Received: 17 April 2022 | Revised: 28 June 2022 | Accepted: 21 July 2022 | Published on: 10 November 2022

DOI: 10.1002/spy2.261

RESEARCH ARTICLE

WILEY

Biometric multi-factor authentication: On the usability of the FingerPIN scheme

Emanuela Marasco | **Massimiliano Albanese** | **Venkata Vamsi Ram Patibandla** | **Anudeep Vurity** | **Sumanth Sai Sriram**

Center for Secure Information Systems, George Mason University, Fairfax, Virginia, USA

Correspondence
Emanuela Marasco, Center for Secure Information Systems, George Mason University, 4400 University Dr, Fairfax, VA 22030, USA.
Email: emarasco@gmu.edu

Funding information
Virginia Research Investment Fund, Grant/Award Number: HN-4Q21-003; National Science Foundation, Grant/Award Number: CNS-1822094

Abstract

Fingerprint-based authentication has been successfully adopted in a wide range of applications, including law enforcement and immigration, due to its numerous advantages over traditional password-based authentication. Despite the usability and accuracy of this technology, some significant concerns still exist, which can potentially hinder its further adoption. For instance, a fingerprint is permanently associated with an individual and, once stolen, cannot be replaced, thus compromising biometric-based authentication. To mitigate this concern, we previously designed a multi-factor authentication approach that integrates Type-1 and Type-3 authentication factors into a fingerprint-based personal identification number (PIN). To authenticate, a subject is required to present a sequence of fingerprints corresponding to the digits of the PIN, based on a predefined secret mapping between digits and fingers. We conducted a preliminary vulnerability analysis and demonstrated that this approach is robust to the compromise of one or more of the subject's fingerprints. The objective of the work presented in this paper is to identify any usability issues for this FingerPIN scheme, collect qualitative and quantitative data through a user study, and determine the participants' satisfaction with the authentication mechanism. We carried out systematic usability tests, designed suitable performance metrics for assessing authentication usability on an initial cohort of 100 individuals, and performed a comparative analysis of the FingerPIN scheme against traditional sequential multi-factor authentication schemes.

KEYWORDS

biometrics, fingerprints, multi-factor authentication

1 | INTRODUCTION

Authentication factors can be classified into three categories: knowledge-based factors (Type-1, something the user knows, such as passwords, PINs and passphrases), ownership-based factors (Type-2, something the user has, such as smart cards, tokens), and biometric-based factors (Type-3, something the user is, known as biometrics, such as fingerprints, iris patterns).[1] Single-factor authentication with a username and password has long been known to be vulnerable to both

social engineering and brute-force attacks, and represents a usability challenge due to the cognitive burden of managing many complex passwords.[2] Biometric authentication is increasingly being adopted to ensure secure access to a variety of devices and applications such as computer network, ATMs, credit card processing, and medical records management. Fingerprints are one of the most accurate and cost effective biometric technology. However, a fingerprint is permanently associated with an individual and, once stolen, cannot be replaced, thus compromising biometric-based authentication. Using these compromised biometrics, attackers can replicate with different presentation attacks (PAs) to circumvent a system by simulating the biometric trait of an authorized user.[3,4,5]

Multi-factor authentication (MFA) uses two or more authentication factors to provide increased security compared to single-factor schemes.[6] Combining multiple factors adds an extra level of protection, making the system more effective, accurate, and reliable.[7] A Type-1 authentication factor (eg, password, PIN) is typically paired with either a Type-2 (eg, token) or a Type-3 authentication factor (eg, fingerprint). Organizations are increasingly transitioning to Multi-Factor Authentication (MFA), requiring users to provide at least two different authentication factors to prove their identity and be granted access to systems. MFA is expected to be the fastest-growing application of biometric technology due to the increasing need to secure system against the theft of sensitive data, especially in government applications. The National Cybersecurity Center of Excellence (NCCoE) recommends the use of MFA on online accounts to mitigate the purchase fraud issue.[8] Widespread smartphone use has also made MFA more prevalent.[6,7,9]

We have recently created a novel MFA system that integrates Type-1 and Type-3 factors into a fingerprint-based personal identification number, referred to as FingerPIN.[10] For the authentication, the system asks the user to provide a finger-digit at a particular position based on the FingerPIN set by the user during the registration phase; this is then verified by the system based on the user's PIN that is stored in the database during the registration phase. The mapping between digits from 0 to 9 to fingers is set during enrollment. Since the mapping between digits and fingers is not predefined but rather determined by the system randomly, an extra layer of protection is added. This system is more robust to compromised fingerprints and brute-force attacks. This approach holds potential to be widely adopted in various government and commercial applications with need to store and secure critical information such as computer network login, important client information, employee records, payroll data, and so forth. This scheme can be implemented on every mobile phone providing users access to credit cards and banking information.[11]

The challenge with MFA is to strike a balance between security and usability. Inadequate accessibility and usability in authentication methods can be a barrier to using important websites, such as tax and benefit services. Unlike one-factor authentication, MFA requires an extra factor; subsequently, users must always carry and maintain the additional device or component, which can lead to loss of the device or exposure of the component.

In our previous work, we designed and assessed a preliminary version of the FingerPIN MFA strategy. The usability and acceptance of the system are also two very important aspects.[12] If the users have difficulty using the system or fail to accept it, the service is likely to fail as well. In the proposed study, we investigate more in-depth the usability of the FingerPIN scheme to promote its adoption. This research study seeks instead to develop a methodology for assessing usability and accessibility of biometric-based MFA systems. The proposed study focuses on gaining a better understanding of the user experience when interacting with an MFA authentication scheme that integrates fingerprints and PINs. We comparatively evaluate the MFA system FingerPIN vs a traditional sequential MFA based on the same two factors fingerprint and PIN verified sequentially.

The main contributions of the work presented in this article are (i) enhancing the FingerPIN scheme by further reducing its vulnerabilities while preserving usability; (ii) designing usability performance metrics for biometric-based MFA schemes; (iii) creating a new database of usability scores generated from the interaction of 100 subjects with a desktop application of the FingerPIN system as well as the traditional MFA scheme involving the two same factors PIN and fingerprint; (iv) assessing and compare the usability of the systems under study and analyze related demographic patterns.

The rest of the paper is organized as follows. Section 2 reviews recent research on biometric-based MFA, whereas Section 3 provides an overview of the specific approach we evaluated in this study. Then, Section 4 presents the performance metrics designed for this study and Section 5 discusses the experimental results. Finally, Section 6 provides concluding remarks and describes possible future work.

2 | RELATED WORK

Prior work on MFA focuses mainly on technological advancements in authentication, while many research questions about system's usability and acceptance remain unanswered.[13] The characteristics of the users are also important for the success of a system.

In 2000, Ashbourn described 12 user characteristics that can influence the performance of a biometric system.[14] Users who are hostile towards the idea of providing biometric information may be more problematic when forced to use biometric devices. Furthermore, familiarity with these devices plays an important role. For example, users familiar with fingerprints will know that the core of the fingerprint contains the most information, so it is important that the core is centered on the biometric reader.

