FingerPIN: An Authentication Mechanism Integrating Fingerprints and Personal Identification Numbers

Emanuela Marasco(✉) and Massimiliano Albanese(✉)

Center for Secure Information Systems, Volgenau School of Engineering, George Mason University, 4400 University Drive, Fairfax, VA 22030, USA
{emarasco,malbanes}@gmu.edu

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. However, despite the usability and accuracy of this technology, some significant concerns still exist, which can potentially hinder its further adoption. For instance, a subject's fingerprint is permanently associated with an individual and, once stolen, cannot be replaced, thus compromising biometric-based authentication. To mitigate this concern, we propose a multi-factor authentication approach that integrates type 1 and type 3 authentication factors into a fingerprint-based personal identification number, or FingerPIN. 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 conduct a vulnerability analysis of the proposed scheme, and demonstrate that it is robust to the compromise of one or more of the subject's fingerprints.

1 Introduction

Robust authentication mechanisms are critical to protect the security of data and applications. While offering a high level of security, biometric-based authentication maintains convenience for the user. In particular, fingerprints provide well-known distinctiveness and persistence properties. Biometric technologies are widely adopted in various government applications such as National ID, border control, and passport control [18], as well as in forensics and in criminal investigations for the identification of terrorists and other criminals. Commercial applications include computer network login, ATMs, credit card and medical records management [7,10]. Fingerprint systems are currently used for unlocking smartphones (e.g., iPhone 5S) or to engage in financial transactions and make purchases. However, if compromised, the same characteristics and advantages of biometrics present a potential threat to the owner of the biometric markers and risks to the businesses that use biometric data. Biometrics are biologically unique to the individual, therefore, once compromised, the individual has no recourse and they are at an increased risk for identity theft.

E. Marasco and M. Albanese—were partially supported by the National Science Foundation under award CNS-1822094.

S. K. Singh et al. (Eds.): CVIP 2020, CCIS 1376, pp. 500–511, 2021.
https://doi.org/10.1007/978-981-16-1086-8_44

Type 1, or *knowledge-based*, authentication is still the most widely adopted form of authentication, despite its many weaknesses. Most user create passwords that are easy to remember, therefore easy to guess or crack through a variety of means including social engineering and dictionary attacks. When longer or difficult-to-remember passwords are chosen, users tend to write them down in easily accessible places, effectively defeating the purpose of using authentication. Furthermore, compromising a single password may represent a risk for multiple applications, as users tend to reuse the same passwords across different applications [7].

To address these limitations, organizations are transitioning to multi-factor authentication, requiring users to provide at least two different authentication factors to prove their identity and be granted access to a system. A type 1 authentication factor (e.g., password, PIN) is typically paired with either a type 2 authentication factor (e.g., token) or a type 3 authentication factor (e.g., fingerprint). In traditional multi-factor authentication approaches, a user would need to *sequentially* prove knowledge of the PIN and validity of their biometrics features by entering the PIN on a keyboard and scanning one or more fingerprints. We propose a multi-factor authentication scheme that *integrates* a type 1 authentication factor (a PIN) and a type 3 authentication factor (fingerprints) into a fingerprint-based PIN, which we refer to as FingerPIN. In this paper, we push the boundaries of multi-factor authentication by combining 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. While such secret mapping may be difficult to remember and may slow down user authentication, what a user really needs to recall is the sequence of fingers corresponding to the digits of the PIN, as both the PIN and the mapping are set once in the enrollment phase and may change infrequently. If either the PIN or the mapping changes, the user would need to determine the new sequence of fingers used for authentication.

The paper is organized as follows. Section 2 discusses related work in multi-factor authentication involving biometrics. Section 3 presents the proposed authentication scheme, whereas Sect. 4 presents metrics to evaluate the strength of FingerPIN, along with an assessment of vulnerabilities in different attack scenarios. Then, Sect. 5 discusses our experimental results. Finally, Sect. 6 gives some concluding remarks and indicates possible future research directions.

