BioDraw: Reliable Multi-Factor User Authentication with One Single Finger Swipe [1]

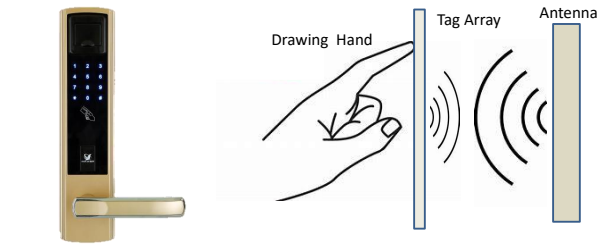
Jianwei Liu, Xiang Zou, Jinsong Han, Feng Lin, Kui Ren
School of Cyberspace Security, Zhejiang University, China
liujianwei, XiangZou@stu.xjtu.edu.cn, hanjinsong, flin, kuiren@zju.edu.cn
Corresponding author: hanjinsong@zju.edu.cn

Abstract. Multi-factor us r authentication (MFUA) becomes increasingly popular due to its superior security comparing with single-factor user authentication. However, existing MFUAs require multiple interactions between users and different authentication components when sensing the multiple factors, leading to extra overhead and bad use experiences. In this paper, we propose a secure and user-friendly MFUA system, namely BioDraw, which utilizes four categories of biometrics (impedance, geometry, composition, and behavior) of human hand plus the pattern-based password to identify and authenticate users. A user only needs to draw a pattern on a RFID tag array, while four biometrics can be simultaneously collected. Particularly, we design a gradient-based pattern recognition algorithm for pattern recognition and then a CNN-LSTM-based classifier for user recognition. Furthermore, to guarantee the systemic security, we propose a novel anti-spoofing scheme, called *Binary ALOHA*, which utilizes the inhabit randomness of RFID systems. We perform extensive experiments over 21 volunteers. The experiment result demonstrates that BioDraw can achieve a high authentication accuracy (with a false reject rate less than 2%) and is effective in defending against various attacks.

1 Introduction

User authentication is of importance for human-involved applications, such as identification, access control, and privacy protection. Typically, users verify their identities via sensitive or biometric information, including "something they know", "something they have", or "something they are". User authentication requires certain equipment for retrieving above information from users, ranging from the password, security token, to biometrics. When collecting these types of information, people are usually bothered with two critical concerns, security and usability, which are usually conflicted with each other. With the increase of threats in cyberspace and recent advance in sensing technologies, people urgently expect to have secure yet user-friendly user authentication systems.

Current user authentication approaches can be divided into two main categories, according to the number of evidence (factors) submitted to the authentication mechanism: single-factor user authentication and multi-factor user authentication. The involved factors include PIN [14], security token [12], pattern information [3], and biometrics [13, 10]. Single-factor authentication approaches are considered user-friendly because only one factor is required during the verification. In these approaches, normally the verification can be done through a single operation only. On the other hand, conventional single-factor authentication is vulnerable to attacks since the security of the whole system depends on this factor [5]. For example, attackers can easily compromise the authentication system by forging user's fingerprint [1], or replaying the signal of authentication information [18].



(a) PIN- and ID card-based lock.

(b) The sketch of BioDraw.

Figure 1. (a) shows a lock with multi-factor access control mechanism. (b) is the sketch of BioDraw.

Later on, multi-factor user authentication (MFUA) is proposed to enhance the security of single-factor user authentication through introducing multiple operations for multiple certificates acquisition [5]. MFUAs have been ubiquitously adopted in industrious community and practice. For example, the lock in Fig. 1(a) is a multi-factor user authentication applied in access control in normal office buildings. RF-Mehndi [24] leverages the RFID to extract the impedance feature of the user and the physical feature of the tag array to authenticate users. The work in [2] leverages unclonable functions and wireless signals' characteristics to achieve two-factor authentication. Nevertheless, most existing multi-factor user authentications just "pile up" multiple factors to enhance the security, resulting in cumbersome multi-operations and extra hardware for collecting factor information during the verification. Users have presented their negative attitude towards the shortcomings of current MFUAs [5] , including the complex operation, lack of user friendliness, and risk of information-leaking. Obviously, it is challenging to balance the trade-off between the security and usability in MFUA.

In order to overcome above embarrassment, we are motivated to enhance the security of user authentication by involving as many necessary factors as possible while simplifying the operation in a min-

[1] 978-1-7281-6887-6/20/$31.00 © 2020 IEEE

imal level. We still adopt the pattern lock/unlock as the basic factor in MFUA, because the pattern is a widely acceptable factor of "something they know". We also leverage four biometric features of a user's hand, i.e., impedance, geometry, composition, and behavioral feature [24, 15, 16], as the other four factors of "something they have" and "something they are". In this way, we are able to achieve high-security guarantee for MFUA, which can make the access control and checking-in more secure. Now the key problem is how to realize such a MFUA with only one single pattern input, instead of performing multiple interactive operations between the user and the authentication system. Fortunately, recent advance of sensing technologies inspires us to fuse the four biometric factors via wireless signals [24, 22, 20]. These approaches show that if well-designed, the radio frequency (RF) signals of RFID systems are capable to retrieve the human biometric features in both contact and non-contact based way.

It is known that using RF signals for retrieving needed multiple factors information remains challenging. The challenge is threefold. 1) Severe coupling effect exists among adjacent tags, deteriorating the accuracy of pattern recognition. 2) It is extremely hard to extract fine-grained biometric features from coarse-grained tags' signals. 3) Similar to wireless systems, RFID inevitably suffers from replay attack [18]. Though there are some effective solutions for resisting replay attacks [18], their implementation usually requires expertise knowledge, e.g. introducing randomness to signals.

In this paper, we propose a user-friendly RFID-based MFUA system, namely BioDraw, while addressing above challenges. As illustrated in Fig. 1(b), in BioDraw, the only needed operation is to draw a pattern on a tag array using one finger. First, we adopt a perpendicular layout in the tag array to alleviate the impact of coupling effect. Meanwhile, we design a novel gradient-based pattern recognition algorithm for accurate pattern recognition. We establish the theoretical foundation behind this design by proposing an equivalent circuit model. Furthermore, we design a CNN-LSTM-based classifier to extract the fine-grained features from coarse-grained tags' signals. We manipulate the inherent randomness of the frame-slot-based slot-ALOHA protocol [7], to detect the replay attack without requiring extra hardware or modification on the existing RFID infrastructure. In particular, we design a novel *Binary ALOHA* mechanism, which leverages and amplifies the randomness in frame-slot-based ALOHA protocol. *Binary ALOHA* produces a binary code as the certificate of a benign authentication activity. It can enlarge the encoding space by reusing the dimension of time. Thus, the security of Biodraw is significantly enhanced.

We build a prototype of BioDraw and evaluate its performance with 21 volunteers. The experiment results show that the average FRR of BioDraw is less than 2%. Besides, the extensive experiment results show that BioDraw is robust and secure. The five factors prevent BioDraw from various categories of attacks.