Frokjaer et al defined system's usability in terms of three key factors: efficiency, effectiveness, and satisfaction. The precision and completeness with which users attain certain goals is referred to as effectiveness. Efficiency represents the relationship between the accuracy and completeness with which users attain certain goals and the resources required to achieve them. User satisfaction is defined as the users' comfort level and good attitude towards using a certain system. The relationship between these three metrics are not always correlated and appear to be affected by a variety of factors, including application domain, user context, user experience, and task complexity. Therefore, they must be considered as being independent aspects of usability.[15]

In 2006, Seffah et al proposed the quality in use integrated measurement (QUIM) model as a hierarchical approach for assessing quality factors for interactive software systems, such as classic GUI-style applications and their usability. The most important metrics for evaluating a system's usability are efficiency, which defines a system's ability to enable the use of the available resources; satisfaction that refers to whether or not a user is satisfied while using a system; and learnability defined as the ease for a user to learn how to productively interact with a system.[16]

In 2007, the NIST Biometrics Usability Group conducted a usability test pertaining to the Ten-Print capture.[17] This study was designed to examine the impact of instructional mode on user performance. They examined the impact of poster, video, and verbal instructions on the time required to capture a Ten-Print slap as well as the number of errors incurred during the process For this study a Ten-Print slap capture includes a right slap, left slap and simultaneous thumbs images. The acquisition was performed in a controlled environment. Participants who received instructions via the poster had the most difficulty performing the fingerprinting task. 54% of these participants were unable to successfully complete the fingerprinting process; those who did took longer and committed more errors. The evaluation follows the ISO 9241-11 [ISO], in which usability is defined as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use". The standard identifies three areas of measurement: effectiveness, efficiency, and user satisfaction. The study pertains to the interaction between 300 selected subjects and the biometric recognition system. Participants were 149 males and 151 females with ages ranging from 18 to 65. Each participant was given a satisfaction survey after completing the test. The questions focused on the fingerprint process and the specific instructional mode provided. The questions included in the assessment scheme were related to the effectiveness and clarity of the instructional materials. After completing the user satisfaction survey, participants were asked to repeat the fingerprint collection task that was operated assisted. The operators were critical to the acquisition process. Without the assistance of an operator, 45% of the participants who received the poster were not able to complete the fingerprinting process correctly. While 98% of the subjects were able to successfully complete the collection process, only 78% completed it without assistance. A 39% of the users commented that they were unsure when to remove their hands from the scanner, 14% were unsure where to position their hands on the scanner, and 2% of the participants were concerned about cleanliness.

In 2009, Jackobson et al developed a model for performing implicit authentication on mobile devices, eliminating the need for users to enter passwords. This method authenticates users based on their behavior (common habits, device data, carrier data, location, etc.) and is best suited for portable computers. They observed that implicitly authenticating a user is more cost effective and improves the usability and security of authentication.[18]

In 2012, Trewin et al studied the usability of three biometric authentication modalities on a tablet device. Speaker, face and gesture verification were compared to passwords.[19] Password, face, and gesture were considered more usable than voice. The requirements for voice sample quality did not always match speaking at a comfortable level. Participants disliked the settings where two biometric authentication modalities were used as sequential combination of factors due to high acquisition failure. The system usability scale (SUS) was used as scale for the overall system usability assessment. Each question was answered on a five-point scale ranging from "strongly disagree" to "strongly agree".[19]

In 2017, Lovisotto et al conducted a longitudinal study related to users' attitude towards the adoption of biometric authentication for online payments.[20] They evaluated the usability of a system using five metrics: effectiveness, efficiency, satisfaction, learnability, and memorability. Effectiveness measures the success rate of a certain task performed by the user. Efficiency is the amount of time needed by a user to complete a certain task. Satisfaction captures perceptions and opinions of the user about the system. Learnability is the time taken by a user to learn how to interact with a system. The system's memorability is measured by how familiar a returning user has become with the system. They

found that the users' familiarity and their willingness to adopt biometrics in mobile financial services increased after the survey.

Information fusion in biometrics entails the combination of different sources of evidence and, it has been extensively shown that it is able to enhance the recognition accuracy compared to a biometric system, which exploits only a single source.[21,22,23,24] There is extensive research focused on multi-biometric systems; however, literature lacks usability studies focused on user perspective for multi-biometric systems including those combining multiple instances of the fingerprint modality.

3 | THE SYSTEM UNDER STUDY: ENHANCED FINGERPIN

The FingerPIN system is a MFA scheme that combines Type-1 and Type-3 factors in such a way that a user must *simultaneously* prove knowledge of the PIN and validity of their biometrics features by scanning multiple fingers in a sequence determined by the PIN through a secret mapping between digits and fingers.[10]

The mapping between digits and fingerprints is not predefined, that is, the user does not assign a unique number to each fingerprint during enrollment; instead, a unique number between 0 and 9 is assigned by the system randomly during enrollment to each of the 10 fingers. This random mapping is stored in the database after being generated. The user does not know the mapping. During registration, the fingerprint sequence chosen by the user is transformed into a 5-digit PIN by the system based on the random mapping previously stored in the database. During authentication, the system challenges the user by asking to provide the fingerprint at a particular position. The secrecy of the mapping avoids exposure of this information to attacks during authentication since it could be captured by a malicious user. A system-generated random sequence is more difficult to break. When the user fails to authenticate after three attempts, the system will automatically change the random sequence. Therefore, the system is extremely robust. This characteristic reduces the burden on the user to provide these details about the transformation fingers to digits as an additional input during enrollment.

This scheme involves the execution of enrollment, registration, and authentication tasks. The enrollment module is responsible for storing the reference biometric data into the system database. During this phase, a sensor captures the subject's 10 fingerprints and creates a digital representation of them. This digital representation is then processed by a feature extractor, yielding a more compact representation known as a template. To account for variations in the biometric trait, multiple templates of an individual are typically stored in the database. The reported success probability of brute-force attacks under different scenarios shows that FingerPIN is more secure than using fingerprints or PINs alone, even when one or more fingerprints have been compromised. In scenarios where the attacker steals one fingerprint of the genuine user, the success rate of a brute-force attack against a 5-digit FingerPIN is practically zero. This demonstrates how the integration of the two authentication factors considered in this study overcomes the limitations of both mechanisms, when used in isolation or sequentially. Figure 1 illustrates the information flow of the proposed enhanced FingerPIN system on desktop application used to collect data from subjects while Figure 2 illustrates the traditional sequential MFA on desktop application used for comparison against FingerPIN.

In order to create a more user-friendly solution, we created a prototype to reduce the user's burden. In the enhanced model, during enrollment, the system internally generates a random mapping between the 10 fingerprints acquired from the user and the digits, while in the initial version of the FingerPIN scheme the mapping was entered by the user as additional input. This choice provides improved usability since the user does not need to remember the mapping as well as enhanced security since it avoids exposure to malicious data capture at enrollment time. The mapping can be changed at any time or with a predefined frequency for added security. When using FingerPIN, the individual does not need to move the hand as when entering a PIN since the acquisition of the next finger-digit is accomplished using the same sensing surface while a traditional PIN requires the finger to be pressed on different keys of a keyboard, thus hand movement.

Figure 3 illustrates the architecture of the traditional MFA used in this article for comparison with the enhanced FingerPIN scheme.