2 Related Works

Traditional authentication solutions based on passwords or graphical patterns suffer from credential theft (e.g., through shoulder surfing) [1,16]. Authentication mechanisms involving physiological biometrics (e.g., fingerprints, iris patterns and face) are less likely to suffer from credential theft. However, different biometric technologies require different devices having a range of costs. Furthermore, they may limit privacy for users [2]. Recent studies exploiting biometric features (e.g., a sequence of 2D handwriting and corresponding pressure) rely on touch screens for feature extraction and are not easy to extend to general security access systems [8,9]. In 2014, driven by the need for increasing robustness against reuse of a fingerprint by a malicious attacker,

Go *et al.* proposed a two-factor authentication system involving fingerprint information and a password [5]. During registration, the users input their fingerprint and a password. A decimal number is associated to each letter of the password by modular arithmetic. The fingerprint template is converted to a square of fixed size to generate a standardized template that is then partitioned into a 3×3 matrix indexed by a sequence number 1–9. The generated nine regions are extracted based on the decimal numbers corresponding to the characters of the password. Partial templates are then relocated into a 3×3 matrix to create a new virtual template from which minutiae points are extracted, which does not follow the traditional matching operation.

In 2017, Nguyen *et al.* presented an authentication mechanism in which the user is asked to draw their PIN through a touch interface instead of typing it on a keypad [19]. This approach offers better security by utilizing drawing traits or behavioral biometrics as an additional authentication factor and it is prone to usability by leveraging user familiarity with PINs. This scheme was evaluated under stronger threat models but experiments were carried out on a small set of subjects. Liu *et al.* proposed the VibWrite system that involves novel algorithms to discriminate fine grained finger-input and that supports three independent passcode secrets including PIN number, lock pattern and gesture features extracted in the frequency domain [8]. However, gesture-based authentication is not as discriminative as the well-established minutiae-based recognition. Additionally, combining a vibration signal into an authentication procedure is vulnerable to blind attacks and the vibration signal itself may be easy to imitate and vulnerable to impersonation attacks.

In 2018, Souza *et al.* presented an optical authentication technique based on two-beam interference and chaotic maps used in conjunction with biometrics [15]. The user registers by recording a biometric template. He then chooses a base image that is encoded through two-beam interference to produce a phase key that is used to encrypt the biometric data. A chaotic sequence is generated from the password and used to scramble this phase key resulting in the possession factor. Cantoni *et al.* proposed an authentication scheme that combines behavioral gaze-based biometrics with a PIN. In particular, eye information is captured by means of an eye tracker when the user enters a PIN through a virtual keypad displayed on a screen [4]. In 2019, Henderson suggested the benefits of a multi-factor security device that would combine a fingerprinting sensor and an LED pulse oximeter which would eliminate most if not all threats to fingerprinting authentication technology [6]. A CNN-based anti-spoofing two-tier multifactor authentication system was proposed in [14]. Tier I integrates fingerprint, palm vein print and face recognition to match with the corresponding databases, and Tier II uses fingerprint, palm vein print and face anti-spoofing convolutional neural networks (CNN) based models to detect spoofing. In the first stage, the hash of a fingerprint is compared with the fingerprint database. After a successful match of the fingerprint, a CNN-based model tests the fingerprint to verify whether it is a spoof or real.

3 The Proposed Authentication Scheme

The proposed authentication scheme combines type 1 and type 3 authentication factors into a new multi-factor authentication mechanism. We investigate the integration of

fingerprints and Personal Identification Numbers (PINs), and develop FingerPIN, an authentication scheme using fingerprint-based PINs: to authenticate, the user is required to scan multiple fingers in a sequence determined by a secret mapping between the user's 10 fingers and digits from 0 to 9, based on the user's PIN. Adding one digit to FingerPIN increases the complexity for an attacker significantly more than adding a digit to a traditional PIN. The two authentication factors are combined in such a way that the user does not need to remember both the PIN and the secret mapping but only a specific sequence of fingers, which is as easy to remember as remembering a PIN.