Our contribution can be summarized as followings: 1) We realize a robust and secure multi-factor user authentication method, named BioDraw, through one single pattern input. BioDraw extracts the fused feature from the impedance, geometry, composition, and behavioral features of human hand. 2) We propose a highly accurate gradient-based pattern recognition algorithm and build an equivalent circuit model to theoretically support its feasibility. 3) We introduce a novel replay attack detection technique, *Binary ALOHA*, based on the inherent randomness of existing frame-slot-based ALOHA protocol. 4) We build a prototype of BioDraw to conduct extensive experiments with 21 volunteers within three months. The experiment results show that BioDraw has a high authentication accuracy (robust and the average FRR is 1.30%) and is capable to defend against a variant of attacks.

2 Related Work

In this section we briefly describe two categories of related user authentication works, single-factor and multi-factor approaches. We also discuss the works related to replay attacks.

Single-factor user authentication: Single-factor user authentication only employs one factor for authentication. Commonly used factors include PIN [14], ID card [12] and pattern [3]. Because the authentication usually requires one operation, authentication is relatively user-friendly. With the development of sensing hardware and technology, collecting single biometric feature for authentication attracts increasing attentions. For example, Li *et al.* [11] propose a fuzzy extractor to facilitate the fingerprint based authentication. Xie *et al.* [19] utilize the finger vein plus deep learning for user authentication. Ye et al. [21] utilize ECG to accurately classify the heartbeat. However, it requires users to attach equipment on their chests rather than their wrists, which brings bad use experience.

Multi-factor user authentication: MFUA is more secure than single-factor authentication. Common multi-factor user authentications usually ask the users to show a combination of various evidences, ranging from the knowledge, possession, to inherence. For instance, the work in [8] conducts authentication by utilizing both finger vein and iris. An advanced design for multiple factors acquisition is collecting all the required certificates through only one operation. Several works have been proposed to reach such an advanced effect. RF-Mehndi [24] fuses two factors, the users' impedance and tags' physical feature. Chen *et al.* [4] leverage the hand's geometry and palm-print to setup a bi-model for authentication. Song *et al.* [15] use the geometry feature and behavioral feature of users' hand to perform authentication on the smartphone. Nevertheless, existing MFUA has the following drawbacks. First, the number of involved factors are limited, usually only two or three types of factors for one MFUA. Second, the multiple factors acquisition relies extra overhead, either from factor-collecting hardware or by human operations for inputting the factors.

Therefore, a fundamental motivation of this work is to eliminate the inconvenience caused by complex operations for inputting multiple factors and avoid costly overhead of introducing extra hardware. An ideal MFUA design is collecting sufficient factors through only one operation with one type of device, which is just the goal of our work, BioDraw.

3 Preliminary

In this section, we first introduce the randomness in the frame-slot-based ALOHA, and then introduce the layout of the tag array adopted in BioDraw.

3.1 Randomness in frame-slot-based ALOHA

Framed-based slot-ALOHA protocol has been widely used for collision avoidance in industrial RFID systems. The core technique supporting this protocol is the randomly allocated slots. Specifically, in a multi-tag RFID session, each tag needs to randomly select a slot in the frame first. The frame is broadcasted from the reader to all the readable tags at the beginning of each interrogation session. Afterwards, each tag reports its ID to the reader via the backscattered RF signal in its randomly selected session. In other slots, the tag stays

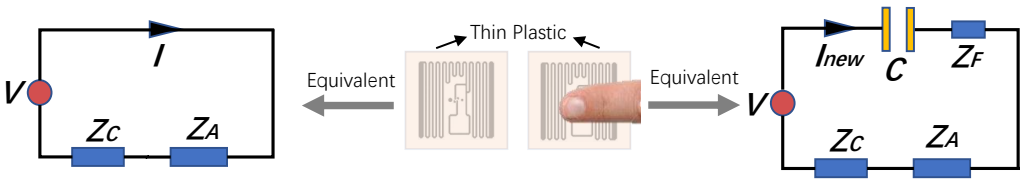


Figure 2. The equivalent circuits of different conditions. When a fingertip is touching on the center surface of the tag covered by the thin plastic, an extra capacitor and an extra impedance are introduced in the original equivalent circuit.

dormant. If collision occurs, i.e., two or more tags select a same slot in a same frame, the reader will discard the received information, because the signals from multiple tags will be overlapped and non-decodable. If a tag encounters a collision in its selected slot (not being identified), it will continue the randomly selection process in the next frame. The reader will continuously carry out the frame until all tags in its cover region are identified. In the above procedure, we can find that the randomness is the main theme that runs throughout. Moreover, the randomness can be represented by the reading order of tags. In Section 8, we will present how we leverage this random property for anti-replaying.

3.2 Perpendicular layout of tags

We employ a tag array, named TagPad, for the pattern input in BioDraw. To save space, we place two adjacent tags to be close to each other (the gap in-between is 3mm). However, the inductive coupling effect exists between two adjacent tags according to [24]. Such effect would weaken the RSS of those tags in the center area, and hence might make them be unreadable. In order to solve this issue while maintaining the size of the TagPad, we resort to the method proposed in [17]. We arrange each pair of adjacent tags in a perpendicular way according to their antennas' directions. In this way, BioDraw effectively alleviates the impact induced by undesirable coupling effect. Finally, because the direct contact between the human hand and the tag may make the tag unreadable, we cover the tag array with a layer of transparent thin plastic to avoid direct contact.

4 Biometric Features in BioDraw

BioDraw contains four biometric factors for authentication, the impedance, geometry, composition, and behavior of human hands. In this section, we describe how they perform as the authentication evidence.

4.1 Impedance, geometry, composition and behavior of human hand

In this part, we separately introduce each category of feature of human hand. Meanwhile, we explain how they are embodied by RF signals.

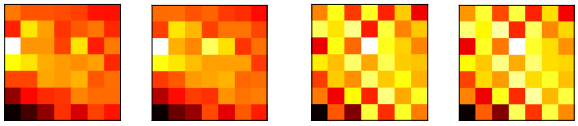
Impedance feature: In order to explain how impedance feature is introduced by the contact of fingertip, and how we can leverage the impedance of a hand to recognize the pattern, we conducted an experiment and then inferred the related theoretic model. In the experiment, a volunteer is asked to use the fingertip to touch the center part of the targeting tag on the tag array.

To avoid direct contact, a layer of plastic is attached on the tag's surface. As a result, the RSS values are stable before touching. However. They decrease rapidly when the fingertip touched the center part of the observed tag. This 'decreasing phenomenon' is explicable theoretically. According to the research introduced in [24], a passive RFID tag can be simplified as an equivalent circuit (shown in the left part of Fig. 2. The impedance of the center chip and the surrounding antenna are denoted by Z_A and Z_C respectively. If the voltage introduced by harvested power is V, the alternating current I in the tag's circuit is $\frac{V}{Z_A + Z_C}$. Recalling that a tag array which is covered by a layer of transparent plastic is used to backscatter signals in BioDraw, the RSS values of a contacted tag will decrease once the finger touches the plastic. This reduction of the RSS values is reasonable because the plastic can be regarded as a kind of dielectric. Specifically, while touching, a capacitor will be constructed by three medium: the tag's antenna, the transparent plastic and the contacted fingertip. This newly constructed capacitor influences the electronic balance of the present circuit and a new balance will be formed afterwards. The new equivalent circuit induced by the fingertip is displayed in the right part of Fig. 2, where the capacitor C is formed by aforementioned three mediums and the impedance Z_F is introduced by the fingertip as well. Hence, the sum of all impedance Z_S caused by contacted fingertip is $Z_F + \frac{1}{j2\pi fC}$, where f is the frequency of the alternating current and j represents the square root of -1.