It consists of two modules, enrollment and authentication module. During enrollment, the system acquires the biometric templates for the 10 fingerprints that are stored in the database. Furthermore, a random mapping that associate each fingerprint to a digit is generated and such a correspondence is stored in the database as well. During authentication, the system verifies the user's identity sequentially by using the fingerprint as the first factor and the PIN as the second factor.

The user provides all his 10 fingerprints and the user sets a 5 digit PIN. This 5 digit PIN along with his 10 fingerprints are stored in the system database. During the authentication phase the user needs to present his fingerprint as the first

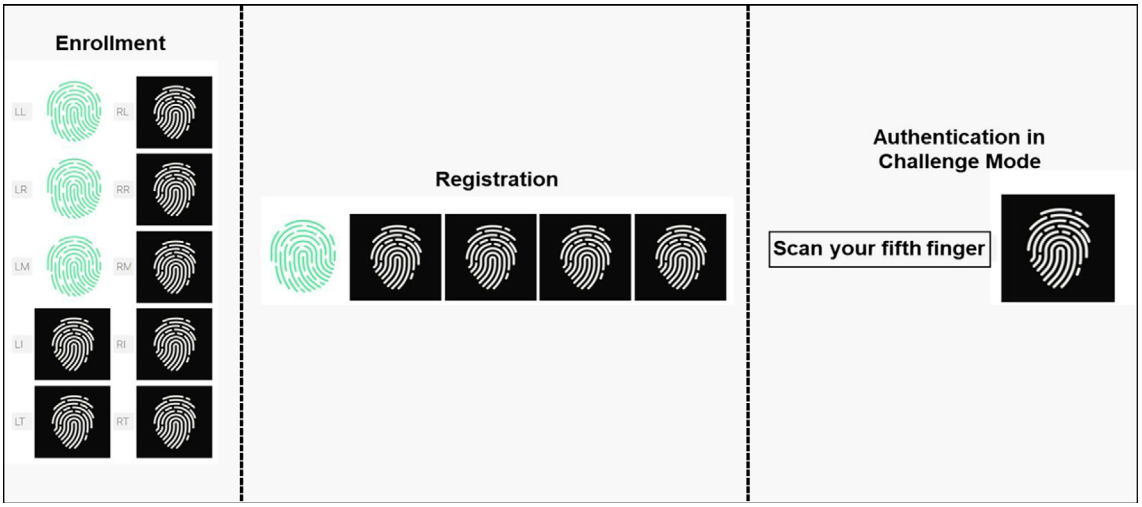

FIGURE 1 FingerPIN desktop application: (A) Enrollment (B) Registration (C) Authentication in challenge mode

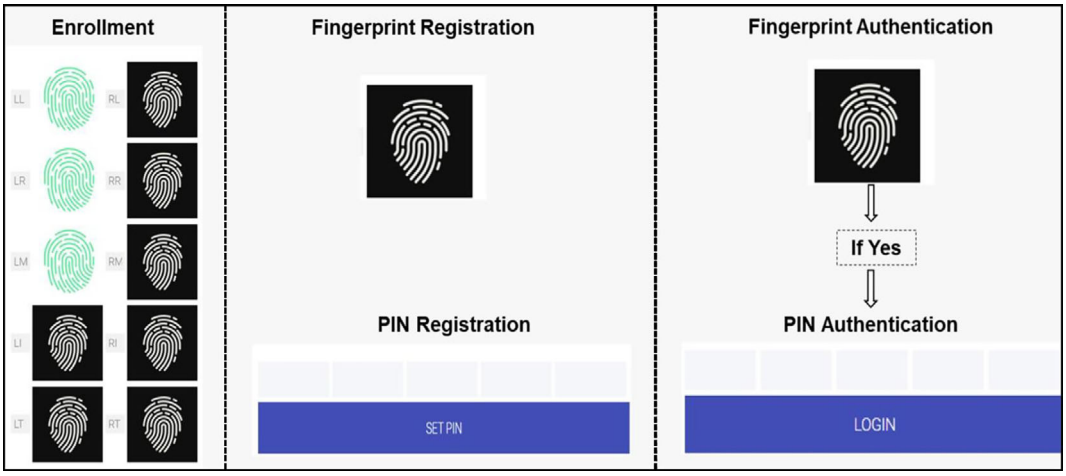

FIGURE 2 The traditional sequential multi-factor authentication (MFA) desktop application: (A) Enrollment (B) Fingerprint and PIN registration (C) Fingerprint and PIN authentication

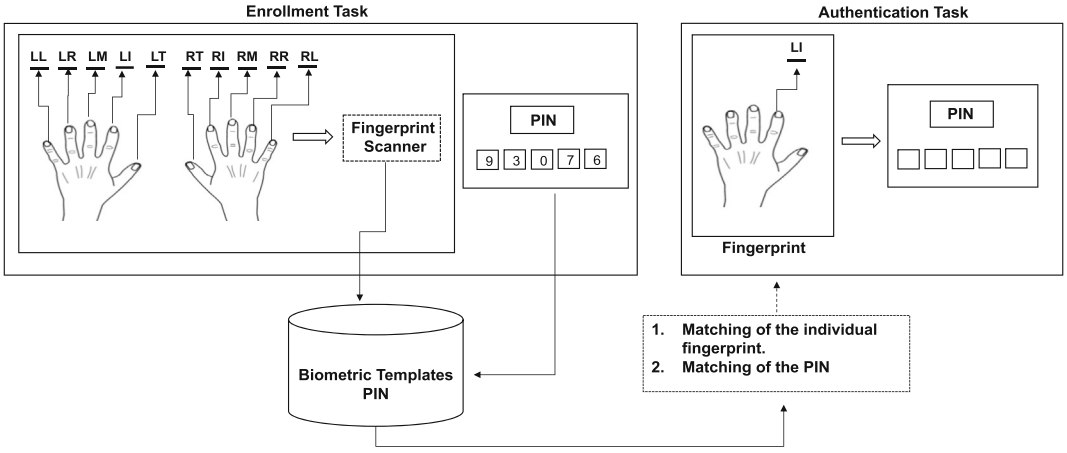

FIGURE 3 The traditional sequential multi-factor authentication (MFA) system mechanism during enrollment and authentication tasks

