactive keyboard illustrations, as shown in Fig. 2. In addition to the keyboard, a special phrase constructed of random characters is also displayed. Subject is then requested to “click-in” the displayed phrase keys. Subject’s response to distracting (shuffled) and non-distracting (QWERTY) keyboards are recorded through the mouse movements for later analysis and feature extraction.

3.2.1. Design Consideration In order to run a successful experiment, the test was designed using the following foundation factors:

- Exposure duration has been found to have strong impact on the effective value attributed to the visual stimulus [19]. Many studies such as [6] and [18] have concluded that the more the subject is exposed to the test, the less his attention gets. Therefore, the test session duration could be at some threshold a confounding factor. In this experiment, the primary factor affecting the test du-
ration is the number of characters in the random text. Therefore, a careful calculation of the random text length was essential to eliminate the exposure long duration effect. A special experiment was designed to experimentally study that effect using a small group of users. Based on the experiment result observations, the random text length of system was chosen to be 25 characters long.

- Short-term memory factor test is implanted in the experiment by selectively duplicating some of the letters in the random text string. Duplicated keys’ measurements are later studied to extract short-term memory factor effect.

- During visual scan, corners of that displayed keyboard image fall near the outer edges of the retina periphery. Image corners are usually regarded as points of curvature discontinuity edges along the contours of detected boundaries [3]. Retina periphery is only capable of transmitting low resolution information to the brain [10] [17], and that is not sufficient to detect a desired key. Therefore, in order to search the corners for a desired letter, subject has to make relatively long saccadic movements for corners to be foveated. The experiment measures subject’s foveated primate vision efficiency at the corners by placing some of the random text letters at the different corners.

3.2.2. Data Acquisition
Publicly available biometric databases such as the European Languages Resource Association (ELRA), Fingerprint Verification Competition (FV2000), and NIST Standard, cut a lot of research time by providing experimental raw data. The Novelty of this research and the type of collected data resulted in losing this privilege. Additionally, in order to build high confidence in the proposed biometric system, a large number of participants was targeted. Furthermore, data acquisition process had to go through iterations till raw data matures to fulfill the desired features extraction. Iterations had to be minimal and efficient, because each iteration failure means to discard valuable participant’s raw data.

3.3. Feature Extraction
The first observation we recoded was the number of features that could be compounded. At ground zero, there were independent parameters collected that are considered features, such as speed, fly time, and distance. The next level of complexity adds features by observing changes in one feature as influenced by others. For example the change in fly time average when keys are located at the different corners of the keyboard image. Moreover, some features allowed establishing complex relations across them. For example, it was observed that if the search for letter is prolonged, some participants tend to slow their mouse speed, while others go even faster as a sign of frustration. Furthermore, we were able to isolate additional features by observing the way features are changing from one state to the other. For example, when subject is clicking the same key more than one time throughout a test session, she starts building a memory awareness of the location of that key. All these feature extraction methods gave a total of more than 100 candidate features that the system can use for this biometric system.

An efficient methodical approach was followed to identify the golden set suitable for the scope of this biometric system. More specifically, the following criteria were considered:

1. Suitability: candidacy is determined according to the relevancy of the feature to the biometric system two cognitive components.

2. Distinctiveness: candidate features must have mean values different from one subject to the other.

3. Reproducibility: data values of features of the same user are reproducible from one session to the other, with relatively small difference.

4. Singularity: candidate features should be examined to see that no two or more features possess the same behavior in response to different test states.

The mentioned selection criteria were carefully used to filter all the candidate features. The feature golden set which were finally selected as the basis for the proposed biometric system are summarized in Table 1.

4. Experiments
A large scale experiment was conducted to evaluate the system. The hypothesis in this experiment was to establish that the proposed framework can be used to discriminate between different users based on the introduced cognitive characteristics.

4.1. Procedure
This experiment involved 275 participating subjects. Subjects possessed high diversity among them; this included gender, age range, right/left handed, different computer skills, and normal (or corrected to normal) vision range. Each participating subject was seated in a non-distracting (audible or visual) testing environment, and did the experiment without prior
knowledge of recorded behaviors or actions. The experiment was composed of 10 consecutive sessions; two sessions used QWERTY keyboards, and the remaining eight sessions used unique shuffled keyboard for each session. There was a delay time between sessions set to 45 seconds to help subjects release their focus and attention before they start the next sessions.

All participating subjects conducted the experiment using the same equipment. The application was designed as JAVA SWING desktop application, developed using SDK 1.6 running on Windows XP SP2 OS. The hardware used is Dell VOSTRO 200, 1.6GHz, and 2 GB RAM. Display is Dell 19’ Flat Screen set to 1600x1200 pixels, where the keyboard image is set to 800x200 pixels.