Conclusively, the new alternating current I_{new} is $\frac{V}{Z_A + Z_C + Z_S}$. Due to the introduction of C and Z_S, I_{new} is smaller than I quantitatively. Furthermore, the power of backscattered signals has positive correlation with the the alternating current 'flowing' in the tag. Hence, for a specific tag, the contact of the fingertip embeds the impedance feature into the signal' indicators (RSS and phase) of the tag. Moreover, the impedance of human body is proved qualified to be manipulated for identifying individuals. In [24], the impedance feature of human hand is amplified by coupling effect in a tag array to verify a user's identity.

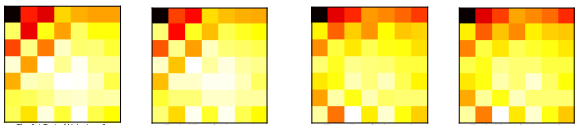
Geometry feature: A human hand can be discerned by its geometry, which makes the geometry of the hand be capable to be embodied as feature for user authentication. Song *et al.* [15] prove that the geometry of human hand is discernible and it is qualified to be used for identity verification. Therefore, the authors of [15] leverage both geometry feature and behavioral feature to authenticate smartphone users. In BioDraw, human hand is a reflector reflecting in-air signals back to the tag [6], which enables the tag harvest extra energy to backscatter signals with high RSS. Furthermore, different human hand, i.e., different geometries, yield different extra energy. We also conduct a related experiment to validate our analysis. A volunteer is asked to touch the edge part rather than the center part of the targeting tag. As a result, the RSS values are stable and low before touching. After touching, the RSS values of the tag increase because of the extra energy.

At present, we have figured out the complete procedure of the vari-



(a) The 1st test of volunteer 1. (b) The 2nd test of volunteer 1. (c) The 1st test of volunteer 2. (d) The 2nd test of volunteer 2.

Figure 3. The visualization result of the impedance feature. Deeper color means larger RSS value.



(a) The 1st test of volunteer 1. (b) The 2nd test of volunteer 1. (c) The 1st test of volunteer 2. (d) The 2nd test of volunteer 2.

Figure 4. The visualization result of the geometry feature. Deeper color means larger RSS value.

ation of the RSS value when the fingertip swipes across the tag: when a fingertip sliding from the tag's edge to the center, and then to another edge, the RSS value first increases (edge) and then decreases (center), at last it increases (edge) again. we can leverage this drastic variation of the RSS value to calculate the gradient of RSS curve to search contacted tags in the pattern (introduced in Section 6).

Composition feature : The surface composition of human hand is skin, and its permitivity is different from other materials. The reflected power of the RF signal, quantified by the RSS value, is sensitive to the reflection material. According to [16], when RF signals meet the interface between two different materials, reflection and incidence will occur concurrently. In BioDraw, transmitted RF signals meet the interface constructed by air and the skin. If we denote the electrical permitivities of air and skin as σ_A and σ_S respectively, the ratio relationship between reflection power P_R and incident power P_I can be formulated as: $\frac{P_R}{P_I} = |\frac{\sigma_A - \sigma_S}{\sigma_A + \sigma_S}|^2$. Hence, the signal power reflected by skin is different from the power reflected by other materials. This trait of power is deemed as a kind of biometric feature in BioDraw as well.

Behavioral feature: The behavioral feature of the human hand stems from human's swiping habit. Song *et al.* [15] have shown that the moving habit of human hand is distinguishable and can be utilized for user authentication. In BioDraw, drawing speed is a kind of behavioral feature which can be represented in time series, i.e., temporal domain.

4.2 Feasibility study

We designed and conducted four experiments to prove that the four biometric features are indeed involved into the backscattered signals and can be utilized for authentication.

Impedance validation: In the first experiment, for visualizing the impedance difference, each volunteer out of two volunteers was asked to touch the center tag in the tag array twice while the other parts of the tag array are covered by tinfoil paper (eliminating the influence of geometry feature). The RSS distributions of the tag array are shown in Fig. 3, which demonstrate that two RSS distributions of the same individual are similar but are distinguishable between different individuals. Moreover, we observed that within three months, the RSS distributions of the same user is stable. Thus, impedance feature is indeed contained in the backscattered signals and can be used to identify individuals.

Geometry validation: As shown in Fig. 4, in the second experiment, we visualized the geometry feature by asking volunteers to pose their hand in front of the tag array statically instead of touching. As expected, the RSS distributions of the same volunteer are similar but dissimilar between different volunteers. Though the individual difference of geometry feature is not as obvious as impedance, one can still easily find the difference between Fig. 4(a) and Fig. 4(c).

Composition validation: In the third experiment, one volunteer who participated in the first experiment was asked to attach different materials: nothing or paper or plastic glove on his hand while drawing. Thus the single variable is the reflection material, i.e., composition feature. We then labeled signal samples according to attached materials and used a neural network to classify these samples. The classification accuracy, 100%, indicates that composition feature is indeed contained by backscattered signals and is able to be utilized for authentication.

Behavioral feature validation: In the last experiment, a motor is leveraged to control the moving speed of the fingertip. Specifically, one end of a fine line is wrapped on the motor while the other end is wrapped on the fingertip. In this way, the moving speed of the fingertip is determined by rotation speed of the motor which is further determined by the driving voltage. We used two different voltages to introduce two different rotation speeds, i.e., two different moving speeds V_1 and V_2. One volunteer is required to draw the pattern '1' with two different speeds V_1 and V_2, where the only variable is the drawing speed, i.e., the behavioral feature. We then processed the signals and labeled the phase features produced by different speeds with 0 and 1 respectively. At last, a neural network is used to classify the phase features. The recognition accuracy is 100%, which declares that behavioral feature is contained in backscattered signals and can be utilized as a factor in MFUA.

We use the fusion feature of these four biometrics to identify users rather than using four individual biometrics to conduct fourfold identification because separately collecting each biometric needs multi-operations and the signal processing will be more complex.

5 BioDraw Design

The system overview is introduced in the first part of this section. The following parts are arranged to introduce the design of each module in BioDraw.

