Developing a New Haptic Passcode for User Authentication with a Personal ID Tag to Prevent Copying Attacks

Seongil Lee 1, Kyohyun Song 2 and Sangmin Kim 3,*

1 Department of Systems Management Engineering, Sungkyunkwan University, Suwon 16419, Korea; silee@skku.edu
2 LG Electronics, Seoul 06772, Korea; kyohyun@skku.edu
3 Department of Industrial Engineering, Sungkyunkwan University, Suwon 16419, Korea
* Correspondence: sangminkim06@gmail.com; Tel.: +82-031-290-7619; Fax: +82-031-290-7610

Received: 7 October 2019; Accepted: 12 December 2019; Published: 15 December 2019

Abstract: We designed a haptic authentication system with a personal identification (ID) tag equipped with an embedded acceleration sensor and a radio frequency identification (RFID) tag that can be used in automated security systems. In the suggested system, users generate a passcode by haptic manipulation of an ID tag instead of typing in passwords using a keypad. An ID tag may be an ideal personalized gadget for ID authentication in many circumstances. The core of the proposed haptic authentication system is the activity-recognizable process that can be manipulated by the probabilistic model we developed and generate a much more secure passcode for authentication. With the system learning a total of 250 trials by 50 users for each haptic gesture, the average successful classification rate for the four-digit haptic passcode authentication was 88.9% using the probabilistic model we developed. Some haptic gestures, such as vertical upward flipping of the ID tag, showed lower accuracy than others due to the difficulty in haptic manipulation of the ID tag. From a copying attack experiment to examine the reliability of our haptic passcode scheme, it was proved that the haptic gestures with enough digits, apparently at least 6, were difficult enough to resist being copied by attackers. The same authentication scheme can also be applied for other personal devices that can be manipulated by hands for making haptic gestures, such as a mobile phone.

Keywords: authentication; gesture; haptic; identification; ID tag; passcode

1. Introduction

Automated security systems are designed to provide an extra layer of security through user identification followed by authentication to prevent illegal break-in at various entry points. Intelligent home networks and automated corporate security systems nowadays adopt various types of security systems mostly based on a single-layered system, such as an identification (ID) detecting system with radio frequency identification (RFID) or ZigBee tags [1–3]. When these single-layered systems experience intrusions of user identification, there is usually no backup system to monitor the entry point and track down trespassers. This shortcoming can be supplemented by implementing a multilayered security system [4,5]. The multilayered security system consists of the main user identification system and a secondary system backing up the main system for additional user authentication. The major challenges that automated security systems now face involve developing methods that cannot be broken into easily in the secondary system.

In case of the home security system, residents are required only to attach a personal ID tag such as resident card with embedded RFID for authentication. However, at some other highly secured entry
points such as the main entrances of corporate and research facilities, it is also required to input a
security code and password or scan a fingerprint as an additional authentication process. In the case of
the automatic teller machine (ATM), customers are asked to insert a bank card for identification and
then input a personalized password for additional authentication. The problem of using a numeric
keypad for secondary authentication is that the input combination can be exposed to the person
standing behind and decoded easily. An authentication system equipped with a keypad, keyboard,
or fingerprint scanner can be damaged unexpectedly and will need to be maintained periodically.
Technologies like Bluetooth and RFID would make it possible for ATMs to identify users without them
inserting bank cards. In this way, mobile phones with personalized tags could replace bank cards in
the near future.

In this paper, we propose a new authentication scheme with the use of a personal ID tag and
haptic gestures for an integrated security system. The haptic passcode recognition module scans for
personalized gesture input made with a personal ID tag equipped with an acceleration sensor; this
would be hard for non-authorized users to copy since the passcode is generated with haptic gestures
instead of in alphanumeric format. We have obtained satisfactory result in terms of accuracy and
usability with the suggested haptic authentication scheme.

In Section 2 of this paper, we elaborate on the integrated architecture of the system and the
hardware prototype. In Section 3, the proposed algorithms of the haptic authentication scheme are
described. Experiment results on user performance in terms of usability are discussed in Section 4.
The possibility of application to mobile phones with the suggested scheme using the same algorithm is
explored in Section 5, and future studies to further develop the authentication system are also suggested.

2. Background and Related Studies

Most authentication schemes request the users to prove possession of either secret knowledge,
such as a password or personal identification number (PIN), or a physical token, like an ID card [6].
RFID has been widely used for user identification and authentication systems [1,2,6,7]. RFID is a
relatively new type of physical token used for basic forms of authentication processes, mostly to grant
access at entry points of an automated system. For example, it provides a convenient method of
authentication for many automated security systems in home networks and at entry points of private
corporate environments. However, single-layered security systems using RFID have shown a lack of
security with untrusted usage of a stolen ID tag, even with a personal photo on it.

Access by keying in correct secret codes can only be made using a certain type of interface.
Traditional authentication methods with alphanumeric passwords for proving secret knowledge have
been criticized for being vulnerable to shoulder-surfing and replay attacks. To prevent this risk, many
alternative approaches to retain ease of use while increasing security have been investigated.