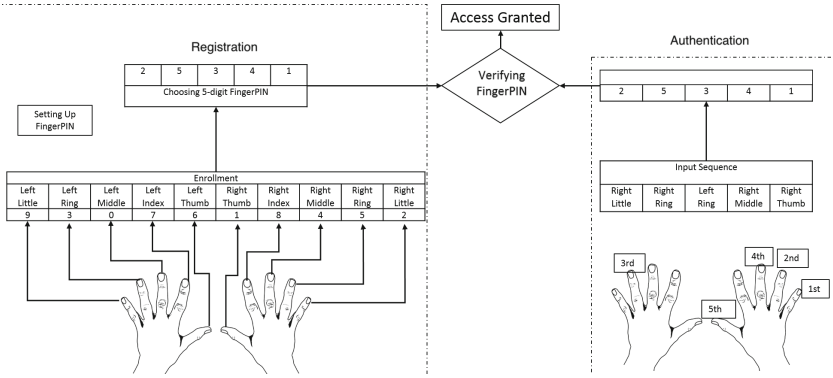


Fig. 1. After enrolling their ten fingerprints, a user chooses 2, 5, 3, 4, 1 as their PIN, which is converted into the sequence Right Little, Right Ring, Left Ring, Right Middle, Right Thumb.

A *finger-digit* is a single fingerprint component of the chosen sequence. The mapping between digits from 0 to 9 to fingers is set during enrollment. For instance, in the example of Fig. 1, the user chooses to map their left little finger to 9, left ring to 3, left middle to 0, and so on. The user then chooses a PIN – 25341 in our example – which determines the sequence of fingerprints to present for authentication. In our example, the first digit of the PIN is 2, which is mapped to the right little finger. The following four digits are mapped to right ring, left ring, right middle, and right thumb respectively. At authentication time, the user presents the sequence: right little, right ring, left ring, right middle, and right thumb. Intuitively, since the mapping between digits and fingers is not predefined, but rather determined by the user, an extra layer of protection is added. FingerPIN involves the execution of enrollment, registration, and authentication tasks. The *enrollment* module is responsible for storing the reference biometric data into the system database [7]. During this phase, the ten fingerprints of the subject are acquired by a sensor and a digital representation is produced. This digital representation is further processed by a feature extractor and a more compact representation, called a template, is obtained. Multiple templates of an individual are usually stored in order to account for variations observed in the biometric trait. Furthermore, the templates in the database may be updated over time. During this phase, the user also defines a mapping between digits and fingers, which can be changed at any time or with a predefined frequency for additional security. During *registration*, the user chooses a PIN, which determines

the sequence of fingerprints to be used for authentication. During *authentication*, the system verifies the identity of a subject based on their FingerPIN. The process compares the biometric data captured from the subject attempting to authenticate with the biometric templates stored in the system database for that same subject. Authentication can operate in one of the two following modes.

- Standard Authentication Mode (Mode 1). All the fingerprints composing the FingerPIN are sequentially matched, one by one, which makes the time required to verify the identity linear with the length of the FingerPIN. Consequently, longer FingerPINs may impact usability. For instance, in the example of Fig. 1, the PIN chosen by the user is mapped to the sequence of fingers: right little, right ring, left ring, right middle, and right thumb. Thus, the user is expected to present their fingerprints in this exact order.
- Challenge Mode (Mode 2). The system presents a challenge, asking the user to provide a specific finger-digit of the FingerPIN (e.g., the third finger-digit). The processing time does not dependent on the PIN's length, and the burden on the user is limited. In the example of Fig. 1, when asked to provide the third finger-digit, the user is expected to present the fingerprint corresponding to their left ring finger.

4 FingerPIN Vulnerability Analysis

This section discusses the properties of the proposed mechanism and demonstrates its advantages over traditional multi-factor authentication.

In a brute-force attack against a traditional PIN, a randomly chosen five-digit sequence is guaranteed to be guessed in 100,000 attempts.

A brute-force attack to a fingerprint system is an indirect attack, e.g., a brute force attack to the feature extractor input or to the matcher input. A False Match Rate (FMR) of 0.001% corresponds to the success of 1 out of 100,000 attempts by using a large number of different fingerprints. Generating or acquiring a large number of biometric samples is much more difficult and time-consuming than generating a large number of PINs. The number of attempts to brute-force a single fingerprint is typically in the same order of magnitude of the number of attempts to brute-force a 5-digit PIN, in addition to the fact that comparing two fingerprints is computationally more demanding than comparing two 5-digit numbers.