5.1 BioDraw overview

Recalling that BioDraw is a MFUA system, multiple factors are collected while authenticating. In the authentication procedure, the user only need to draw his/er secrete pattern on the tag array and concurrently fusion features carried by backscttered signals are collected by the server. Then the server processes the received raw data (original signals) and recognize the identity of the user. As shown in Fig. 5, BioDraw mainly contains four modules: *signal preprocessing*, *gradient-based pattern extraction*, *user identity recognition* and *key match*. The first module is used to preprocess the received raw signal and provide data with consist format (dimensionality) for the following modules. Then the pattern, which will be used for matching in the last module, is extracted by using a gradient-based algorithm in the *gradient-based pattern extraction* module. Meanwhile, the user's

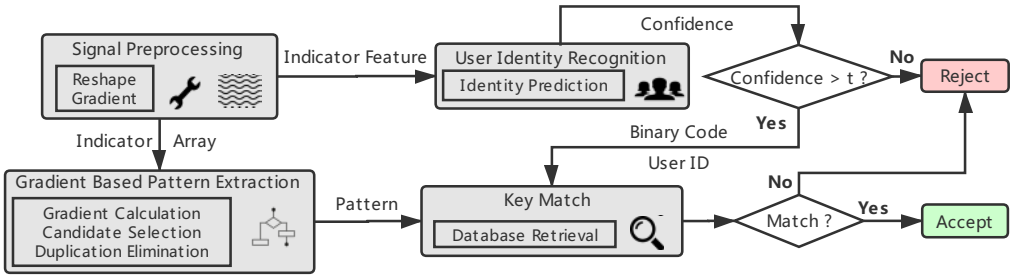


Figure 5. The workflow of BioDraw. BioDraw mainly consists of four modules: *signal preprocssing*, *gradient-based pattern extraction*, *User identity recognition* and *key match*.

identity is recognized by the *user identity recognition* module. The outputs of this module are the user's ID, corresponding confidence and the binary code. If the confidence is smaller than a threshold t, the authentication activity will be directly rejected. Through empirical study, we set t as 0.85 in BioDraw. In the last module, BioDraw matches two keys (pattern and user's ID) to decide whether this authentication activity should be accepted or not. Moreover, the new binary code is checked in this module, if the new binary code is found repetitive in the database, the new authentication activity is regarded as replay attack and rejected.

5.2 Signal preprocessing

The received raw data is preprocessed in this module. Before extracting pattern from the signal indicators of all n tags in the tag array (49 tags in our basic experiment setup), we align n time-series-format signal indicators so that they have the same length. Particularly, we first search the time stamps of the first anticlimax point and the last anticlimax point, between which the whole drawing procedure is recorded. Then we segment the signal series of each tag according to these two time stamps. Afterwards, an interpolation is used to align the n time series. In this way, we get n time-series-format RSS arrays, namely indicator arrays. We do not consider phase arrays because the periodical jump of the phase induced by moving hand obscures the trace of the pattern. Then the indicator arrays are inputted into *gradient-based pattern extraction* module. For forming the indicator feature for the *user identity recognition* module, BioDraw let the first saltation point as the beginning of the drawing. Then for each tag, 30 RSS values and 30 phase values received after the beginning time stamp are utilized to form 60 indicator arrays. In this way, the final indicator features prepared for user recognition have the dimension of $2 \times 30 \times 7 \times 7$, where '2' represents RSS and phase, '30' represents 30 time points and '7×7' represents 49 tags in our tag array.

5.3 Pattern recognition

After getting the indicator arrays from the first module, the gradient series of the time-series-format signal indicators of each tag are calculated based on our proposed pattern recognition algorithm. The details are elaborated in Section 6. In the end, the key pattern of the user is extracted and prepared for the last module of BioDraw.

5.4 User recognition

In this module, a CNN-LSTM-based classifier is employed to recognize users by using the indicator feature as input. The outputs of this module are three folds: binary code, user ID and its confidence. If the confidence that the input should be classified as this ID is smaller than 0.85, the authentication will be rejected without entering the last module. The details are introduced in Section 7.

5.5 Key match

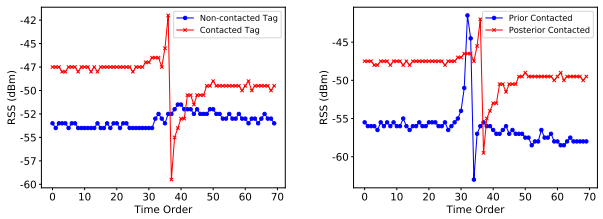
The data sources (key pattern and user identity) of this module are derived from the *gradient-based pattern recognition* module and the *user identity recognition* module. The user ID is then used as the key to search corresponding pattern in the database established when users register. Meanwhile, BioDraw compares the new extracted binary code with each binary code of the user stored in the database. If and only if the stored key pattern and the extracted key pattern are identical and the new binary code is different from any binary code stored in the database before, the user will be verified successfully. The details of binary code extraction are elaborately introduced in Section 8.

6 Pattern Extraction

The recognition of the pattern is crucial for BioDraw because the authentication activity is accepted if and only if the extracted pattern can correctly match the corresponding user ID stored in the database. In this section, we first present the trends of RSS variations of different kinds of tags, i.e., prior contacted tag, posterior contacted tag and non-contacted tag in the first part. Then we introduce how to calculate the gradient arrays of the RSS arrays. Afterwards, we show the method for contacted tag searching and false positive elimination. At last, BioDraw merges all repetitive contacted tags and extract a compete pattern.

6.1 RSS variation caused by drawing hand

Before pattern recognition, two kinds of RSS relationships are particularly need to be clarified, i.e., 1) the contacted tag and the non-contacted tag and 2) the prior contacted tag and posterior contacted tag. When both kinds of relationships are figured out, we can find all the contacted tags and confirm the contacted order of these contacted tags. Finally, the extracted electrical product codes (EPCs) of contacted tags and the contact order cooperatively specify the pattern.



(a) The RSS variation of contacted tag is more significant than that of non-contacted tag.

(b) The drastic RSS variation of prior contacted tag occurs earlier than that of posterior contacted tag.

Figure 6. The RSS variation difference between (a)non-contacted tag and contacted tag, (b)prior contacted tag and posterior contacted tag.

6.1.1 *Relationship one analysis*

For analyzing the RSS difference between the contacted tag and the non-contacted tag, we display their RSS curves in Fig. 6(a). The blue curve represents the RSS variation of the non-contacted tag and the red curve represents the RSS variation of the contacted tag. Through comparison between these two curves, we can summarize following two observations: 1) Both RSS curves vibrate noticeably when the fingertip is sliding on the tag array. 2) The vibration gradient and the vibration range of the curve of contacted tag are much more drastic than the vibration range of the curve of the non-contacted tag.

Based on above observations, there is potential to utilize a metric, which is capable to reflect the variation rate, to separate the contacted tag and non-contacted tag from all the tags in the tag array.

6.1.2 *Relationship two analysis*

We plot two curves which belong to two different contacted tags in the tag array in Fig. 6(b) to analyze the corresponding relationship. As can be easily observed from Fig. 6(b) that: 1) The drastic variation trend of the prior contacted tag is similar with the variation trend of posterior contacted tag. 2) The RSS peak of the prior contacted tag occurs earlier (in time domain) than the posterior contacted tag.

According to above two observations, We can design related algorithm to sort all contacted tags on the basis of their occurrence orders of RSS peaks in the time domain.

6.2 Gradient-based pattern recognition algorithm

For the sake of precise pattern extraction, four steps in our gradient-based algorithm need to be operated in succession: gradient calculation, contacted tag search, false positive elimination and repetitive tag merging.