One of those approaches was to utilize pattern recognition [5,8–11]. Gesture patterns, eye-gaze
patterns, and facial patterns have also been used as personal security codes. Studies based on gesture
recognition require two key components: (1) acceleration sensors to obtain gesture pattern data
and (2) robust probabilistic inference algorithms to analyze the data gathered and classify them into
gestures. Since acceleration sensors have the advantage of small size, robustness, and convenience to
be embedded into any wearable or portable devices over other sensors, they have been one of the main
sensor selections for arbitrary activity recognition through gestures. With an acceleration sensor, for
example, a mobile phone can be a practical authentication device that creates a password from discrete
gestures [12,13]. Even though it was reported that a text-based PIN is superior to a gesture passcode
in terms of memory retention [12], since text can contain meanings or personal context in a limited
manner, gesture passcodes using a mobile phone showed a possibility to utilize a user’s kinesthetic
memory to effectively recall the passcode.

In selecting gesture-based patterns for a passcode, in a similar study using the Wii remote [14],
users seemed to be concerned with the practical use of gestures and selected patterns based on such
factors as “easy to remember”, “convenient movement”, and “fast to perform”.

Applied Sci. 2019, 9, 5520
However, gesture-based passwords can cause security problems for users since gestures are likely to be more visible than text. Since gestures are subject to easy observation and hence lack robustness against leakage, other types of haptic information have also been explored. Haptic devices can provide very rich information about hand movements in terms of direction, pressure, force, angle, speed, and position of the user’s interaction, called behavioral characteristics. Using these haptic features, keystroke dynamics, handwritten signatures, user patterns of mouse movements, and finger motions can be used for characterizing personal attributes. Orozco et al. [15] constructed a simple maze application to test the possibility of haptic authentication, but they reported problems in the reliability and accuracy of the algorithm. Better performance results with probability of correct user identification ranging from 81% to 93% were reported with an improved haptic authentication system to characterize a user with haptic signature analysis [16,17]. These studies, however, used a fixed haptic device, such as the Phantom, that cannot be embedded at entry points for an automated security system.

Behavioral biometrics use a user’s operational habits and preferences as identify information, and hand gesture is a typical example investigated for authentication to capture biometric information on many smartphone platforms. Many researchers tried to distinguish users based on their input patterns and touch characteristics by extracting information from touch movements on smartphones [18–23]. These studies concluded that it is possible to positively improve the security of password patterns on touchscreens by integrating behavioral biometrics. Swipe patterns—continuous gestural touch behaviors made on touch screens—have been adopted as a popular password method for user verification or identification on many Android smartphones. In public, however, the swipe passwords on touchscreens may become visible to attackers who engage in shoulder surfing. To prevent over-the-shoulder attacks, Cain et al. [18] empirically explored the factors for creating secure swipe passwords and found that symmetrical swipe patterns were more difficult to replicate than asymmetrical patterns. They also found out that providing visual feedback of entry gestures on the screen would make the swipe authentication vulnerable to the over-the-shoulder attacks; thus, it is recommended to turn off the visual feedback on the screen when the authentication is made.

The behavioral characteristics of users when making a swipe gesture on smartphones, such as pressure strength, rhythm, or angle used, result in discriminative patterns that can be exploited to authenticate users. Pozo et al. [19] explored a statistical approach to the performance across different kinds of swipe operations and revealed that some gestures hold more user-specific information and are more discriminative than others. Antal and Szabo [20] extracted 11 different behavioral characteristics of swipe gestures used on touchscreens, such as duration, length of trajectory, velocity, pressure, and average gravities in touch points on three axes. Among those characteristics, the average x, y, and z gravities were found to be the most discriminative behavioral features. It was also reported that five consecutive swipe movements, instead of a single swipe movement, yielded satisfactory error rates for authentication [20]. Combined with hand geometry information, behavioral characteristics may provide an accurate and reliable authentication scheme. Song et al. [21] designed multi-touch gestures combining hand geometry information and behavioral characteristics to develop a simple and reliable swipe-based authentication method for mobile devices equipped with touchscreens. With only simple touch with fingers straight and together gestures such as vertical, horizontal, and L swipes, Song et al. [21] still came up with secure multi-touch authentication that resulted in error rates comparable with those in other studies [19,20,22]. The behavioral characteristics of gestures provide an additional layer of security to the proposed gesture-based authentication methods since those characteristics are not explicitly visible to the attackers while the gestures and touch movements themselves are graphical and somehow visible.

Using eye-gaze patterns for authentication requires eye tracking. De Luca et al. [24] created the “EyePassShapes” using eye gestures to construct an EyePIN, and Kumar et al. [25] used gaze patterns by tracking eye-focus points when the users found passwords. Although these authentication methods deter or prevent a wide range of break-ins or hacking, they have been criticized due to the high price of the equipment and system setup that would not be acceptable for practical use.
Meanwhile, the facial recognition technique requires supplementary equipment such as a high-resolution camera and a lighting device for nighttime use [11].

3. Design and Implementation

The system uses gestures on or manipulation of an ID tag to generate a haptic passcode (Table 1). These gesture or manipulation patterns include tapping, shaking, and flipping of the ID tag. The signals acquired through the acceleration sensor are processed on five different axes \((x, y, z, y-z, x-z)\), and passcodes are generated from various combinations of signals from each axis. Currently, seven different patterns of haptic manipulations can be differentiated after a probabilistic inference analysis on the signals acquired from the five axes is performed. The passcode in haptic format is then sent to the automated security system via a Bluetooth communication module for a personal authentication check. The automated security system then matches the passcode patterns with the pre-stored personal passcode patterns and decides whether to allow access.