A brute-force attack against FingerPIN is studied by estimating the probability of a success in different scenarios, based on the information available to the attacker. In Scenario 1, the ten fingerprints of the user are unknown to the attacker. In Scenario 2, one fingerprint template has been stolen by the attacker. In this case, we assume that the matching during authentication will occur with an accuracy of 100%. In Scenario 3, all the ten fingerprint templates are known to the attacker. Furthermore, for each case we consider when the secrecy of the mapping is compromised as well. In the following subsections, we will use k to denote the length of the PIN. We will also assume that the number of repetitions of a certain fingerprint in the chosen sequence is zero.

4.1 Scenario 1: Brute-Force Attack with No Fingerprint Compromised

In a brute-force attack, the attacker has no knowledge about any fingerprint of the genuine user. Given a FingerPIN, we compute the probability $P(Success)$ that a sequence of k arbitrary fingerprints presented by an attacker during a brute-force attack is successfully matched against the FingerPIN, allowing the attacker to achieve authentication. Let $P(FM_{ij})$ be the probability of False Match (FM) of the i^{th} fingerprint used by the attacker against the i^{th} finger-digit of the FingerPIN, with $P(F_{ij})$ indicating the probability that the i^{th} finger-digit maps to digit j, and $\sum_{j=0}^{9} P(F_{ij}) = 1$. When the system operates in Mode 1, assuming that finger-digits are independent and equally distributed, $P(Success)$ is given by Eq. 1 below.

$$P(Success) = \prod_{i=1}^{k} P(Success_i) = \prod_{i=1}^{k} \sum_{j=0}^{9} P(FM_{ij}) \cdot P(F_{ij}) \tag{1}$$

Regarding the term $P(FM_{ij})$, an empirical estimate of the probability with which the system incorrectly declares that a biometric sample belongs to the claimed identity when the sample belongs to a different subject (impostor) can be provided by the False Match Rate (FMR) [12]. FMR is typically selected based on the level of security required by the application and the corresponding threshold is set for the system.

It is clear from Equation 1 that the probability of k random fingerprints matching k finger-digits is much smaller than the probability of k random digits matching a k-digit PIN. When the attacker does not have any genuine fingerprints available, knowledge of the secret mapping or the PIN would not help the attacker increase this probability.

4.2 Scenario 2: Brute-Force Attack with One Fingerprint Compromised

In this scenario, one fingerprint of the genuine user has been stolen and a brute-force attack is attempted. We analyze how the probability $P(Success)$ changes when one fingerprint is compromised. The matching accuracy varies across different instances of an individual's fingerprints. A vulnerability in FingerPIN is found when the cross-instance match score is high for one or multiple fingerprint instances. In this case, the vulnerable instance can potentially be matched to more than one fingerprint which makes the scheme less secure. Although, in the scientific literature, there is not yet convergence for the term *non-zero effort attack*, in this paper it refers to the exploitation of any of the vulnerability points present in a typical fingerprint system [3,11,13]. Let $P(NFM_i^{SF})$ be the probability of Non Zero-Effort Attack Same-Finger False Match (NFM^{SF}) of the i^{th} fingerprint in the FingerPIN sequence. Let $P(NFM_i^{CF})$ be the probability of Non Zero-Effort Attack Cross-Finger False Match (NFM^{CF}) of the i^{th} fingerprint when the stolen fingerprint is from a different finger than the one chosen in the FingerPIN sequence. Let F_s indicate the fingerprint stolen. When the system operates in Mode 1, assuming that finger-digits are independent and equally distributed, $P(Success)$ is given by Eq. 2 below.

$$P(Success) = \prod_{i=1}^{k} \sum_{j=0}^{9} (P(F_{ij}, F_{sj}) \cdot P(NFM_j^{SF}) + P(F_{ij}, F_{s\neq j} \cdot P(NFM_j^{CF})) \tag{2}$$

Whether the secrecy of the correspondence between fingers and digits is compromised, the probability that a brute-force attack can be simplified as follows:

$$P(Success) = \prod_{i=1}^{k} \sum_{j=0}^{9} (P(F_{sj}) \cdot P(NFM_j^{SF}) + P(F_{s \neq j} \cdot P(NFM_j^{CF})) \quad (3)$$