6.2.1 *Gradient calculation*

Due to *relation one* shows that significant gradient difference exists between contacted tag and non-contacted tag, we design a gradient coefficient G for contacted tag searching. Recalling that the indictor array has been formed in the *signal preprocessing* module, we further leverage the RSS values in the RSS array of each tag to form a RSS window for each tag. The length L of the RSS window is the number of the RSS arrays in the window. The gradient coefficient G is then formulated as:

$$G_i^k = |\frac{RSS_{i+2}^k - RSS_i^k}{time_{i+2}^k - time_i^k}|, \quad i \in [1, L-2], \tag{1}$$

where G_i^k denotes the gradient coefficient of the k_{th} tag in the i_{th} RSS array and $|time_{i+2}^k - time_i^k|$ is the corresponding time interval. Then we reconstruct these 49 (49 tags) groups of RSS gradient coefficients as gradient coefficient array.

6.2.2 *Contacted tag search*

In this step, we search the candidate tags which are potential to be contacted tags. In each gradient coefficient array, those tags whose gradient coefficients are larger than a threshold GT are deemed as candidate tags. GT is an empirically set. If more than one candidate tags are extracted in the same gradient array, we choose the candidate tag whose time stamp is smallest as the contacted tag. In this way, no more than one tag is selected as candidate tag in each gradient coefficient array. If the fingertip is staying at the middle between two tags, no tag will be selected as candidate tag because their gradients are smaller than GT.

6.2.3 *Repetitive tags' IDs merging*

Recalling that our algorithm search candidate tags array by array, if the pattern is drawn slowly, it is possible that the same tag is selected in multiple continuous arrays as candidate tag, i.e., the fingertip is contacting on the same tag during the time interval of these continuous arrays. Fortunately, this issue can be easily solved by specifying that the two successive contacted tags must be different in BioDraw's pattern. Therefore, as a solution, we retrieve through the EPC sequence of contacted tags and merge all continuous repetitive tags.

By operating aforementioned three steps, we finally get a continuous contacted tag sequence which represents a specific pattern.

7 CNN-LSTM-based User Classifier

Recalling that the device employed to backscatter signals is a tag array composed of multiple tags and the tag array is a 2-dimensioal square, any two tags have a certain location relationship in the flat, namely spatial feature. Obviously, the geometry feature of a human hand can be represented by the location relationships (*e.g.*, the distance between two fingers) between any two different parts of the hand. It is worth noticing that CNN uses multi-dimensional kernels to extract spatial features in a multi-dimensional input [25, 9]. Thus CNN is significant qualified for geometry feature and composition extraction. Moreover, though we use perpendicular layout to alleviate the coupling effect between tags, slight coupling effect still exists between two adjacent tags. Hence, the introduction of the impedance of human hand not only changes the signal states of the specific contacted tag but also all the tags in the tag array. Therefore, the impedance feature can also be regarded as a kind of spatial feature in

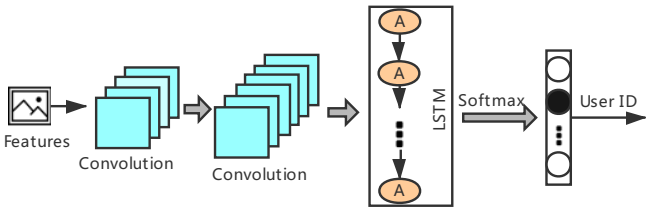


Figure 7. The architecture of CNN-LSTM-based user classifier.

BioDraw. By using CNN, impedance feature, geometry feature and composition feature can be extracted. As for the extraction of behavioral feature, LSTM is a suitable tool because it has been widely used to extract features in temporal domain and sequence data [25, 9] (*e.g.*, the vector converted from text in natural language processing).

Ultimately, a CNN-LSTM-based classifier is constructed for user recognition. As shown in Fig. 7, it mainly consists of two convolutional layers and a LSTM part. A batch normalization function and a ReLU activation function are adopted behind each convolutional layer. At last, a fully connected layer is utilized to project middle features into prediction confidences. BioDraw regards the ID which has the maximal confidence as the final result. Yet if the confidence is not as large as the threshold we set before, the new authentication activity will be regarded as replay attack and directly rejected.

8 Binary ALOHA

According to the tutorial about frame-slot-based ALOHA described in Section 2, the off-the-shelf randomness embedded in the frame-slot-based ALOHA protocol has potential to be leveraged for replay attack prohibition. In this section, we will descriptively introduce our tactful design, namely *Binary ALOHA*, towards replay attack detection. Particularly, *Binary ALOHA* can be easily implemented without introducing any modification on commercial devices.

As introduced, frame-slot-based ALOHA protocol primarily is used for collision avoidance in multi-tag communication settings, in which each tag randomly selects a slot in the given frame. In case a frame past, i.e., a round of communication is finished, the reader will reallocate a new frame with suitable number of slots according to the amount of readable tags in the previous round. In the next round, each tag will reselect a new slot. In this way, in each round, the order that the tags reply to the reader is random as well. It is the order randomness that allows us to devise a binary encoding scheme.

Specifically, we select two tags: T_A (with EPC_A) and T_B (with EPC_B) in our tag array as the encoding target. In each round of communication, the response order of T_A and T_B is uncertain and the order can be represented by their EPC sequence. An alternative encoding scheme is that: the order $[EPC_A, EPC_B]$ is regarded as '0' and the order $[EPC_B, EPC_A]$ is encoded as '1'. Therefore, in each communication round, a '0' or a '1' can be randomly obtained as one bit of the binary code. Though only one bit can be obtained in one round, when the randomness accumulates with the increasement of communication rounds, the randomness will be amplified infinitely.

Particularly, 30 arrays, i.e., 30 rounds, are used to form indicator features in BioDraw. By extracting 30 bits in 30 arrays, we can form a binary code with the length of 30 bits. Hence, BioDraw has a encoding space of 2^{30}, which is larger than 10^9. Statistically, if the encoding space is denoted as S and the use times of BioDraw is denoted as T, the probability that there is no repetitive binary code appears in T times of authentication activities can be calculated by:

$$P_{S,T} = \frac{(S-1)(S-2)\cdots(S-T+1)}{S^{T-1}}. \tag{2}$$

When we set S and T as 10^9 and 10^4 respectively, the probability $P_{10^9,10^4}$ is larger than 95%. It means that in 10^4 times of uses, the probability that each binary code is unique is larger than 95%. Meanwhile, 10^4 is a reasonable use times for user authentication. Furthermore, if a larger use times is necessary, more extra bits for binary code formalization is inevitable. However, enlarging the encoding space almost does not require extra effort. The only effort for the extension of the number of the bits in the binary code is extracting bits from more communication rounds.

In database retrieval, each user not only has a key pattern but also has previous used binary codes stored in the database. When a new authentication activity comes, a new binary code is extracted while the indicator features are formed. After the identity is recognized, the new binary code will be retrieved in the database accordingly. Only and if only no binary code which is the same as the new one is found in the database, this new authentication activity will be regarded as benign. This new binary code will be added in the database. Otherwise, the new extracted binary code will be discarded and this new authentication activity will be rejected. Due to that *Binary ALOHA* does not require any extra hardware, any multi-tag RFID system which adopts frame-slot-based ALOHA protocol is able to implement it readily.