**Table 1. Description of the finalized haptic gestures to generate a passcode.**

| Pattern | Description of Manipulation of the Identification (ID) Tag | Latency (ms) | User Preference | Data from Axes |
|---------|--------------------------------------------------------|--------------|-----------------|----------------|
| TAP     | TAPping on the frontal side of the tag                  | 622          | 17.8%           | \(x, y, z\)    |
| SHK     | SHaKing the tag                                         | 1790         | 10.4%           | \(x, y, z, y-z\)|
| VF90    | Vertical upward Flipping by 90 degree                   | 1315         | 13.3%           | \(x, z, y-z\)  |
| VF180   | Vertical upward Flipping by 180 degree                  | 1527         | 11.1%           | \(x, z, y-z\)  |
| HFR     | Horizontal Flipping by 90 degree to the Right           | 1353         | 24.4%           | \(x, y, z, y-z\)|
| HFL     | Horizontal Flipping by 90 degree to the Left            | 1257         | 15.6%           | \(x, y, z, y-z\)|
| TO      | Turning Over and back to the normal position            | 3137         | 7.4%            | \(x, z, x-z\)  |

To generate a passcode by combining haptic gestures such as tapping, flipping, or shaking an ID tag, an interval of approximately half a second between each haptic manipulation is required.

3.1. Hardware and Functional Units

The ID tag consists of a three-axis acceleration sensor (model MMA7260, an Atmega 16 L Microprocessor from Atmel, Microchip Technology, Chandler, AZ, USA) from NXP Semiconductor
(Eindhoven, Netherlands) running at 8 MHz maximum clock speed and an RFID tag with 915 MHz frequency. The acceleration sensor output is sampled at a bandwidth of 33 Hz.

The dimensions of the entire hardware enclosure in the ID tag are $60 \times 75 \times 4$ mm, and the weight of the ID tag is 64 g including a battery. Figure 1 shows a user manipulating the prototype ID tag with an acceleration sensor and an RFID tag to generate the haptic passcode once the initial entry authentication process is completed.

![Figure 1. Manipulation of a prototype ID tag to generate haptic passcodes.](image)

3.2. Haptic Gestures for Passcode

We generated more than 10 candidate haptic gestures for creating passcodes with an ID tag and tested them to adopt those that maintain security levels as a final haptic gesture set. Some gestures resulted in acceleration sensor signal patterns that were too similar to be distinguished from each other, and some gestures were too difficult to be made with an ID tag. Based on learning to classify the gestures using the classification algorithm we developed (Algorithm 1), the system learned a total of 250 trials by 50 college students for each haptic gesture to define the normalized value in signals and the threshold probability of each gesture. We finalized only seven haptic gestures that showed concrete repeatability and relatively high accuracy in classification learning for a final haptic gesture set. Table 1 provides a description of the seven finalized haptic gestures we selected to generate passcodes in this study, and Figure 2 shows the acceleration sensor signals from five axes of the seven haptic gestures.

3.3. Classification Algorithm

An important component of the haptic authentication system is the program for classifying gesture signals into different patterns. The classification algorithm was developed using a probabilistic inference model with flow shown in Algorithm 1. The algorithm normalizes the sensor information from the acceleration sensor in five different axes: $x$, $y$, $z$, and two combined axes of $x$–$z$ and $y$–$z$, shown in Figure 2. The system learned a total of 250 trials by 50 users for each manipulation gesture to define the normalized value in signals and the threshold probability of each gesture. Manipulation gestures are classified by how the normalized values and their probability thresholds in signal distribution on the five axes vary among the patterns. Compared with traditional pattern recognition, which only deals with one stream of signal data, our algorithm has to handle multiple data streams including position, orientation, acceleration, and movement.
The ID tag consists of a three-axis acceleration sensor (model MMA7260, an Atmega 16 L running at 8 MHz maximum clock speed and an RFID tag with 915 MHz range) and a built-in battery with an ID tag mass of 64 g including a battery. Figure 1 shows a user manipulating the prototype ID tag (Eindhoven, Netherlands) running at 8 MHz maximum clock speed and an RFID tag with 915 MHz range.

Even though signals from the haptic gestures are acquired with a duration ranging approximately from 600 ms to 3100 ms (Table 1), the inference algorithm needs only the signals for the first 50 samplings, which last for about 1500 ms, to differentiate and classify the haptic gestures with high enough accuracy and efficiency.

Users can combine these various haptic gestures to make a multiple-digit passcode with a minimum latency of 1750 ms between patterns. The minimum latency is the duration required for the processing of the first 50 samplings of signal plus the inter-pattern interval.

During the first phase of the algorithm, the moving average of the ith data point for each axis is calculated as follows: if \( a_i \) denotes the moving average of the \((i - 9)\)th through ith data points from the \(a\) axis, then

\[
a_i = \frac{\sum_{k=i-9}^{i-1} k - \text{th raw data of } a\text{-axis}}{n}, \; n \leq i
\]  

where \( n \) is the minimum number of data points to calculate the moving average (the default for which is set at 10).

The normalized moving average of the data for each axis is calculated as follows.

Assuming that \( N_a \) denotes a normalized value of the \(a\)-axis data and that \( a_i \) denotes the moving average of the \(a\)-axis data, then

\[
N_a = \frac{a_i - \mu}{\sigma}
\]

where \( \mu \) denotes the average value and \( \sigma \) refers to the standard deviation during the initial \( t \) seconds (where \( t \) is set at 5). In order to detect the starting point of sampling for 50 data points, a specific data point \( N_z \) is used and is given through the normalization process, since the most sensitive axis of the acceleration sensor during the haptic manipulations seems to be the \( z \) axis.