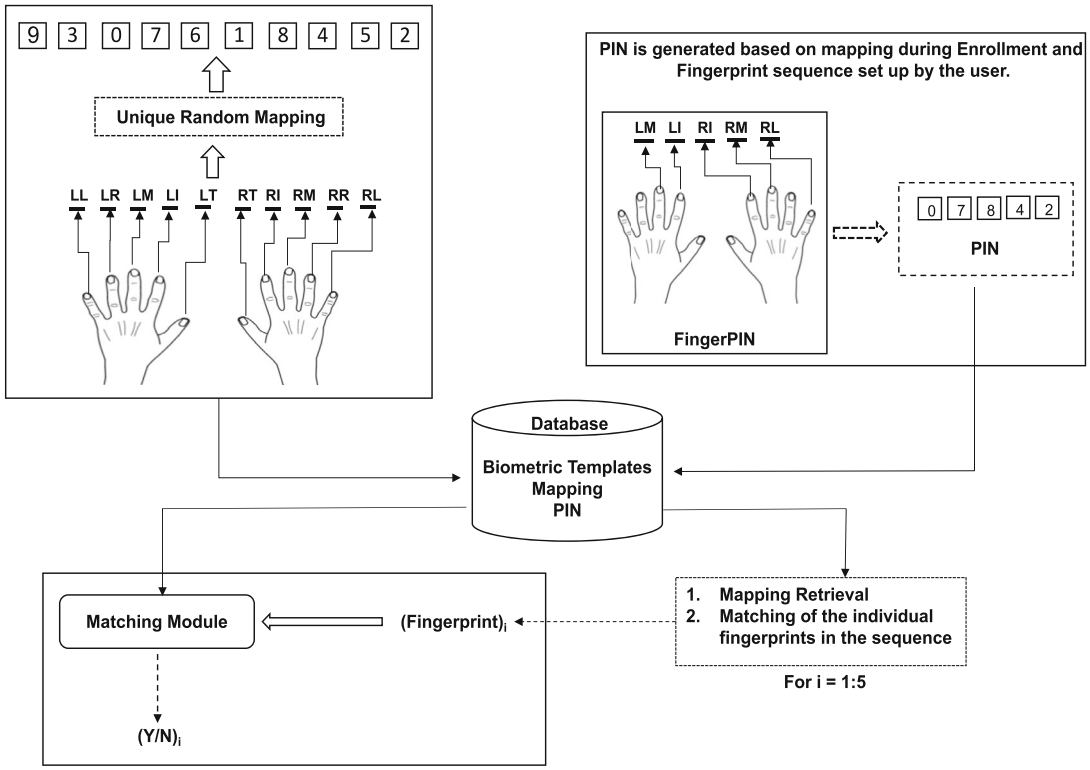

FIGURE 4 The FingerPIN architecture consists of three modules: (1) Enrollment module, (2) Registration module, and (3) Authentication module

factor of authentication and if it is a match, the user's need to enter their 5 digit PIN as the second factor of authentication which was set during enrollment. If both the fingerprint and PIN are matched, the traditional sequential MFA system is successful.

Figure 4 shows more details about the authentication mechanism under study. During enrollment, a sensor captures the subject's 10 fingerprints and creates a digital representation of them which is saved in the database as a reference. The mapping is also randomly generated during this phase and the corresponding digits are stored as well. During registration, the user selects 5 fingers in a certain sequence, which is mapped to 5 digit PIN and stored in the database. During authentication, the user claims his identity, which triggers the system's challenge requiring the user to provide a certain finger-digit of his previously chosen FingerPIN (eg, the third finger-digit). The biometric data is compared to the corresponding template retrieved through the mapping. The match scores were generated using the Neurotechnology VeriFinger matcher 12.2.*

While the user is the only one who can change the FingerPIN, the mapping can be updated automatically by the system administrator periodically (eg, every 2 weeks) or after a certain number AF of consecutive authentication failures. If the authentication fails AF times, the user receives an email with a security code; upon successful verification of the security code, the user can re-register his/her FingerPIN. The user is unaware that the mapping has been modified. The PIN intended as a digit sequence derived by mapping the user's fingerprint sequence (FingerPIN) into the range 0 to 9, is revised as a result of the updated mapping. If the mapping changes, the PIN will change because each fingerprint instance will be assigned to a different digit based on the new mapping.

3.1 | Security assessment of FingerPIN in challenge mode

We discuss the security performance of the FingerPIN system operating in challenge mode when an attacker carries out a brute force attack without knowledge of the 10 genuine fingerprints nor their sequence. Given a FingerPIN, we compute the probability $P(Success)$ that the fingerprint presented by the attacker during a brute-force attack is successfully matched against the challenge, allowing the attacker achieve authentication. Let $P(FM_{ij})$ be the probability of False Match (FM) of

the ith fingerprint used by the attacker against the ith finger-digit of the FingerPIN, with $P(F_{ij})$ indicating the probability that the ith finger-digit maps to digit j, and $\sum_{j=0}^{9} P\left(F_{ij}\right) = 1$. When the system operates in challenge mode, assuming the finger-digits are independent and equally distributed, $P(Success)$ is given by Equation (1).

$$P(Success) = \frac{k}{10} \sum_{j=0}^{9} P\left(FM_{ij}\right) \cdot P\left(F_{ij}\right). \tag{1}$$

$P(FM_{ij})$ is an empirical estimate of probability with which the system incorrectly declares that a biometric sample belongs to the genuine user when the sample belongs to a imposter. The term $\frac{k}{10}$ captures the requirement for the challenge instance to be selected among the fingerprints in the FingerPIN sequence of length k.

4 | THE DESIGNED USABILITY PERFORMANCE METRICS

Usability can be defined in terms of user performance and satisfaction.[8] Usability is not a one-dimensional property of a system; it is a combination of factors including how quickly an experienced user can complete tasks, whether a user can remember how to effectively use the system in future visits, how frequently users make errors while using the system, how users recover from the errors, and whether the user enjoys using the system. The taxonomy in Figure 5 illustrates the various categories of schemes for evaluating authentication usability. In this work, we adopted authentication usability metrics pertaining to objective usability and perceived usability. These metrics are described below.

4.1 | Objective usability

The term objective usability refers to measuring a system's performance, task completion, and duration. It is determined by using the two-performance metrics effectiveness and efficiency, as described below.

- *Efficiency* indicates the time required by the user to complete an authentication task. It is defined as the elapsed time from the moment when the authentication page is opened until the verification of the identity is completed.
- *Effectiveness* is determined by false positive and false negative rates. Indeed, authentication is ineffective if it denies access to a valid user while allowing access to an unauthorized user. In the challenge mode, false acceptance occurs when the malicious user knows the correct position of the stolen fingerprint in the FingerPIN. False rejection occurs when the position of the fingerprint is wrong and or there the matching operation rejects the input.

Because of their quantifiability, efficiency and effectiveness represent usability aspects that are reasonably simple to analyze.

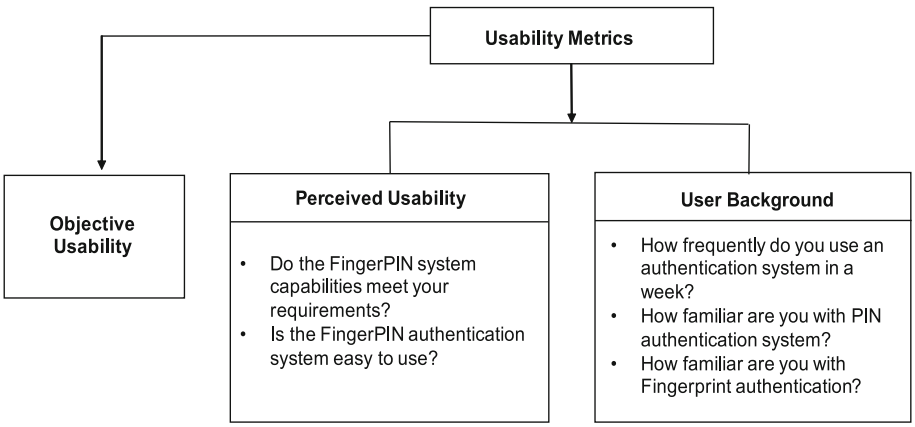

FIGURE 5 Taxonomy of biometric multi-factor authentication (MFA) usability metrics