9 Evaluation

In order to evaluate the performance of BioDraw, we built a prototype of BioDraw in a normal laboratory and conducted necessary related experiments to validate BioDraw quantitatively.

9.1 Implementation and experimental Setup

As shown in Fig. 8, the reader's antenna is placed 15cm away from the tag array parallelly, a user is drawing a pattern on the surface of the tag array. The hardware type of the reader, the 1-dimensional antenna and the tags used in BioDraw are Impinj R420 (COTs reader), Larid A9028 and Alien-9629, respectively. We use EPC Gen2 standard protocol for communication and frame-slot-based ALOHA protocol for collision avoidance. Furthermore, The communication procedure is achieved by *Visual Studio* with C#. We invited 21 volunteers (19 postgraduates and 2 teachers) from our laboratory to participate in the experiments and all the experiments were completed within three months. The ages of the volunteers vary from 20 years old to 44 years old and they are 7 females and 14 males.

9.2 Performance of BioDraw

In this part, we first define four metrics and then separately evaluate the performance of gradient-based pattern recognition algorithm, CNN-LSTM-based user classifier and *Binary ALOHA* with those four metrics. The security of BioDraw is elaborately analyzed in Section 10.

Four metrics: For evaluating BioDraw in quantity, we define four metrics: $similarity$, $accuracy$, *false reject rate* (FRR) and *defence success rate* (DSR). Among them, $similarity$ measures the performance of gradient-based pattern recognition algorithm. We calculate the $similarity$ between the ground truth pattern and the pattern extracted by our algorithm. The higher the $similarity$ is, the better the algorithm is. A higher $accuracy$ declares that our CNN-LSTM-based user classifier is better. Besides, BioDraw can be regarded as a user-friendly system if FRR is low. Due to that FRR indicates the performance of the whole system, we mainly consider the variation of FRR under different conditions.

Specifically, the metric $similarity$ represents how similar two patterns are, it can be formulated as:

$$similarity = \frac{L_O}{L_W}, \tag{3}$$

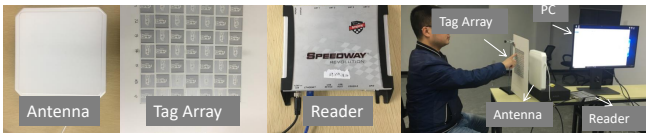


Figure 8. The experiment setup for the evaluation of BioDraw.

where L_O is the length (the number of the tags) of the overlapping fraction of two considered patterns and L_W is the length of the longest pattern between these two patterns. Likewise, $accuracy$ can also be represented by a formula: $accuracy = \frac{N_{cor}}{N_{all}}$, where N_{cor} is the number of corrected authenticated test samples and N_{all} is the number of all test samples. If N_M^i represents the number of the mistakenly recognized samples of user i and the number of all test samples of user i is denoted by N_A^i, FRR^i, i.e., the FRR of user i can be calculated by:

$$FRR^i = \frac{N_M^i}{N_A^i}. \tag{4}$$

DSR is defined to measure the security of BioDraw. Specifically, if we let N_{def} denote the number of times that BioDraw successfully defense against attacks and let N_{att} denote the number of times of attacks, DSR can be reprsesented by:

$$DSR = \frac{N_{def}}{N_{att}}. \tag{5}$$

Performance of the pattern recognition algorithm: As mentioned above, we define $similarity$ to evaluate the gradient-based pattern recognition algorithm. Hence, we asked the volunteers to draw ten different lengths of patterns where the lengths vary from 4 to 22 and with the stride of 2. For each length of pattern, each volunteer was required to draw it for 20 times. The final $similarity$ for a specific length of pattern is calculated by averaging the $similarities$ of samples from all volunteers. We found that in most of the lengths, the $similarities$ are 100%. When the length is 16, the $similarity$ is 98.75%, indicating that BioDraw extracted several wrong patterns. Intuitively, longer pattern leads to higher possibility of wrong pattern recognition. However, when the length continues increasing from 16 to 20, the $similarity$ increases back to 100%. This phenomenon demonstrates that the imperfect $similarity$ is probably caused by incautious negative experiment operation. In conclusion, our proposed gradient-based pattern extraction algorithm performs significantly well.

Performance of CNN-LSTM-based classifier: We first let each volunteer subjectively select a pattern as his/er key pattern and then each volunteer drew his/er key pattern for 50 times in different days. Finally, we conducted recognition via our classifier. As expected, the overall recognition accuracy is more than 99%+. Nearly all of the individual accuracy are 100%, which illustrates that our classifier can effectively extracts the fusion feature of the volunteers and recognizes volunteers accurately. Furthermore, to evaluate how BioDraw rejects authentic users, we display the FRR^i of each volunteer in Fig. 9(a). Though the false reject is possible to be triggered by three factors: low confidence, wrong classification and repetitive binary code, the negligible low FRR^i declares that user can get outstanding use experience. Nevertheless, the recognition accuracy under the worst condition in which that all the users choose the same key pattern should be explored. Therefore, we designed additional nine groups of exploratory experiments that all the volunteers share the same pattern in the same group. The lengths of patterns in different groups are different. In group one, the length is two-tags and the length of each latter group is one tag longer than the length of its first previous group. As a result, Fig. 9(b) shows that a good recognition accuracy as high as 90% can be achieved by only using two tags. When the length of the pattern is higher or equals four tags, the recognition accuracy increases to 99%, which is sufficient high for a user authentication system. Conclusively, to make BioDraw perform outstandingly, the lengths of the key patterns selected by users should larger than four tags. We then explore the effect of the volume of the training set in Fig. 9(c). The result shows that by training with only 35 samples per user, BioDraw can achieve significant high authentication accuracy. Considering the time consumption, collecting 35 samples costs each user no more than 2 minutes, which makes BioDraw user-friendly.

Performance of *Binary ALOHA*: We evaluated *Binary ALOHA* from the perspectives of storage space consumption and time consumption, and the evaluation results are displayed in Fig. 9(d). Recalling that *Binary ALOHA* prevents BioDraw from replay attack by comparing the new binary code with the previously used binary codes. We count the time consumption that the new binary code operates XOR with 10^4, 10^5, 10^6 and 10^7 binary codes respectively. As illustrated by the blue curve, even though the new binary code is operated XOR with all 10^7 binary codes one by one, the time consumption is under 1 seconds. This short time interval of XOR operations demonstrates that the new authentication activity would be processed by BioDraw promptly. The red curve, which represents the storage space consumption needed by *Binary ALOHA*, declares that the storage consumption only approximates 3.72GB even if 10^9 binary codes are stored in the database. If each user possesses 10^4 binary codes, BioDraw can concurrently protect 10^5 users from replay attack with the storage space less than 4GB.