**Figure 2.** Sample moving average plots: (a) Plots of the raw acceleration sensor signals from five axes for the “tapping (TAP), shaking (SHK), horizontal flipping to right (HFR), horizontal flipping to left (HFL), vertical flipping at 90 degree (VF90), vertical flipping at 180 degree (VF180), turning over (TO)” sequence when the system was embedded in an ID tag; (b) Plots of rearranged normalized signal plots for the same seven haptic gestures.

- **(a)**
- **(b)**
In the second phase of the classification algorithm, comparisons are made for each pattern between the acquired normalized value from each axis and the learned pattern information. The decision tree method is used to classify the patterns as follows.

We assume that axis a and axis b denote arbitrary axes among the x, y, z, x–z, and y–z axes. The decision procedure then becomes the following:

```plaintext
if (Pr_interaction\text{axis}_a \geq \text{Threshold}_\text{level}[k]){
    \text{change } k \text{ through predefined rule;}
    \text{if (Pr_interaction}\text{axis}_b \geq \text{Threshold}_\text{level}[k]) {
        \text{type_of_interaction} = \text{haptic_interaction}[k];
        \text{break;}
    }
    ...
} else ...
```

where,

\[\text{arrayN}_l = \text{set of all normalization data of } l\text{ – axis}
\]
\[\text{with size of DATA_SIZE}
\]
\[
S = \{ k \in \text{arrayN}_l | \text{Thr}_{\text{low}}[k] < k < \text{Thr}_{\text{high}}[k] \}
\]
\[
\text{Pr}_\text{interaction}_l = \frac{|S|}{\text{DATA_SIZE}}
\]

*Threshold_value*[k]: k-th probability values learned from the 250 trials to branch.

*Thr_low*[k], *Thr_high*[k]: the kth upper or lower range value of the l axis in order to decide type_of_pattern or branch.

*haptic_pattern*[k]: name of the kth haptic pattern.

The normalized values on all of the five axes were different among the seven haptic gestures shown in Table 1. For example, all the data from the 250 points had a distribution with normalized probability values of \(-90 \leq N_z \leq 90\). The range of normalized probability for each haptic pattern was calculated from the previous phase. The classification algorithm categorizes the seven haptic gestures based on the difference of each signal in the normalized probability distribution range on the five axes from the acceleration sensor.

For example, to classify a TO pattern, the initially gathered acceleration data of each axis sequentially go through a moving average and normalization process. After this process, using the resulting \(N_z\) value, a pattern is determined to have either occurred or not. In this process, termed Phase 1, the predefined \(\text{Thr}_{\text{low}}\) and \(\text{Thr}_{\text{high}}\) values are set to \(-90\) and \(90\), respectively (Figure 3a). If this process returns true, the sensor data of each axis are gathered to the \(\text{DATA_SIZE}\) limit and then classified in Phase 2. In order to classify a TO pattern during the first stage of Phase 2, the \(\text{Pr}_{\text{interaction}}\text{z}\) value is set to 0.4 in the range of \(\text{Thr}_{\text{low}}[k] = -70, \text{Thr}_{\text{high}}[k] = -15\) (Figure 3a). In the second stage of Phase 2, the \(\text{Pr}_{\text{interaction}}\text{x}\) value is set to 0.8 in the range of \(\text{Thr}_{\text{low}}[k] = 0, \text{Thr}_{\text{high}}[k] = 20\) (Figure 3b). Through this process and using the predefined threshold values, a TO pattern can be classified effectively from a gathered raw data set.
Algorithm 1. Pseudocode of the authentication algorithm: (a) Phase 1. Detecting effective gestures; (b) Phase 2. Classification of the seven haptic gestures

(a) Phase 1: Algorithm for detecting effective gestures

**Input:** a piece of raw data from each of the five axes of the acceleration sensor  
**Output:** TRUE or FALSE. TRUE when an effective gesture has been detected  
**Definition of variable in Phase 1:**  
`Thr_low`,`Thr_high`: threshold values in order to search a starting point of haptic gesture  
t: the duration for initial data gathering. Default is 5 seconds  
HZ: Sampling frequency of the gathered data per sec

While(t*HZ) {  
  Gather current x, y, z, x–z, and y–z axis data from the sensor;  
  Calculate moving average of z axis;  
  Normalize the calculated moving averages and store to `Nz`;  
  if!(Thr_low < Nz < Thr_high)  
  Return TRUE //effective gesturedetected!  
}

(b) Phase 2: Gesture classification algorithm

**Input:** a piece of raw data from each of the five axes of the acceleration sensor  
**Output:** classified haptic pattern  
**Definition of variable in Phase 2:**  
`DATA_SIZE`: the number of data to discriminate the seven haptic gestures (default is 50)  
for(i = 0; i < `DATA_SIZE`; i++) {  
  Gather current x, y, z, x–z, and y–z axis data from the sensor;  
  Calculate moving average of x, y, z, x–z, and y–z;  
  Normalize the calculated moving averages and store to `Nx`, `Ny`, `Nz`, `Nx-z`, and `Ny-z`;  
  array`N_x`[i] = `N_x`;  
  array`N_y`[i] = `N_y`;  
  array`N_z`[i] = `N_z`;  
  array`N_y-z`[i] = `N_y-z`;  
  array`N_x-z`[i] = `N_x-z`;  
}  