### 4.2. Biometric Analysis

As explained in Section 3.3, four criteria were considered in selecting the feature golden set. Among which, reproducibility and distinctiveness are numerically quantifiable, and could be presented in numbers. These two factors, considered as the measurement criteria of the system success, can be quantified by computing the variance between sessions from each user (expected to be relatively small) and the variance between sessions from different users (expected to be relatively large). The measurement criteria mentioned above are the foundation of the biometric analysis defined as the process of validating that a user is who she claims to be.

The system compares input template of an identity claim against a stored genuine template of that user. Biometric analysis is done using Neural Network; it is divided into two phases: user enrollment, defined as the creation of user’s master template, and user verification using an efficient classification mechanism. The user’s master template uses the golden feature list defined in Table 1 to train a customized neural network. The produced template is used in the second phase to evaluate a user claim (verification) by comparing her input with the stored master template.

Our enrollment strategy consists of dividing the user population into two different sets, known as legal and impostor groups. Building a profile for a legal user consists of training the neural network using sample data from only the legal group. By using the genuine feature data samples from a user being profiled (self data), as well as data samples from other legal users (non-self data), the neural network generates and stores a master template for that user.

The neural network was constructed using Feedforward network with two hidden layers (of 15 and 20 nodes respectively), in addition to the input and the output layers. Linear, Log Sigmoid, and Linear are the transfer functions for the two hidden layers and the output layer respectively. The neural network produces a confidence value output ranges from 0 to 1, where 0 represents a perfect no-match, and 1 represents a perfect match result. Based on a predetermined threshold, an output confidence value is determined to be a match or non-match.

A special data feed technique (we call divide and select) is used, in which, input data are clustered into two separate features groups. Each group is fed to separate but identical neural networks. The two produced outputs from the two network segments are allowed to compete to be picked as the representative of the overall output. The champion is the one that has a stronger yes (close to 1), or no (close to 0). In the case that both are hesitant or giving confident but opposite answers, they are averaged to produce the final output. This model is shown in Figure 3.

### 4.3. Data Analysis

For all the participating subjects, collected raw data was used to calculate the golden features’data values. To prove the research initial hypothesis is valid, data values of the features were studied to validate the reproducibility and distinctiveness explained in Section 3.3. Table 2 demonstrates in numbers these two data

<table>
<thead>
<tr>
<th>Feature</th>
<th>Biometric Component</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>W-n-F</td>
<td>Visual Scan &amp; Detection and Short-Term Memory Groups</td>
<td>Wait and Fly is defined as the short silence time (no mouse activity) right after a key click till the user decides on the next move.</td>
</tr>
<tr>
<td>FT</td>
<td>Visual Scan &amp; Detection and Short-Term Memory Groups</td>
<td>Fly Time is defined as the elapsed time while user is actively (continuous mouse activity) searching for the next key.</td>
</tr>
<tr>
<td>FT Q2S</td>
<td>Visual Scan &amp; Detection Group</td>
<td>Defined as the ratio of average Fly Time in QWERTY to Shuffled keyboards of the same user.</td>
</tr>
<tr>
<td>FT OCC</td>
<td>Short-Term Group</td>
<td>Measures the Fly Time improvement rate as the one key occurrence increases in one test session.</td>
</tr>
<tr>
<td>DST Q2S</td>
<td>Visual Scan &amp; Detection Group</td>
<td>Defined as the ratio of average Traveled Distance in QWERTY to Shuffled keyboards of the same user.</td>
</tr>
<tr>
<td>DST OCC</td>
<td>Short-Term Group</td>
<td>Measures the Traveled Distance decrease rate as the one key occurrence increases in one test session.</td>
</tr>
</tbody>
</table>

**Table 1. Biometric Feature Set**
qualities using data from four random users, three ses-
sessions each. Looking at data values of any feature, we
find values to be relatively close to each other for
the same user, and relatively different across different
users.

<table>
<thead>
<tr>
<th>USER</th>
<th>Session</th>
<th>WnF</th>
<th>FT Q2S</th>
<th>FT OCC</th>
<th>DST Q2S</th>
<th>DST OCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>User 1</td>
<td>1</td>
<td>1074</td>
<td>4603</td>
<td>0.63</td>
<td>0.87</td>
<td>0.36</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1021</td>
<td>4733</td>
<td>0.59</td>
<td>0.85</td>
<td>0.39</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1002</td>
<td>4587</td>
<td>0.60</td>
<td>0.88</td>
<td>0.32</td>
</tr>
<tr>
<td>User 2</td>
<td>1</td>
<td>906</td>
<td>2376</td>
<td>0.78</td>
<td>0.40</td>
<td>1.02</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>954</td>
<td>2340</td>
<td>0.79</td>
<td>0.52</td>
<td>1.07</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>819</td>
<td>2412</td>
<td>0.77</td>
<td>0.48</td>
<td>1.03</td>
</tr>
<tr>
<td>User 3</td>
<td>1</td>
<td>733</td>
<td>2879</td>
<td>0.61</td>
<td>0.22</td>
<td>0.81</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>746</td>
<td>2956</td>
<td>0.61</td>
<td>0.28</td>
<td>0.77</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>714</td>
<td>2843</td>
<td>0.65</td>
<td>0.21</td>
<td>0.76</td>
</tr>
<tr>
<td>User 4</td>
<td>1</td>
<td>1410</td>
<td>1834</td>
<td>1.10</td>
<td>0.71</td>
<td>1.09</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1524</td>
<td>1965</td>
<td>0.94</td>
<td>0.64</td>
<td>1.12</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1493</td>
<td>1964</td>
<td>0.94</td>
<td>0.73</td>
<td>1.10</td>
</tr>
</tbody>
</table>