1. **The users' requirements are met by the FingerPIN System.**

Strongly Disagree				Strongly Agree
1	2	3	4	5

2. **The FingerPIN authentication system is easy to use.**

Strongly Disagree				Strongly Agree
1	2	3	4	5

3. **The users' requirements are met by the traditional sequential MFA system.**

Strongly Disagree				Strongly Agree
1	2	3	4	5

4. **The traditional sequential MFA system is easy to use.**

Strongly Disagree				Strongly Agree
1	2	3	4	5

FIGURE 6 Perceived usability: (1) Strongly disagree; (2) Disagree; (3) Neither agree nor disagree; (4) Agree (5) Strongly agree

4.2 | Perceived usability

The 10-item System Usability Scale (SUS) is a tool for measuring a user's perception of a system's usability. It has been recommended as a standard metric for comparing authentication system usability.[25,26] More study using the SUS to assess authentication is needed, either to build a new, more relevant questionnaire or to decide that the SUS questionnaire is sufficient and/or acceptable. UMUX-LITE is a two-item questionnaire based on the Usability Metric for User Experience (UMUX) questionnaire.[25] It has been shown to have high reliability and validity. A regression-adjusted version called the UMUX-LITEr has been found to correspond closely with the SUS in assessing user satisfaction in a given system. For our study, as shown in Figure 6, we selected two questions from the UMUX-LITE questionnaire items:

- "Does this system's capabilities meet your requirements?", Subjects are asked to respond to a 5 item SUS based on factors such as system uniqueness, performance, security, efficiency, and the speed with which the subject is authenticated.
- "Is this system easy to use?", Subjects are asked to rate a system on a 5 item SUS based on how easy they felt to use a system.
- *Satisfaction* is intended as the subjective responses from users about their feelings when using a system (ie, "Is the system easy to use?"). It describes the user's level of satisfaction with the system's interaction experience. The System Usability Scale (SUS) is the standard for measuring satisfaction through a survey that collects subjects' perspectives. This metric assesses their perceptions of the system's overall usability. As shown in Figure 6, data is usually collected using numeric scale ratings (eg, numeric scales from 1 to 5) through questionnaires.[27]

4.3 | User background

- *Authentication familiarity level* measures, how familiar the user is with authentication systems. It is expressed in terms of how often an individual uses a PIN and/or a fingerprint system in a certain period. The corresponding questionnaire items are described as follows:

  1. "In the past year, how frequently did you use any authentication system in a week?" This question is used to understand how many times in a week during the last year the user has used an authentication system.

  2. "How familiar are you with authentication systems?" This question is used to know the user's familiarity with an authentication system.

3. "How many times do you use Personal Identification Number (PIN) for authentication in a week?" This question determines the subject's familiarity with the Personal Identification Number authentication system.

4. "How many times do you use Fingerprint for authentication in a week?". This question is used to determine the subject's familiarity with the fingerprint authentication system. The familiarity levels used in the proposed study are: *Always*: the subject uses an authentication system more than 2 or 3 times per day; *Often*: the subject uses an authentication system at least once per day; *Sometimes*: the subject uses an authentication system 3 or 4 times per week; *Rarely*: the subject uses an authentication system once or twice per week; *Never*: a subject who never used an authentication system over the past year.

We also included two additional questionnaire items reported as follows: (1) "Which features of the FingerPIN assigned authentication system do you enjoy, and would you like to suggest any change?". This question evaluates which aspect of the proposed FingerPIN system was favored by the subjects over the traditional sequential multi-factor authentication system. (2) "Would you prefer to use the assigned FingerPIN authentication system over traditional sequential multi-factor authentication?". This question assesses which system the subjects prefer between FingerPIN and the traditional sequential MFA.

5 | EXPERIMENTAL RESULTS

5.1 | The dataset

The experiments were carried out using data collected at George Mason University from 100 subjects 18 or older from the Northen Virginia region, including campus students, their families and friends. Demographic information about the subjects was also collected through a separate questionnaire. The age group ranged between 18 and 35 years old for the majority of the subjects, that is, 94%. In terms of ethnicity, 75% of the subjects were Asians, 18% were Asian Americans, and the remaining 7% were South Asians and African American. Regarding gender, 68% of the participants were male, see Figure 7.

The participants were required to submit a survey document as an evaluation of their experience with the two MFA systems under study. The subjects also provided information about their familiarity level with PIN and fingerprint systems alone. Two desktop applications, FingerPIN, and sequential MFA were developed and used by the participants during data collection to provide feedback on the usability of both systems, see Figures 2 and 4. Both systems were explained to the subjects before collecting the information. The order of the first system submitted to the individual was randomized to minimize bias since the interaction with the second system may be easier. A 50 subjects used the FingerPIN system first, while the remaining 50 subjects used the traditional MFA first. The estimated total participation time for each subject is approximately 10 minute.

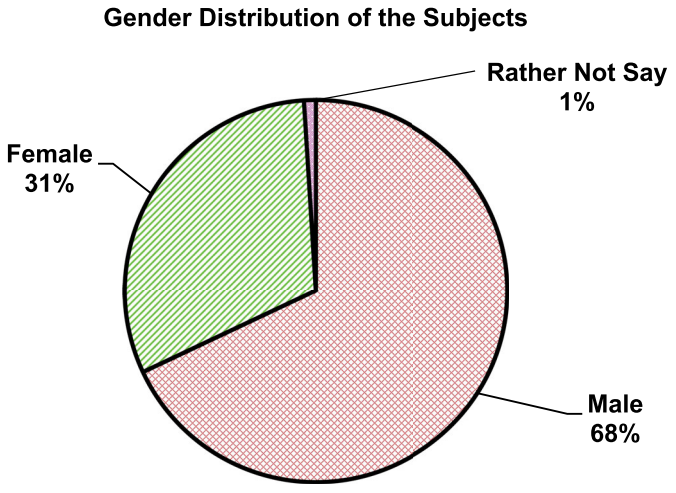

FIGURE 7 Gender distribution of the 100 subjects enrolled in the data collection

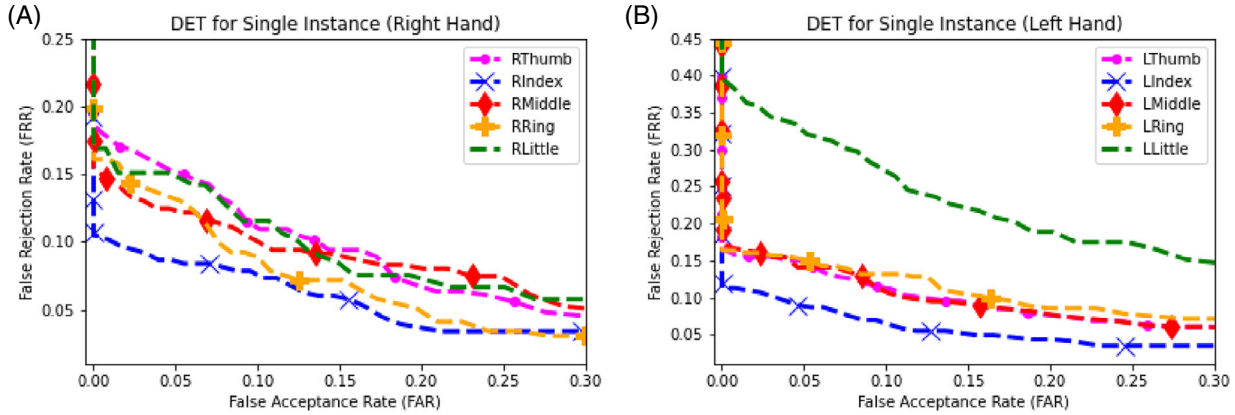

FIGURE 8 Detection error trade-off (DET) curves for the fingerprints of the (A) left and (B) right hand

The proposed system was evaluated using the Futronic FS88H device as the sensing module for enrollment and authentication modules. VeriFinger version 12.2 was used as the matching algorithm in this device. This proposed framework is general; it allows changes in the sensor and/or the matcher modules.