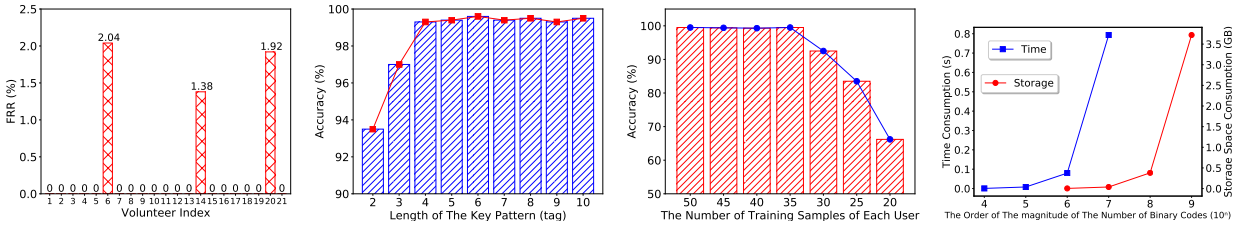
9.3 Related factors

9.3.1 Impact of ring, water and watch

In this part, we consider that some daily necessities such as ring and watch, may produce adverse effect on BioDraw. The water on the fingertip may trigger high FRR. The results are shown in Fig. 10(a), we collected data under different conditions and tested with the model trained by normal data. $R+WH$ means the combination of ring and watch, $R+WT$ means the combination of ring and water. Specifically, We first collected data when the volunteers were drawing with the ring, or the watch, or water, or the both of the ring and the watch, or the both of the watch and water on their hands. Then we evaluated BioDraw by using the model trained by data collected with no impact factor imposed on their hands. The results demonstrate that ring, watch and water indeed more or less have some adverse impacts on BioDraw. Making a comparison between individual factors, The ring triggers the smallest overall FRR (1.79%) and the water triggers the largest overall FRR (6.67%). When BioDraw is impacted by both water and ring, the overall FRR increases to 8.22%. The relatively trivial adverse impacts illustrate that BioDraw is robust.

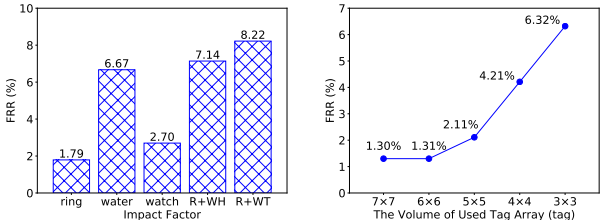
9.3.2 Impact of distance

In this part, we explore whether different distances between the antenna and the tag array induce different FRRs. We set the distance from 10cm to 20cm with stride of 2cm. It can be found that the FRRs



(a) The FRR^i of 21 volunteers. (b) The recognition accuracy under the worst condition. (c) The variation of recognition accuracy caused by the volume of the training set. (d) The storage space consumption and time consumption of *Binary ALOHA*.

Figure 9. The performance of BioDraw.



(a) The impact of ring, water and watch. (b) The impact of the volume of the tag array.

Figure 10. The performance of BioDraw under different related conditions.

induced by different distances are all less than 2%, i.e., the distance has negligible impact on BioDraw within 20cm.

9.3.3 Impact of tag array volume

At last we consider that the volume of the tag array may has impact on BioDraw because the volume of the tag array is directly related to the volume of the indicator features. We found from Fig. 10(b) that the FRR produced by using the tag array with size (volume) of 7×7 tags is significantly similar with the FRR produced by using the tag array with size of 6×6 tags. However, the FRR increases 5.01% when the volume decreases from 6×6 to 3×3. Yet, the FRR is still small even if only nine tags are utilized to collect indicator features, which proves that BioDraw is flexible with regards to the volume of the tag array.

9.4 Comparison with existing works

We compare BioDraw with three outstanding wireless signal-based authentication systems proposed in recent years: RF-Mehndi [24], WiFi-ID [23] and WiWho [22]. Considering the user-friendless, BioDraw, WiWho and WiFi-ID are device-free while RF-Mehndi is device-need. Considering the security, BioDraw can defend against replay attacks, RF-Mehndi can defend them to some extent, while WiFi-ID and WiWho are incapable to defend them.

10 Security Analysis

10.1 Threat model

Except for the replay attack, we design other three threat models in this part.

Zero-effort attack: In this attack, the attacker has little knowledge about the victim's key. The attacker randomly selects a pattern to attempt to be recognized as the victim by BioDraw. While drawing, the attacker use his/er own natural drawing speed.

Pattern-behavior-aware attack: In this attack, the attacker first observes the activity of the victim while the victim is authenticating. Afterwards the attacker tries to draw the correct pattern of the victim and mimic the drawing speed of the victim.

Pattern-geometry-material-behavior-aware attack: Pattern-geometry-material-behavior-aware attack (PGMBA) is a kind of 4-factor-aware attack. We assume that the attacker is aware of the pattern and can counterfeit the geometry feature, material feature and behavioral feature of the victim.

Replay attack: In this attack, the attacker first records the authentication signals while the victim is authenticating. Then the recorded signals are replayed to BioDraw by the attacker.

10.2 Attack simulation

Key pattern is the first handicap which protects BioDraw from attacks. If the attacker attempts to attack BioDraw by impersonating the victim, s/he must speculates the key pattern of the victim first. However, it is significantly difficult for the attacker to speculate because the pattern space is extremely large. Recalling that the fusion feature composed of four kinds of features are utilized to specify a person, though behavioral feature is easy to be mimicked, the geometry feature, material feature and impedance feature which reflect the biometric characteristics of users are significantly difficult to be filched. Even if more than 3 factors are forged by the attacker, the remaining features would prohibit the attack. Therefore, the attack conducted by using counterfeiting hand is ineffective. We conduct four simulation experiments towards four different threat models in this part.

Zero-effort attack: For evaluating BioDraw's ability of defending against zero-effort attack, we randomly invited 10 volunteers to select 10 patterns according to their preference. Then nine volunteers (attackers) were asked to guess the pattern of the remaining volunteer (victim). Each attacker has five chances to guess the victim's pattern. As a reslut, no attacker can correctly speculate the victim's pattern because the pattern space is extremely large.

Pattern-behavior-aware attack: As for the pattern-behavior-aware attack, we randomly selected five pairs of attackers and victims. In each pair, the attacker first learned the pattern and the drawing behavior of the victim. Then the attacker attempted to authenticate with BioDraw for 40 times. The experiment result, 100% of

DSR, indicates that BioDraw is capable to defend against pattern-behavior-aware attack effectively. The attack activities are rejected either because of the low confidence or because of the wrong prediction.

PGMBA: For simulating PGMBA, we asked two volunteers to attach paper on their hands and let them "impersonate themselves" for 40 times. The defense results show that the DSR is higher than 99%, which means the impedance feature prevents BioDraw from PGMBA successfully.

Replay attack: We invited 10 volunteers to replay their before used signals to BioDraw. As a result, all replayed signals are rejected.

11 Discussion

Recalling that we employ a CNN-LSTM-based deep model to extract fusion features and recognize users, thus we do not extract the fusion feature by mathematical calculation. If we can extract it as a 1-dimensional feature vector, it is possible to use a more lightweight machine learning algorithm to recognize users. Further, if we make a feature vector as feature template, we can easily recognize users by calculating the *Pearson correlation coefficient* between the template and new extracted feature vector [18]. Specifically, if the calculated *Pearson correlation coefficient* is larger than a threshold we set before, we will accept this authentication activity.