Decide the type of gesture by comparing `arrayN_x`, `arrayN_y`, `arrayN_z`, `arrayN_y-z`, `arrayN_x-z` to the predefined pattern information of each gesture;  
Return type of gesture;  
}
were collected. A standby status. The passcode was then decomposed into unit haptic gestures and compared with an average age of 26.4, tried to generate a passcode through haptic manipulation of the ID tag to performance in a laboratory. A regular ID tag with an RFID tag provided a convenient platform for implementation on the assumption that users in the intelligent and automated environment need to carry an ID tag as a means of personal identification. Fifteen college students, eleven of them male, with an average age of 26.4, tried to generate a passcode through haptic manipulation of the ID tag to successfully access the authentication system. No repetition of the same gesture was allowed for creating a passcode. Participants were allowed to have at least 10 min to practice generating all four-digit passcode, composed of four different haptic gestures from the final set shown in Table 1, that matched the passcode they predefined and stored using the ID tag. The acceleration sensor generates signals according to the patterns until the user stops the gesture to return to the normal, in other words, a standby status. The passcode was then decomposed into unit haptic gestures and compared to the preselected gestures according to the algorithm described in Section 3.3. A total of 150 trials were collected.

4. User Performance and Usability

4.1. Experimental Setup

The proposed haptic passcode authentication system was implemented and tested for its performance in a laboratory. A regular ID tag with an RFID tag provided a convenient platform for implementation on the assumption that users in the intelligent and automated environment need to carry an ID tag as a means of personal identification. Fifteen college students, eleven of them male, with an average age of 26.4, tried to generate a passcode through haptic manipulation of the ID tag to test for successful access to the authentication system.

Participants first created and predefined their own four-digit passcode by designating four gestures in succession out of the seven haptic gestures provided and stored them in the authentication system. No repetition of the same gesture was allowed for creating a passcode. Participants were to match this stored passcode with their haptic gestures with an ID tag to successfully access the authentication system. Participants were allowed to have at least 10 min to practice generating all seven haptic gestures before the test. During the test, participants were asked to perform ten times the four-digit passcode, composed of four different haptic gestures from the final set shown in Table 1, that matched the passcode they predefined and stored using the ID tag. The acceleration sensor generates signals according to the patterns until the user stops the gesture to return to the normal, in other words, a standby status. The passcode was then decomposed into unit haptic gestures and compared to the preselected gestures according to the algorithm described in Section 3.3. A total of 150 trials were collected.

4.2. Results

4.2.1. System Accuracy

The system accuracy was analyzed out of 150 trials in terms of success and failure using a confusion matrix. The levels of recognition accuracy of each haptic gesture and confusion with each other are presented in Table 2.
Table 2. Confusion matrix for recognition accuracy of the haptic gestures using the ID tag.

| Recognized Pattern | TAP | SHK | HFR | HFL | VF90 | VF180 | TO |
|--------------------|-----|-----|-----|-----|------|-------|----|
| TAP                | 95.3| 0   | 0   | 0   | 0    | 0     | 0  |
| SHK                | 0   | 92.7| 0   | 0   | 0    | 0     | 0  |
| HFR                | 0   | 0.7 | 92.0| 9.3 | 0    | 0     | 10.0|
| HFL                | 0   | 0   | 88.0| 0   | 94.0 | 7.3   | 0  |
| VF90               | 0   | 0   | 0   | 0   | 0    | 74.0  | 0  |
| VF180              | 0   | 0   | 0   | 0   | 0    | 0     | 82.0|
| TO                 | 0   | 0   | 0   | 0   | 0    | 0     | 82.0|
| No Response        | 4.7 | 6.7 | 8.0 | 2.7 | 6.0  | 18.7  | 3.3|

The average rate of successful recognition for the four-digit haptic passcode authentication was 88.9%. Due to the difficulty in haptic manipulation of the ID tag, some haptic gestures showed lower accuracy than others. For example, the vertical flip of 180 degrees (VF180) and turning over (TO), which require 180-degree horizontal flipping manipulation, seemed to be difficult for the participants to make. Participants tended to think they flipped the tag enough for 180 degrees even though they actually flipped the tag for less than the required threshold. The VF180 gesture was prone to errors and being mistakenly recognized as vertical flip of 90 degrees (VF90) or as some other undefined pattern. Since the haptic gesture of complete TO takes longer duration compared to the other gestures, it can accidentally be recognized as a horizontal flipping in the case when users make the motion too rapidly or too slowly. The TO gesture includes flipping manipulations in both the left and right directions. It showed rather high ratios of confusion with both horizontal flipping of 90 degrees to the right (HFR) and horizontal flipping of 90 degrees to the left (HFL). The haptic gestures that resulted in no response occurred when gestures were made too rapidly, causing a lack of sufficient signal accumulation for sampling.

4.2.2. User Preference Evaluation

Some haptic gestures were preferred by the participants above others. To test the usability of the haptic passcode, we performed a second test with the same participants on user preference of haptic gestures used to construct the passcode.

Firstly, we asked the participants to construct a personal passcode in the range of three to six digits and examined their preferences. Participants were allowed to use same gestures repetitively to make the passcode. The numbers of each haptic gesture used to construct each digit were counted out of the total 270 digits. It was found that the favorite gesture for making a haptic passcode with the ID tag by the participants was HFR followed by TAP and HFL. The least preferred haptic gesture was TO, followed by shaking (SHK) and VF180. The participants tended to avoid those patterns which require relatively bigger motion and take a longer time to make. The TO and VF180 gestures were the ones with both lower recognition accuracies and lower preference by the participants among all the gestures. The preference of each gesture used to construct a passcode is shown in Table 1.