5.2 | Baseline biometric performance

Before discussing usability, we illustrate the baseline performance of the fingerprint system alone by using detection error trade-off (DET) curves. Figure 8A,B show the DET curves for every fingerprint instance of the right and left hand, respectively. In the traditional MFA sequential scheme, if the fingerprint used for authentication is compromised and the PIN is known to the attacker, the security mechanism can be broken. In FingerPIN, if the fingerprint and the PIN have been compromised, the mapping guarantees that the protection mechanism is not be broken.

The data collection aimed to assess user usability, we did not store any fingerprint images as agreed with IRB. The images used for this baseline are taken from the ManTech Innovations Fingerprint Study Phase I collection released to George Mason University by West Virginia University. It contains fingerprints pertaining to 500 subjects acquired using 7 optical sensors. We used images of the 10 fingers acquired using the I3 digID Mini sensor. Among the participants, the 20-33 age groups was the largest, accounting for 61% of the subjects. With respect to ethnicity, Caucasians accounted for 57% of the subjects. There was a nearly equal number of male and female participants with a 51% to 49% ratio. Every subject provided two sets of rolled fingerprints for both hands.

5.3 | Usability results

To carry out the proposed usability assessment, users' backgrounds may play an important role. The pie charts in Figure 9A illustrates the participants' familiarity level with authentication systems, Figure 9B describes how many times in a week an user has interacted with an authentication system during the past year, Figure 9C,D report the PIN and fingerprint use frequency, respectively.

Our analysis shows that in Figure 9A, 69% of the subjects claim that they are highly familiar with authentication systems. A 30% of them are moderately familiar and only 1% of the participants have low familiarity. From Figure 9B, in the past year, 56% of the subjects always used MFA systems in a week, and 35% used it at least once a day. A 6% used MFA on weekly basis and 3% of the participants used it rarely. From this figure, we can also illustrate that every participant used some kind of MFA in a week. In Figure 9C,D, we can see that 58% always use PIN authentication and 43% always use fingerprint authentication in a week. A 23% often use PIN and 23% also use Fingerprint systems during the day. Often usage of both the systems is exclusive to each other. Although there are 10% of the subjects never used the Fingerprint authentication system and every participant used PIN authentication. From the results, we observed that the majority of the subjects are highly familiar with the authentication systems under study and have frequently used MFA last year. In particular, 82% of the subjects uses PIN authentication, and 66% using fingerprint on daily basis.

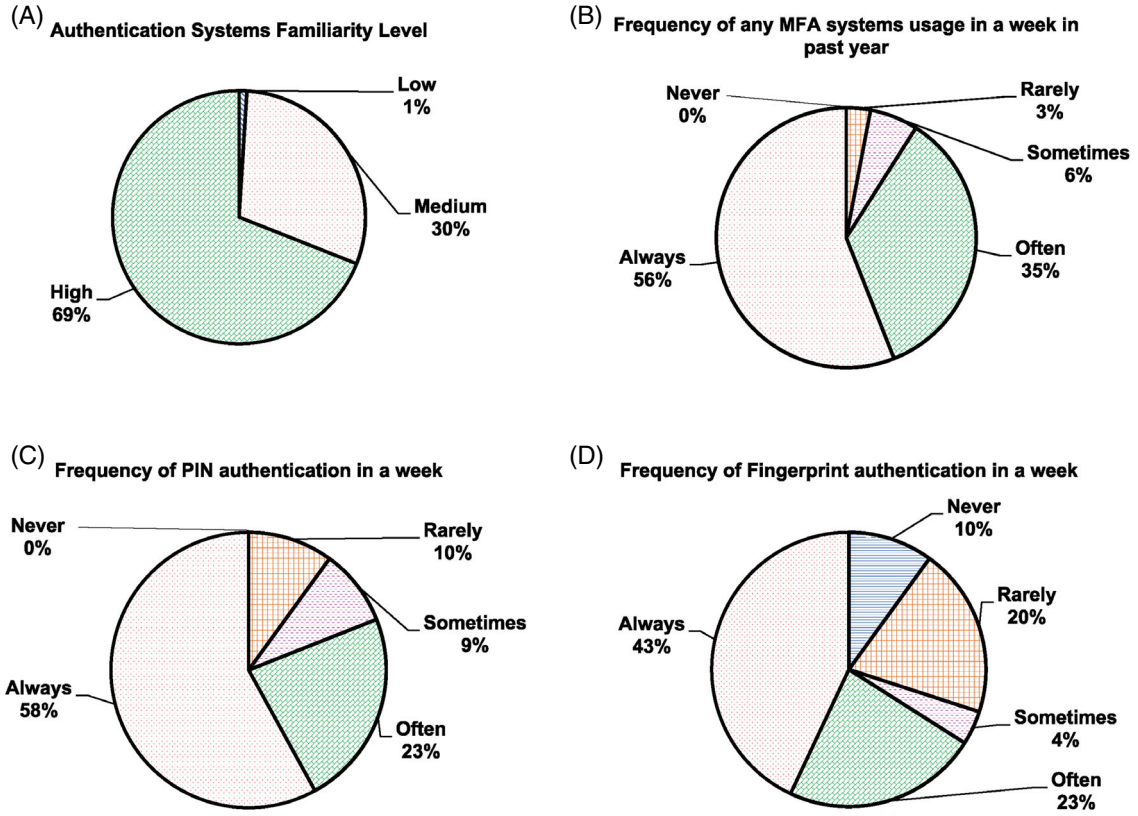

FIGURE 9 The pie charts illustrates the authentication familiarity

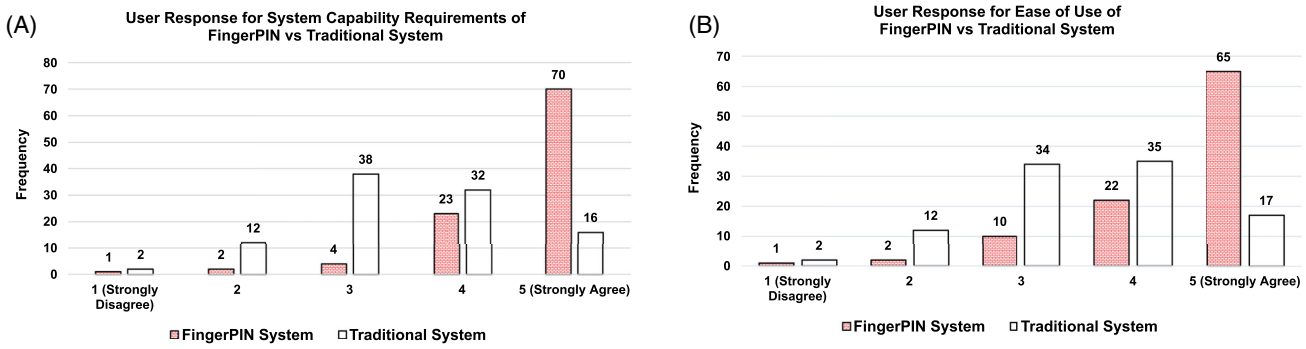

FIGURE 10 Histograms pertaining to the users' responses to perceived usability for both FingerPIN and the multi-factor authentication (MFA) traditional system