12 Conclusion

We propose a 5-factor user authentication system named BioDraw, in which five verification factors: key pattern, impedance feature, geometry feature, material feature and behavioral feature are simultaneously used to complete the verification of the user's identity. The key pattern recognition is realized by using a gradient-based pattern recognition algorithm. For user identity recognition, a CNN-LSTM-based classifier is leveraged to recognize the user's identity. A novel technique, namely *Binary ALOHA*, is designed to prohibit replay attack. Through a series of experiments within three months, we prove that BioDraw can perform significant well on pattern recognition and the average FRR for user authentication is as low as 1.30%.

REFERENCES

[1] Iphone fingerprint sensor hacked with a finger made of clay at mwc. http://www.techworm.net/2016/02/, 2016.

[2] Muhammad Naveed Aman, Mohamed Haroon Basheer, and Biplab Sikdar, 'Two-factor authentication for iot with location information', *IEEE Internet of Things Journal*, **6**(2), 3335–3351, (2019).

[3] Panagiotis Andriotis, George C. Oikonomou, Alexios Mylonas, and Theo Tryfonas, 'A study on usability and security features of the android pattern lock screen', *Inf. & Comput. Security*, **24**(1), 53–72, (2016).

[4] Wen-Shiung Chen and Wei-Chang Wang, 'Fusion of hand-shape and palm-print traits using morphology for bi-modal biometric authentication', *IJBM*, **10**(4), 368–390, (2018).

[5] Sanchari Das, Bingxi Wang, and L. Jean Camp, 'MFA is a waste of time! understanding negative connotation towards MFA applications via user generated content', *CoRR*, **abs/1908.05902**, (2019).

[6] Jinsong Han, Chen Qian, Xing Wang, Dan Ma, Jizhong Zhao, Wei Xi, Zhiping Jiang, and Zhi Wang, 'Twins: Device-free object tracking using passive tags', *IEEE/ACM Trans. Netw.*, **24**(3), 1605–1617, (2016).

[7] Zhong Huang, Rui Xu, Chu Chu, Zhenbing Li, Yubin Qiu, Jian Li, Yugang Ma, and Guangjun Wen, 'A novel cross layer anti-collision algorithm for slotted aloha-based UHF RFID systems', *IEEE Access*, **7**, 36207–36217, (2019).

[8] S. Ilankumaran and Deisy Chelliah, 'Multi-biometric authentication system using finger vein and iris in cloud computing', *Cluster Computing*, **22**(Suppl 1), 103–117, (2019).

[9] Md Tamzeed Islam and Shahriar Nirjon. Wi-fringe: Leveraging text semantics in wifi csi-based device-free named gesture recognition, 2019.

[10] Masashi Komatsu and Takako Akakura, 'A facial authentication method robust to postural changes in e-testing', in *Human Interface and the Management of Information. Information in Intelligent Systems - Thematic Area, HIMI 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26-31, 2019, Proceedings, Part II*, pp. 372–384, (2019).

[11] Li Li, Siqin Zhou, and Hang Tu, 'Fingerprint authentication based on fuzzy extractor in the mobile device', *IJESDF*, **11**(3), 321–337, (2019).

[12] Trinh Hoang Nam and Vuong Duc Hoang Quan, 'Multi-dimensional analysis of perceived risk on credit card adoption', in *Beyond Traditional Probabilistic Methods in Economics, ECONVN 2019, International Econometric Conference of Vietnam, Ho Chi Minh City, Vietnam, 14-16 January, 2019*, pp. 606–620, (2019).

[13] Obi Ogbanufe and Dan J. Kim, 'Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment', *Decision Support Systems*, **106**, 1–14, (2018).

[14] Srinivasan Rajarajan and Ponnada Priyadarsini, 'UTP: a novel PIN number based user authentication scheme', *Int. Arab J. Inf. Technol.*, **16**(5), 904–913, (2019).

[15] Yunpeng Song, Zhongmin Cai, and Zhi-Li Zhang, 'Multi-touch authentication using hand geometry and behavioral information', in *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*, pp. 357–372, (2017).

[16] Deepak Vasisht, Guo Zhang, Omid Abari, Hsiao-Ming Lu, Jacob Flanz, and Dina Katabi, 'In-body backscatter communication and localization', in *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication, SIGCOMM 2018, Budapest, Hungary, August 20-25, 2018*, pp. 132–146, (2018).

[17] Chuyu Wang, Jian Liu, Yingying Chen, Hongbo Liu, Lei Xie, Wei Wang, Bingbing He, and Sanglu Lu, 'Multi - touch in the air: Device-free finger tracking and gesture recognition via COTS RFID', in *2018 IEEE Conference on Computer Communications, INFOCOM 2018, Honolulu, HI, USA, April 16-19, 2018*, pp. 1691–1699, (2018).

[18] Ge Wang, Haofan Cai, Chen Qian, Jinsong Han, Xin Li, Han Ding, and Jizhong Zhao, 'Towards replay-resilient RFID authentication', in *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, MobiCom 2018, New Delhi, India, October 29 - November 02, 2018*, pp. 385–399, (2018).

[19] Cihui Xie and Ajay Kumar, 'Finger vein identification using convolutional neural network and supervised discrete hashing', *Pattern Recognition Letters*, **119**, 148–156, (2019).

[20] Tong Xin, Bin Guo, Zhu Wang, Mingyang Li, Zhiwen Yu, and Xingshe Zhou, 'Freesense: Indoor human identification with wi-fi signals', in *2016 IEEE Global Communications Conference, GLOBECOM 2016, Washington, DC, USA, December 4-8, 2016*, pp. 1–7, (2016).

[21] Can Ye, B. V. K. Vijaya Kumar, and Miguel Tavares Coimbra, 'Heartbeat classification using morphological and dynamic features of ECG signals', *IEEE Trans. Biomed. Engineering*, **59**(10), 2930–2941, (2012).

[22] Yunze Zeng, Parth H. Pathak, and Prasant Mohapatra, 'Wiwho: Wifi-based person identification in smart spaces', in *15th ACM/IEEE International Conference on Information Processing in Sensor Networks, IPSN 2016, Vienna, Austria, April 11-14, 2016*, pp. 4:1–4:12, (2016).

[23] Jin Zhang, Bo Wei, Wen Hu, and Salil S. Kanhere, 'Wifi-id: Human identification using wifi signal', in *International Conference on Distributed Computing in Sensor Systems, DCOSS 2016, Washington, DC, USA, May 26-28, 2016*, pp. 75–82, (2016).

[24] Cui Zhao, Zhenjiang Li, Ting Liu, Han Ding, Jinsong Han, Wei Xi, and Ruowei Gui, 'Rf-mehndi: A fingertip profiled RF identifier', in *2019 IEEE Conference on Computer Communications, INFOCOM 2019, Paris, France, April 29 - May 2, 2019*, pp. 1513–1521, (2019).

[25] Yue Zheng, Yi Zhang, Kun Qian, Guidong Zhang, Yunhao Liu, Chenshu Wu, and Zheng Yang, 'Zero-effort cross-domain gesture recognition with wi-fi', in *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services, MobiSys 2019, Seoul, Republic of Korea, June 17-21, 2019.*, pp. 313–325, (2019).