4.3 Scenario 3: Brute-Force Attack with All the Fingerprints Compromised

In this scenario, all the ten fingerprints of the genuine user have been stolen and a brute-force attack is attempted. The FingerPIN is guaranteed to be guessed in 10^k attempts – corresponding to all possible sequences of length k of the 10 fingerprints – requiring a total of $10^k \cdot k$ fingerprint comparisons. By contrast, a brute a force attack against a traditional PIN would require only 10^k comparison between k-digit numbers. The secrecy of the mapping between the digits from 0 to 9 and the subject's fingers adds complexity to the scheme, making a brute-force attack more onerous. In fact, even when all fingerprints have been compromised, the attacker still needs to run a brute-force attack to compromise the FingerPIN, and every trial involves matching k fingerprints.

5 Experimental Results

5.1 Dataset

The dataset used in our experiments is a subset of the ManTech Innovations Fingerprint Study Phase I collection. It contains fingerprints of 500 subjects acquired using 7 optical sensors. We used images of the ten fingers acquired using the I3 digID Mini sensor. Among the participants, the age group between 20–33 was the largest, accounting for 60.6% percent of the subjects. With respect to ethnicity, Caucasians accounted for 57.2% of the subjects. There was a nearly equal number of male and female participants with a 51% to 48% ratio. Every subject provided two sets of rolled fingerprints for both hands, see sample images in Fig. 2.

Fig. 2. Examples of fingerprint images from the ManTech Phase I collection used in this study

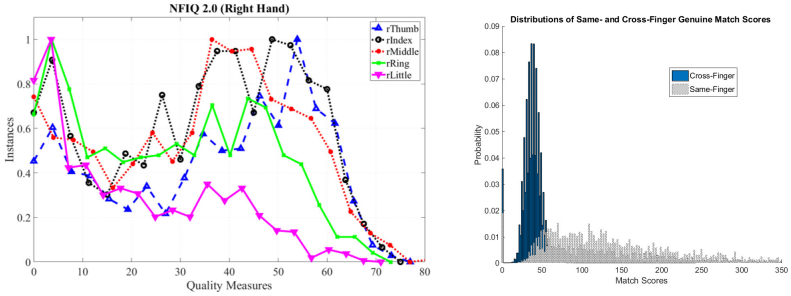
5.2 Evaluation Metrics

For a PIN Number-based scheme, the Attack Success Rate can be computed as the percentage of correctly verified PIN numbers entered by the attacker during the user authentication process. It includes the complete PIN sequence verification accuracy

and the PIN digit verification accuracy. Biometric matching performance is assessed using: (i) False Match Rate (FMR), the proportion of instances where an impostor is incorrectly labelled as a genuine match with respect to the total number of impostor comparisons; (ii) False Non-Match Rate (FNMR), the proportion of instances where a genuine match is incorrectly labelled as an impostor with respect to the total number of genuine comparisons; and (iii) Detection Error Trade-off (DET) curve, which plots FMR and FNMR as a function of the decision threshold [7]. The inputs to the matcher are two fingerprint samples (e.g., gallery and probe images) and the output is a match score that indicates the proximity of the two samples. A threshold is applied to this match score to determine if the samples correspond to the same identity.

5.3 Experimental Results

Baseline. Match scores were extracted using Neurotechnology VeriFinger Version 10.0[1]. The quality measures were extracted using the NIST Fingerprint Image Quality (NFIQ 2.0) software[2], see Fig. 3(a) [17]. These distributions shows that right thumb, left thumb and right index exhibit a better image quality than other fingers.