Once we gained the knowledge that the familiarity levels of each participant were satisfactory, we proceeded with the perceived usability analysis. The histograms in Figure 10 illustrates the participants' perceived usability. This is expressed in terms of users' responses to the questions "Does the systems meet your requirements?", see Figure 10A and "Are the systems easy to use?", see Figure 10B. From Figure 10A, we can see that 93% of the subjects agreed (with scores 4 and 5) that the FingerPIN system meets the capability requirements, while only 48% of the subjects agreed to sequential MFA. About 3% of the subjects disagreed (with a score of 1 or 2) that the FingerPIN system met their capability requirements. In comparison, 14% strongly disagreed that the traditional system met their capability requirements. Overall, 42% of the subjects were neutral (with a score of 3) with respect to both systems.

The 100 subjects interacted with both systems. When using FingerPIN, 87 out of 100 subjects agreed that the system is easy to use. When using the sequential MFA, only 52 out of 100 subjects considered the system easy to use, see Figure 10B. A 3% of the participants strongly disagreed that using the FingerPIN system was challenging. By contrast, 14% strongly

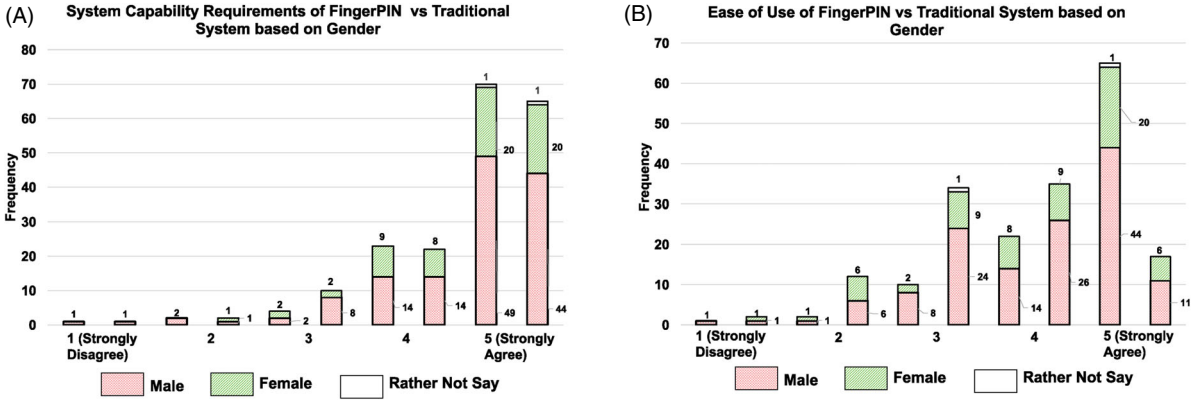

FIGURE 11 Gender impact on the perceived usability of both FingerPIN and the multi-factor authentication (MFA) traditional system

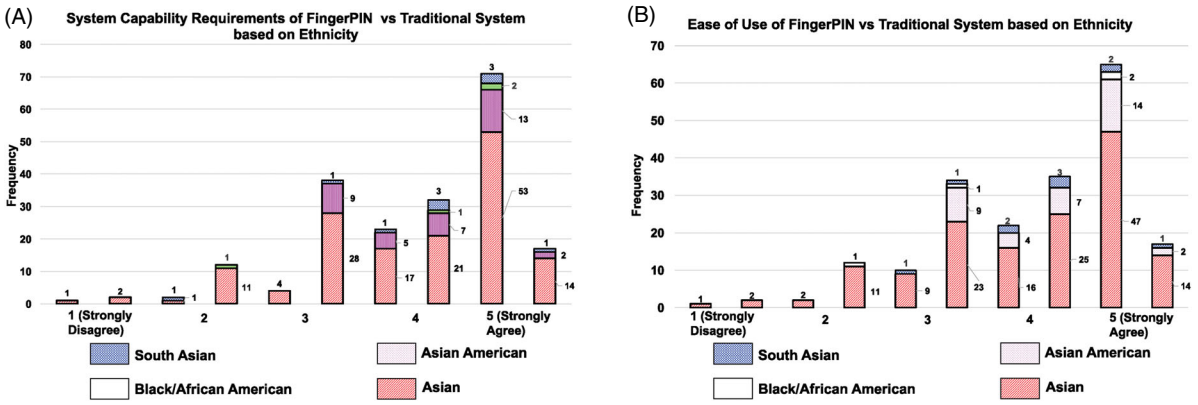

FIGURE 12 Ethnicity impact on the perceived usability of both FingerPIN and multi-factor authentication (MFA) traditional system

disagreed that the traditional system was easy to use. A 44% of the subjects stayed neutral and felt that both systems were neither easy nor difficult to use.

To have a deeper understanding about the factors influencing perceived usability, we conducted a demographic analysis. The results show that system capability requirements are not specific to a gender group and FingerPIN system had a positive response from both the genders. Figure 11B shows that additional 48% of the male participants as well as additional 45% of females strongly agreed that the FingerPIN system is easier to use compared to the traditional MFA system. Furthermore, we analyzed the ethnicity impact on the responses to the questions "Does the systems meet your requirements? and "Are the systems easy to use?" in Figure 12A,B, respectively. We can see that the system capability requirements as well as the ease of use of FingerPIN are not subjected to population differentials.

Since the FingerPIN system is based on parallel MFA, more than 90% of the subjects felt it was faster than comparable sequential MFA. In this regard, 70% of the subjects completed the authentication in less than 5 seconds while using the FingerPIN system and 14 seconds when using sequential MFA. They also enjoyed keeping the hand in the same position during authentication, in contrast with the PIN-based authentication scheme in which they need to move the hand to use the keyboard. Most of the participants preferred the challenge mode; in particular, some of the subjects faced difficulties and were perplexed in remembering the 5-fingerprint sequence. Out of 100 subjects, 93% of the subjects preferred to use the FingerPIN system over the traditional sequential MFA system. An aspect that we did not considered in this work pertains to an evaluation of the verbal guidance provided to the participants of the data.