The average time taken to complete a passcode input linearly increased with the number of digits made with the gestures. It was observed that the average time to completely input six digits of a passcode was more than 19 s while the estimated time based on latency calculation was approximately 10 s (Figure 4). The difference can be explained in two ways. First, the average completion time is composed of the system response time and the time taken for user recognition of the system confirmation since the participants needed to pause until the system confirmed the user input with visual, auditory, or tactile feedback before making a gesture for the next digit. The other reason may be the burden of memory. As the passcode included more digits to construct, participants seemed to need more time to retrieve their passcode combinations. The required time to complete the six-digit passcode
increased more rapidly as a result. The participants suggested that the time to input a passcode took too long for the system to recognize and needs to be faster.

![Figure 4. Measured and estimated times for completion of haptic passcodes with various digit lengths.](image)

### 4.2.3. Copying Attack Experiment

For an authentication system to be reliable and successful, it needs to be difficult for others to copy and intrude into the system illegally. It is always the dilemma for designers to decide between usability and security.

From the previous experiment of constructing passcodes with various digits, participants responded that they did not have problems with the ID tag passcode construction except for some particular gestures with low accuracy, such as the TO gesture.

The extent of easiness to copy a haptic passcode was examined by asking the participants to copy the others’ passcodes by watching from the side. Each participant was asked to watch another participant making a passcode from the right side at a 90 degree angle and 2 m away, and to reproduce the observed passcode 10 s later. The participant was informed the number of digits that the other participant was making before every trial.

Figure 5 shows the success rate of copying the other’s code, and Table 2 shows the confusion matrix in the copying situation. It was considered as a failure if any one digit was not correctly matched with the intended passcode. In the three-digit passcode cases, almost 85% of participants successfully copied. However, the success rate decreased dramatically as the number of digits increased. For the six-digit passcode, the success rate dropped below 30%.

It was found from the interview sessions with the participants that the TO gesture was the most difficult to copy while the HFL was the easiest to copy. The TAP gesture was the second most difficult to duplicate for the copying attackers because the gesture was made too quickly and too simply to be recognized as a concrete gesture from the copier’s viewpoint.
The implementation of multilayered security systems will definitely require greater computational cost and more complicated configurations [12]. In this study, we proposed an authentication system that uses a personal ID tag equipped with an embedded acceleration sensor and an RFID tag. In the suggested system, users could generate a passcode via haptic manipulation of the ID tag to present not only the possession of a physical token for identification but also a personal code for access. The classification algorithm and the software breathe life into an otherwise ordinary personal ID tag to make it a useful authentication tool. The passcode for authentication does not have to be in alphanumeric format but rather is presented as a certain pattern of haptic manipulation of the ID tag. From a user’s point of view, the most natural way to interact with a computerized system would be through either a speech or gesture interface. Even though gesture-based authentication has been criticized as being vulnerable to attackers since human actions are the weakest link in the authentication chain [25] and the gestures innately provide visual feedback to attackers [18], manipulating an ID tag hanging on the chest to generate secret patterns basically blocks shoulder surfing from behind.

It was also proved in this study that the haptic gestures were difficult enough to resist being copied and replayed by attackers when enough digits were used to create the passcode. Considering the fact that the attackers watched the gestures manipulating the ID tag wide open from the side with no barriers at all, the results of the copying attack experiment can be said to be encouraging and positive. With the current trends of making passwords more complicated using both alphanumeric text and symbols to make passwords long enough, for example, almost 10 characters, applying more than 6 digits of haptic gestures would provide good-quality passcodes for authentication purposes.

According to Hayashi et al. [26], an ideal authentication system needs to provide features such as no unauthorized access, universal use, limited scale, minimal training, rapid setup, rapid authentication, low error rates, and high memorability. The proposed haptic authentication meets many of these requirements, particularly security, universal use, limited scale, minimal training, low error rates, and high memorability. The proposed system, however, could not meet an important requirement in terms of rapid authentication, and needs to be improved.

The suggested system was made to be simple, using a personal ID tag as a portable accessory that is omnipresent in today’s corporate environment, so that the actions of manipulating the device make the recognition and classification processes easier and seamless. Therefore, inconvenient authentication processes of explicitly scanning a personal object or typing in a personal password can be removed [27]. In addition, since the accelerator sensor is relatively cheap, although it requires additional battery...
support, the cost to set up the required infrastructure to support an authentication system can be minimized using the suggested authentication system.

5.2. Mobile Application

The same haptic authentication algorithm can be applied to personal devices such as smartphones which are equipped with a built-in acceleration sensor. With the widespread use of acceleration sensors these days, a mobile phone may be a good alternative to a traditional ID tag in terms of security [27]. We briefly tested the same authentication system on a mobile phone (Galaxy Note 8 model by Samsung (Seoul, Korea) with 6.3 inch display, 2960 × 1440 resolution) to test system validity with the same participants who engaged in the copying attack experiment. Just like in the ID tag cases, the haptic manipulation for the VF180 (vertical flip of 180 degrees) gesture was difficult to make with a mobile phone. Manipulation of a mobile phone with the required haptic movement needs one hand to firmly grab the phone, not like when an ID tag is hung on the neck, with the other hand to tap, flip, and shake. Since manipulation of a mobile phone was much more difficult to do than that of an ID tag, VF90 and VF180 needed to be replaced with VF45 (for 45 degrees) and VF90, respectively, to enhance the accuracy. Even though the signals were different from those from an ID tag in form and duration, the same algorithm could still be applied to classify the haptic gestures.