(a) (b)

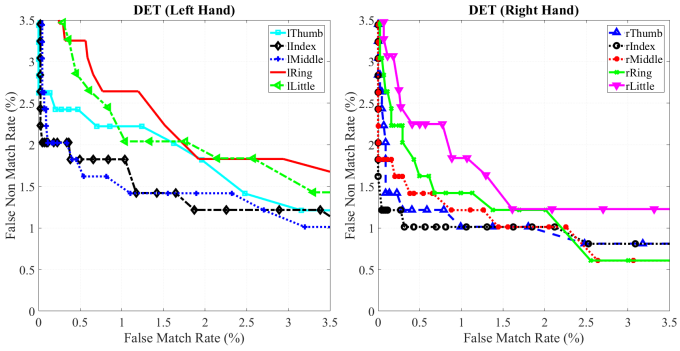
Fig. 3. (a) NFIQ 2 distribution of the fingers of the right hand. Little fingers exhibit lower image quality, a similar trend was observed for the left hand as well; (b) Distributions of same-finger and cross-finger match scores, fingerprints being compared pertain to the same identity

Figure 3(b) shows the probability distributions of the match scores output by comparing fingerprints pertaining to the same subject in both cross- and same-finger scenarios. In this graph, genuine match scores were generated by comparing same fingers of the same subject, while impostor scores were obtained by matching different fingers of the same subject. We can notice a relatively small overlap area between the two distributions. In the scientific literature, an analysis of cross-finger matching when the identity is the same is rarely carried out. The attack-resistance of a fingerprint system alone, expressed as the probability of successfully launching a brute-force attack, is 1

[1] https://www.neurotechnology.com/verifinger.html.
[2] http://www.nist.gov/services-resources/software/development-nfiq-20.

out of 100,000 attempts. The baseline fingerprint verification performance alone can depicted using the Detection Error Trade-off graph for all the ten fingers, see Fig. 4(a) and Fig. 4(b). For certain fingerprint instances such as left and right little fingers, error rates are higher. Thus, we wondered if the security of FingerPIN is affected when those instances are chosen as components of the authentication sequence.

System Performance of Verifying Legitimate User. We discuss experimental results related to scenarios 1 and 2 in which one or multiple fingerprints used in FingerPIN have been captured by an attacker. As case study, ten random 5-digit PINs with no repetitions were generated for every subject. For simplicity, the compromised fingerprint instance is assumed to be the same for all the authorized users. The FMR of the fingerprint system is 0.01%. Although such scenarios may seem critical, we found out that the success rate to break the FingerPIN scheme is very low.



(a) (b)

Fig. 4. DET curves for the fingerprints of the left (a) and right (b) hands.

Results are summarized in Table 1. Cross-finger matches refer to comparisons between different fingerprint instances carrying the same identity and they are highlighted in bold. FM^{CF} indicates the proportion of the cross-finger matches wrongly accepted with respect to all the cross-finger matches. Findings show that with one compromised finger-digit, the additional four are able to keep high the level of protection. When the stolen fingerprint is the right index for all the subjects, only a few cross-finger false matches occur. The gallery was the right middle in 7 out of 8 false matches, while it was the left ring only in one case. These matches involved comparison between fingerprints pertaining to different identities.

Findings showed also that with two compromised finger-digits, the remaining three can guarantee robustness. When the stolen instance was the right thumb, only three cross-finger false matches among all the possible combinations were found. In two of these cases, the galleries were the right index and the left ring of the same subject, while in the third case the gallery was the left middle finger from a different subject. In this critical scenario, the proposed scheme would still be secure given the presence of the fifth component. Similar to the above, when the stolen fingerprint is the right middle

finger for all the subjects, six cross-finger false matches were found. In two cases the galleries were right index and right little fingers pertaining to the same subject, while in four cases the galleries were right index, right ring (twice) and left ring fingers from different individuals. When the compromised finger-digit is the right ring, the gallery was the right middle finger in 5 out of 6 cross-finger false matches. When the right little finger is stolen, results are similar to the scenario previously encountered with the difference that the galleries are from different subjects. Regarding the fingers of the left hands, with the left index fingerprint compromised, there were eight occurrences of cross-finger false matches, in six of them the left middle finger was the gallery. Among the remaining fingers, the left thumb showed less risk with only one cross-finger found while the left ring the highest with 14 cross-finger false matches.

Table 1. Security results in Scenario 2: cross-finger false match rate for one stolen fingerprint.