6 | CONCLUSIONS

This article focuses on the usability assessment of the FingerPIN MFA scheme that combines in parallel the two factors PIN and fingerprint for increased security. This work enables a better understanding of the user experience regarding

biometric authentication factors integrated with PINs, their eventual increased usability and their accessibility, leading to higher adoption and broader access to these services. The pilot study was conducted by collecting data from 100 people and using two metrics: perceived usability and familiarity level. Using these metrics, we analyzed whether the users prefer FingerPIN compared to the traditional sequential MFA system. The outcome was positive for the majority of the subjects. In terms of perceived usability, we found that 95% of the participants felt that the FingerPIN system met their capabilities requirements, and approximately 90% of the participants felt that it is easy to use when compared to the sequential MFA. Finally, the subjective responses provided by the subjects about their perceptions of both systems revealed that the FingerPIN system is more efficient, faster, easy to use and secure when compared to the traditional sequential MFA system. The majority of the subjects were able to authenticate quickly using our parallel MFA scheme; while, using the sequential MFA approach, the authentication was completed approximately 10 seconds later.

These findings were not linked to any specific demographic trend, for example, gender, or ethnicity. In future work, we will: (i) develop a similar prototype of a mobile app and extend the usability study to it, (ii) evaluate the interoperability of the proposed system by changing the acquisition device as well as the matching algorithm in both intra- and inter-device acquisition settings (in the latest, the device used for enrollment will differ from the one used for authentication), (iii) build a MFA scheme based on the parallel integration of facial and fingerprint recognition, (iv) extend the usability metrics by incorporating personality styles, and (v) analyze users' needs and usability in people with disabilities.

ACKNOWLEDGMENTS

This research was sponsored by Virginia Research Investment Fund under award number HN-4Q21-003 and was also partially supported by the National Science Foundation under award number CNS-1822094.

DATA AVAILABILITY STATEMENT

Research data not shared

ENDNOTE

*https://www.neurotechnology.com/verifinger.html

ORCID

Emanuela Marasco https://orcid.org/0000-0003-3373-074X
Massimiliano Albanese https://orcid.org/0000-0002-2675-5810

REFERENCES

1. Ometov A, Bezzateev S, Mäkitalo N, Andreev S, Mikkonen T, Koucheryavy Y. Multi-factor authentication: a survey. *Cryptography*. 2018;2(1):1.
2. Bonneau J, Herley C, Van Oorschot PC, Stajano F. Passwords and the evolution of imperfect authentication. *Commun ACM*. 2015;58(7):78-87.
3. Marasco E, Shehab M, Cukic B. A methodology for prevention of biometric presentation attacks. Proceedings of the 2016 Seventh Latin-American Symposium on Dependable Computing (LADC); 2016:9-14.
4. Marasco E, Cando S, Tang L, Ghiani L, Marcialis GL. A look at non-cooperative presentation attacks in fingerprint systems. Proceedings of the 2018 Eighth International Conference on Image Processing Theory, Tools and Applications (IPTA); 2018:1-6.
5. Marfella L, Marasco E, Sansone C. Liveness-based fusion approaches in multibiometrics. Proceedings of the 2012 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS); 2012:1-7.
6. Gunson N, Marshall D, Morton H, Jack M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Comput Secur*. 2011;30(4):208-220.
7. Multifactor Authentication Market Size and Forecast. https://www.verifiedmarketresearch.com/product/global-multifactor-authentication-market-size-and-forecast-to-2025/; 2021 Accessed: August 30, 2022.
8. Bevan N, Carter J, Earthy J, Geis T, Harker S. New ISO standards for usability, usability reports and usability measures. *Int Conf Hum Comput Int*. 2016;9731:268-278.
9. BIO-Key. Why Your Multifactor Authentication Platform Should Include Biometrics. https://www.bio-key.com/wp-content/uploads/2020/04/White-Paper-Why-Biometrics-MFA-2020.pdf; 2020, Accessed: August 30, 2022.
10. Marasco E, Albanese M. FingerPIN: an authentication mechanism integrating fingerprints and personal identification numbers. Proceedings of the International Conference on Computer Vision and Image Processing, 1367, Springer; 2020:500-511.
11. Dodini S, Lopez-Fernandini AA, Merry EA, Thomas L, others. Consumers and Mobile Financial Services 2016. Tech. Rep., Board of Governors of the Federal Reserve System, (USA); 2016.
12. Patrick AS. *Fingerprint Concerns: Performance, Usability, and Acceptance of Fingerprint Biometric Systems*. Canada: National Research Council of Canada; 2008.

13. Chayanam P, Inskeep T, Miller EW, Newton C, Shroyer DC. Reusable Authentication Experience Tool. 2013. US Patent publication number: US8595809B2.
14. Ashbourn J. *Biometrics: Advanced Identity Verification: The Complete Guide: XVIII, 200; No. 1*. London: Springer; 2014.
15. Frøkjær E, Hertzum M, Hornbæk K. Measuring usability: are effectiveness, efficiency, and satisfaction really correlated? Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2000); 2000:345-352.
16. Seffah A, Donyaee M, Kline RB, Padda HK. Usability measurement and metrics: a consolidated model. *Softw Qual J*. 2006;14(2):159-178.
17. Theofanos MF, Stanton BC, Orandi S, Micheals RJ, Zhang NF, others. Usability Testing of Ten-Print Fingerprint Capture. Tech. Rep, National Institute of Standards and Technology; 2007.
18. Jakobsson M, Shi E, Golle P, Chow R, others. Implicit authentication for mobile devices. Proceedings of the Fourth USENIX Conference on Hot Topics in Security. USENIX Association; 2009:9.
19. Trewin S, Swart C, Koved L, Martino J, Singh K, Ben-David S. Biometric authentication on a mobile device: a study of user effort, error, and task disruption. Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC); 2012:159-168.
20. Lovisotto G, Malik R, Sluganovic I, Roeschlin M, Trueman P, Martinovic I. *Mobile Biometrics in Financial Services: A Five Factor Framework*. Oxford, UK: Tech. Rep., University of Oxford; 2017.
21. Ross A, Jain AK. Multimodal biometrics: an overview. Proceedings of the 2004 12th European Signal Processing Conference; 2004:1221-1224.
22. Marasco E, Ross A, Sansone C. Predicting identification errors in a multibiometric system based on ranks and scores. Proceedings of the 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS); 2010:1-6.
23. Jain A, Nandakumar K, Ross A. Score normalization in multimodal biometric systems. *Pattern Recognition*. 2005;38(12):2270-2285.
24. Marasco E. *Secure Multibiometric Systems*. PhD Dissertation. Naples, Italy: Dept. Inf. Sistemistica, Univ. Naples Federico II; 2010.
25. Ruoti S, Roberts B, Seamons K. Authentication melee: a usability analysis of seven web authentication systems. Proceedings of the 24th International Conference on World Wide Web (WWW 2015); 2015:916-926.
26. Lewis JR, Utesch BS, Maher DE. UMUX-LITE: when there's no time for the SUS. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; 2013:2099-2102.
27. Lazar J, Feng JH, Hochheiser H. *Research Methods in Human Computer Interaction*. 2nd ed. Boston: Morgan Kaufmann; 2017.

How to cite this article: Marasco E, Albanese M, Patibandla VVR, Vurity A, Sriram SS. Biometric multi-factor authentication: On the usability of the FingerPIN scheme. *Security and Privacy*. 2023;6(1):e261. doi: 10.1002/spy2.261