Many smartphones today are embedded with an acceleration sensor and durable battery for a variety of functions. Smartphones seem to be a good candidate for a functional device to be used as a personal tool for authentication process. It has been proved that discrete gesture patterns are hard for users to retain [12], and attackers would have a hard time distinguishing and memorizing another user’s haptic manipulations of their phone. Since the haptic manipulations of a phone look very similar to each other, they are difficult for attackers to figure out and to reconstruct.

People with physical disabilities who cannot make precise manual inputs into mobile phones due to the small keypad can take advantage of the simple haptic manipulations to enter a personal passcode with the proposed system, even though they may need much longer to make a passcode.

5.3. Future Studies

We previously demonstrated the possibility and usability of ID tags in interaction with computerized systems [27–29]. The following problems for the proposed authentication scheme using an ID tag need to be solved in order for it to be an effective and efficient authentication system in real practices.

First, controlling the battery power more efficiently for the ID tag needs to be resolved since the system cannot be powered on all the time. It would be a much more efficient system if the power turns on only when the authentication process is to be started [28,29].

Second, a more efficient way of processing the signal is needed for the system to be improved in terms of usability. The latency for each haptic gesture currently needs to be long, with 1500 ms needed to obtain enough signals to be classified. There needs to be another 1000 ms latency between each haptic gesture in addition for reliable data gathering. Users would expect the authentication procedure to be completed as fast as finger scanning or password typing on a keyboard. To make the authentication system usable and convenient, the latency between each haptic gesture should be far less than one second at maximum while maintaining the current accuracy level. At the same time, the diversity of gestures needs to be improved for the authentication process to make the system more secure. With at least ten distinct and concrete haptic gestures, the current system can completely replace any authentication system that uses a numeric key input for passwords as each gesture can be mapped to each Arabic number for the complete input. Furthermore, additional gestures will make it harder for copying attackers to replay the haptic passcode.

Third, the classification rates of some difficult-to-make haptic gestures, such as the VF180 gesture, need to be improved. Those gestures should be generated with higher classification rates from a
less-strictly-defined range of motions. Limited choices in haptic gestures and potentially frequent 
errors are possible reasons for users to avoid the suggested system of making haptic passcodes. 

Further studies are in progress to make a secured authentication system by adding additional 
haptic gestures to the current structure, for example, “double tap” and “rotation” of the ID tag. Another 
study is also underway to improve the user customization by utilizing unique personal characteristics 
during haptic gestures. Personal biometric characteristics such as the speed of manipulation, the 
location to tap and hold, and the force grabbing the ID tag can be extracted by observing the behaviors 
of each user over an extended period of time, and these may provide a lead to finding personal habits 
and preferences. Haptics can provide rich data for extracting unique personal characteristics, just like 
biometric data, such as fingerprints, facial patterns, and irises, which are also used for authentication 
and identification purposes [30]. Those extracted characteristics can be used to make more personal 
and secure haptic passcodes. Such personal factors uniquely characterizing the user can add another 
layer of security to prevent security breakdown by attackers [15,17,19–23].

Author Contributions: Conceived the concept and surveyed references, S.L.; Designed and performed the 
experiments, S.L., K.S.; Analyzed the data, S.L., K.S., S.K.; Wrote the original draft, S.L., S.K.; Edited the paper, S.K.

Funding: This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the Grand 
Information Technology Research Center support program (IITP-2019-2015-0-00742) supervised by the IITP 
(Institute for Information & communications Technology Promotion).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ayoade, J. Security implications in RFID and authentication processing framework. Comput. Secur. 2006, 25, 
207–212. [CrossRef]
2. Feldhofer, M. An authentication protocol in a security layer for RFID smart tags. In Proceedings of the 12th IEEE 
Mediterranean Electrotechnical Conference (IEEE Cat. No. 04CH37521), Dubrovnik, Croatia, 12–15 May 2004; pp. 759–762.
3. Hwang, I.-K.; Baek, J.-W. Wireless access monitoring and control system based on digital door lock. IEEE 
Trans. Consum. Electron. 2007, 53, 1724–1730. [CrossRef]
4. Bardram, J.E.; Kjær, R.E.; Pedersen, M.O. Context-aware user authentication–supporting proximity-based 
login in pervasive computing. In Proceedings of the International Conference on Ubiquitous Computing, 
Seattle, WA, USA, 12–15 October 2003; pp. 107–123.
5. See, J.; Lee, S.-W. An integrated vision-based architecture for home security system. IEEE Trans. Consum. 
Electron. 2007, 53, 489–498. [CrossRef]
6. Langheinrich, M. RFID and privacy. In Security, Privacy, and Trust in Modern Data Management; Springer: 
Berlin, Germany, 2007; pp. 433–450.
7. Jabbar, H.; Jeong, T.; Hwang, J.; Park, G. Viewer identification and authentication in IPTV using RFID 
technique. IEEE Trans. Consum. Electron. 2008, 54, 105–109. [CrossRef]
8. Park, S.; Locher, I.; Savvides, A.; Srivastava, M.B.; Chen, A.; Muntz, R.; Yuen, S. Design of a wearable sensor 
badge for smart kindergarten. In Proceedings of the Sixth International Symposium on Wearable Computers, 
Seattle, WA, USA, 10 October 2002; pp. 231–238.
9. Patel, S.N.; Pierce, J.S.; Abowd, G.D. A gesture-based authentication scheme for untrusted public terminals. 
In Proceedings of the 17th Annual ACM Symposium on User Interface Software and Technology, Santa Fe, 
NM, USA, 24–27 October 2004; pp. 157–160.
10. Villar, N.; Schmidt, A.; Kortuem, G.; Gellersen, H.-W. Interacting with proactive public displays. Comput. 
Graph. 2003, 27, 849–857. [CrossRef]
11. Zuo, F.; de With, P. Real-time embedded face recognition for smart home. IEEE Trans. Consum. Electron. 
2005, 51, 183–190.
12. Chong, M.K.; Marsden, G. Exploring the use of discrete gestures for authentication. In Proceedings of the 
IFIP Conference on Human-Computer Interaction, Uppsala, Sweden, 24–28 August 2009; pp. 205–213.
13. Mayrhofer, R.; Gellersen, H. Shake well before use: Authentication based on accelerometer data. In Proceedings of the International Conference on Pervasive Computing, Toronto, Canada, 13–16 May 2007; pp. 144–161.