Cross-Finger False Match FM^{CF} (%)										
Stolen Fp	Rx Thumb	Rx Index	Rx Middle	Rx Ring	Rx Little	L Thumb	L Index	L Middle	L Ring	L Little
Rx Thumb	-	**0.0037**	-	-	-	-	-	0.0037	**0.0037**	-
Rx Index	-	-	0.0259	-	-	-	-	-	0.0037	-
Rx Middle	-	**0.0111**	-	0.0074	**0.0074**	-	-	-	0.0037	-
Rx Ring	-	-	0.0185	-	-	-	-	-	-	-
Rx Little	-	0.0037	-	-	-	-	-	-	0.0037	-
L Thumb	-	-	0.0037	-	-	-	-	-	-	-
L Index	0.0037	-	0.222	-	-	-	-	-	0.0037	-
L Middle	-	0.0074	-	-	-	-	0.0296	-	0.0111	-
L Ring	0.0037	-	0.0074	-	-	-	0.0111	0.0296	-	-
L Little	-	-	-	-	-	-	-	-	-	-

For a more user-friendly authentication, the constraint of choosing a sequence without repetitions can be relaxed. For instance, a user is allowed to repeat or not a particular finger-digit in the sequence. The repetitions are not expected but allowed. For every fingerprint instance, there is no constraint regarding the number of expected repetitions. The probabilities of repetitions of each stolen fingerprint are summarized in Table 2. The probability of choosing a given finger-digit five times in the sequence is always zero. One stolen fingerprint is repeated twice in the FingerPIN sequence in about 7% of the cases, in which three cross-finger false matches should occur for a brute force attack to succeed.

Based on a preliminary usability assessment involving our research group, applying FingerPIN does not require any change in the position of the hand given the acquisition of the next finger-digit can be done through the same sensing surface. No movement of the hand is necessary given that the user only need to change finger. In a traditional PIN, the (same) finger needs to be pressed on different keys of a keyboard requiring movement of the hand.

Table 2. Probability of repetitions for a given fingerprint instance.

Stolen Fp	P(Rep = 1)	P(Rep = 2)	P(Rep = 3)	P(Rep = 4)	P(Rep = 5)	P(Rep)
Rx Thumb	0.3300	0.0766	0.0088	$4\ e^{-4}$	0	0.4158
Rx Index	0.3272	0.0732	0.0064	$8\ e^{-4}$	0	0.4076
Rx Middle	0.3326	0.0768	0.0062	$4\ e^{-4}$	0	0.4160
Rx Ring	0.3208	0.0730	0.0104	0	0	0.4042
Rx Little	0.3326	0.0660	0.0062	$4\ e^{-4}$	0	0.4052
L Thumb	0.3324	0.0708	0.0082	$4\ e^{-4}$	0	0.4118
L Index	0.3226	0.0792	0.0086	$8\ e^{-4}$	0	0.4114
L Middle	0.3212	0.0758	0.0076	$8\ e^{-4}$	0	0.4054
L Ring	0.3290	0.0706	0.0084	$4\ e^{-4}$	0	0.4084
L Little	0.3266	0.0712	0.0084	$6\ e^{-4}$	0	0.4068

6 Conclusions

In this paper, we proposed a new approach to multi-factor authentication that integrates knowledge- and inherence-based authentication factors into a fingerprint-based PIN. Computing the probabilities for a brute-force attack to succeed, we demonstrated that FingerPIN is less vulnerable than a PIN or a fingerprint system used alone. The nature of the information integrated in the proposed authentication scheme challenges an attacker's success more than traditional mechanisms. FingerPIN is more secure against a brute-force attack with and without compromised fingerprints compared to existing approaches. In scenarios where the attacker steals one fingerprint of the genuine user, the success rate of a brute-force attack breaking a 5-digit FingerPIN was zero. The overall probability of cross-finger false match was 0.004% and, only with a maximum of two fingers pertaining to the same subject. We can conclude that, a 5 finger-digits scheme guarantees robustness to brute-force attacks even in the presence of one stolen fingerprint. This result demonstrates how the parallel integration of the two factors considered in this paper overcomes the limitations of both a PIN mechanism alone as well as an authentication purely based on fingerprints. In future efforts, we will: *i)* extend experiments to additional touch-based fingerprint databases as well as to contactless fingerprint technologies, *ii)* integrate additional biometric modalities to further improve security, *iii)* extend the analysis to scenarios featuring repetitions of finger-digits in the chosen FingerPIN sequence, *iv)* explore the security level of the proposed scheme when more than one fingerprint is compromised, and *v)* carry out a large-scale usability assessment to validate the preliminary evaluation discussed in this work and to explore potential behavioral patterns with respect to gender, age group and ethnicity.