Table 2. Sample Feature Data of Three Sessions of Four Users. Among one user’s sessions, values of each feature are relatively close (stable), but different (distinctive) from one user to the other.

4.4. Performance Results

Performance of the biometric analysis is expressed in terms of Equal Error Rate EER. EER is achieved when the rate at which the system cannot recognize a user’s biometrics (False Rejection) is equal to the rate at which the system falsely matches a biometric data to a user (False Acceptance).

The evaluation was done using five-fold cross validation. The user population was divided into 5 subsets of equal size. Therefore, 5 testing rounds were performed before final EER value could be produced. For each round, one out of the five subset divisions are considered legal subset. Then sessions of each user in that group are fed to the network to build profile as explained in Section 4.2. For testing, sessions from the legal group that were not used for training, as well all sessions from the other four subsets are used. Based on the threshold, a confidence value is rounded to either 1 or 0. Each rounded value is compared against its producing session to measure system correctness. To properly calculate the performance, different counters are used to count the number of correct and false results produced by the Neural Network. Counter values are later used to calculate the average False Acceptance and False Rejection rates explained above. Table 3 shows the performance of the biometric analysis at five different threshold values, where the middle row represents the EER value.

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Divide &amp; Select Model &quot;Far (%)&quot;</th>
<th>FRR (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>20%</td>
<td>37.33</td>
<td>21</td>
</tr>
<tr>
<td>40%</td>
<td>19.55</td>
<td>2.94</td>
</tr>
<tr>
<td>62%</td>
<td>3.88</td>
<td>3.88</td>
</tr>
<tr>
<td>75%</td>
<td>1.73</td>
<td>20.09</td>
</tr>
<tr>
<td>90%</td>
<td>0.52</td>
<td>26.14</td>
</tr>
</tbody>
</table>

Table 3. Sample Evaluation Performance for the Neural Network Model.

Given the novelty of the proposed biometric factors, the achieved results are considered promising when compared to performance of other known biometrics. For example, in voice biometrics, in the 2006 NIST SRE competition, D.E. Sturim et al. [20] introduced a voice biometric algorithm that proved EER performance of 4.04%. For hand signature biometrics, a Hidden Markov Chain based model showed an EER of 9.253% [14]. In keystroke dynamics, Jiang et al. [15] approach achieved an EER performance of 2.54%. Finally, comparing the results with the mouse dynamics, Ahmed and Traore’s work [2] achieved through their patent pending approach an EER performance of 2.4649%.

Additional observation from the results is that depending on the security targets, the threshold can be adjusted to meet these targets. For example, setting the threshold at 90% will give high confidence that no one will be falsely accepted; however, that will...
be at the cost of high percentage of legal users being denied access at their first attempt.

5. Conclusions and Future Work

5.1. Conclusions

In this paper, we introduced new cognitive features that were long studied by medicine and psychology researchers, to the world of biometrics. The modeling architecture provided an integrated solution suite suitable for capturing, filtering, analyzing, and building quantified profile for each user. Additionally, the designed experiment used a simple visual test, and the standard mouse to read user responses; this is a notable contribution as compared to the sophisticated medical devices that reads eye and brain activities, and the long test procedures that researchers of psychology use. Experiment results numerically supported the research hypothesis that the introduced cognitive factors can be used as discriminative basis between users. This was further verified through biometric analysis. An efficient neural network model that was designed for the analysis showed a promising EER of 3.88%.

5.2. Future Works

The new human physiological factors presented in this paper opened doors for a new group of physiological attributes to be effectively used in static user authentication. The proposed modeling system showed that data values of the features were reproducible for each user, and distinct from one another; these are two of the most important factors in designing a static authentication system. In this case, the achieved biometric accuracy might not be efficient enough for commercial user authentication system. There are number of techniques that could be used as future work to enhance the overall performance; one of which is the use of fuzzy decision tree classification technique. Statistical attributes of data values of each user’s features, such as means and standard deviations, are used to build a decision tree. Trees are later used to authenticate users. Another important feature of the proposed system is the fact that the system uses only the standard mouse. Additionally, the proposed system requires very lightweight GUI. The proposed implementation used JAVA SWING of a total size of about 20KB. These two features make it possible to propose this system as an effective web-login tool designed to target consumer applications, such as web-banking.

References