14. Liu, J.; Zhong, L.; Wickramasuriya, J.; Vasudevan, V. User evaluation of lightweight user authentication with a single tri-axis accelerometer. In Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services, Bonn, Germany, 15–18 September 2009; p. 15.

15. Orozco, M.; Asfaw, Y.; Shirmohammadi, S.; Adler, A.; El Saddik, A. Haptic-based biometrics: A feasibility study. In Proceedings of the 2006 14th Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems, Alexandria, VA, USA, 25–26 March 2006; pp. 265–271.

16. Iglesias, R.; Orozco, M.; El Saddik, A. Haptics for recognizing and quantifying hand movement patterns for authentication. In Proceedings of the 2007 IEEE International Symposium on Intelligent Signal Processing, Alcala de Henares, Spain, 3–5 October 2007; pp. 1–6.

17. Alsulaiman, F.A.; Cha, J.; El Saddik, A. User identification based on handwritten signatures with haptic information. In Proceedings of the International Conference on Human Haptic Sensing and Touch Enabled Computer Applications, Madrid, Spain, 10–13 June 2007; pp. 114–121.

18. Cain, A.A.; Chiu, L.; Santiago, F.; Still, J.D. Swipe authentication: Exploring over-the-shoulder attack performance. In Advances in Human Factors in Cybersecurity; Springer: Berlin, Germany, 2016; pp. 327–336.

19. Pozo, A.; Fierrez, J.; Martinez-Diaz, M.; Gallbally, J.; Morales, A. Exploring a statistical method for touchscreen swipe biometrics. In Proceedings of the 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 23–26 October 2017; pp. 1–4.

20. Antal, M.; Szabó, L.Z. Biometric authentication based on touchscreen swipe patterns. Procedia Technol. 2016, 22, 862–869. [CrossRef]

21. Song, Y.; Cai, Z.; Zhang, Z.-L. Multi-touch authentication using hand geometry and behavioral information. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 357–372.

22. Meng, W.; Li, W.; Wong, D.S.; Zhou, J. TMGuard: A touch movement-based security mechanism for screen unlock patterns on smartphones. In Proceedings of the International Conference on Applied Cryptography and Network Security, Guildford, UK, 19–22 June 2016; pp. 629–647.

23. De Luca, A.; Hang, A.; Brudy, F.; Lindner, C.; Hussmann, H. Touch me once and i know it’s you!: Implicit authentication based on touch screen patterns. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Austin, TX, USA, 5–10 May 2012; pp. 987–996.

24. De Luca, A.; Denzel, M.; Hussmann, H. Look into my eyes!: Can you guess my password? In Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, CA, USA, 15–17 July 2009; p. 7.

25. Kumar, M.; Garfinkel, T.; Boneh, D.; Winograd, T. Reducing shoulder-surfing by using gaze-based password entry. In Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 18–20 July 2007; pp. 13–19.

26. Hayashi, E.; Dhamija, R.; Christin, N.; Perrig, A. Use your illusion: Secure authentication usable anywhere. In Proceedings of the 4th Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 23–25 July 2008; pp. 35–45.

27. Lee, S.; Song, K.; Choi, J. Access to an automated security system using gesture-based passwords. In Proceedings of the 2012 15th International Conference on Network-Based Information Systems, Melbourne, Australia, 26–28 September 2012; pp. 760–765.

28. Lee, S.; Song, K.; Kim, J.; Choi, J. Ambient widget: An ambient information system using gesture-based interactions. In Proceedings of the 2012 15th International Conference on Network-Based Information Systems, Melbourne, Australia, 26–28 September 2012; pp. 703–708.

29. Lee, S.; Song, K.; Choi, J.; Choi, Y.; Jang, M. Designing a gesture-based interaction with an ID tag. In Proceedings of the 2010 IEEE International Conference on Systems, Man and Cybernetics, Istanbul, Turkey, 10–13 October 2010; pp. 2220–2225.

30. Vetter, R. Authentication by biometric verification. Computer 2010, 43, 28–29. [CrossRef]