References

1. Angeli, A.D., Coutts, M., Coventry, L., Johnson, G.I., Cameron, D., Fischer, M.H.: VIP: a visual approach to user authentication. In: Proceedings of the Working Conference on Advanced Visual Interfaces (AVI 2002), pp. 316–323. ACM, Trento, Italy (2002)

2. Arakala, A., Jeffers, J., Horadam, K.J.: Fuzzy Extractors for Minutiae-Based Fingerprint Authentication. In: Lee, S.-W., Li, S.Z. (eds.) ICB 2007. LNCS, vol. 4642, pp. 760–769. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74549-5_80
3. Barkadehi, M.H., Nilashi, M., Ibrahim, O., Fardi, A.Z., Samad, S.: Authentication systems: A literature review and classification. Telematics and Informatics **35**(5), 1491–1511 (2018)
4. Cantoni, V., Lacovara, T., Porta, M., Wang, H.: A study on gaze-controlled PIN input with biometric data analysis. In: Proceedings of the 19th International Conference on Computer Systems and Technologies, pp. 99–103. ACM, Ruse, Bulgaria (2018)
5. Go, W., Lee, K., Kwak, J.: Construction of a secure two-factor user authentication system using fingerprint information and password. J. Intell. Manuf. **25**(2), 217–230 (2012). https://doi.org/10.1007/s10845-012-0669-y
6. Henderson, L.: Multi-factor authentication fingerprinting device using biometrics. Technical report, Villanova University (2019)
7. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circ. Syst. Video Technol. **14**(1), 4–20 (2004)
8. Liu, J., Wang, C., Chen, Y., Saxena, N.: VibWrite: towards finger-input authentication on ubiquitous surfaces via physical vibration. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS 2017), pp. 73–87. ACM, Dallas, TX, USA (2017)
9. Luca, A.D., 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 (CHI 2012), pp. 987–996. ACM, Austin, TX, USA (2012)
10. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition, 2nd edn. Springer, London (2009)
11. Marasco, E., Ross, A.: A survey on antispoofing schemes for fingerprint recognition systems. ACM Comput. Surv.**47**(2) (2014)
12. Poh, N., Chan, C.H., Kittler, J., Fierrez, J., Galbally, J.: Description of metrics for the evaluation of biometric performance. Technical Report, D3.3, BEAT (2012)
13. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Syst. J. **40**(3), 614–634 (2001)
14. Sajjad, M., et al.: CNN-based anti-spoofing two-tier multi-factor authentication system. Pattern Recogn. Lett. **126**, 123–131 (2019)
15. Souza, D., Burlamaqui, A., Souza Filho, G.: Improving biometrics authentication with a multi-factor approach based on optical interference and chaotic maps. Multimedia Tools Appl. **77**(2), 2013–2032 (2017). https://doi.org/10.1007/s11042-017-4374-x
16. Suo, X., Zhu, Y., Owen, G.S.: Graphical passwords: a survey. In: Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005). IEEE, Tucson, AZ, USA (2005)
17. Tabassi, E., Grother, P.: Fingerprint image quality. In: Li, S.Z., Jain, A. (eds.) Encyclopedia of Biometrics, pp. 635–643. Springer, Boston, MA (2015). https://doi.org/10.1007/978-0-387-73003-5_52
18. Trader, J.: The top 5 uses of biometrics across the globe (2016). http://www.m2sys.com/blog/biometric-hardware/top-5-uses-biometrics-across-globe/
19. Van Nguyen, T., Sae-Bae, N., Memon, N.: DRAW-A-PIN: authentication using finger-drawn pin on touch devices. Comput. Secur. **66**, 115–128 (2017)