RFace: Anti-Spoofing Facial Authentication Using COTS RFID

Weiye Xu[1], Jianwei Liu[1], Shimin Zhang[1], Yuanqing Zheng[2], Feng Lin[1], Jinsong Han[1], Fu Xiao[3], and Kui Ren[1]

[1]Zhejiang University, China
[2]The Hong Kong Polytechnic University, Hong Kong, China
[3]Nanjing University of Posts and Telecommunications, China
xuweiye@zju.edu.cn, liujianwei@stu.xjtu.edu.cn, shiminzsm@gmail.com, yqzheng@polyu.edu.hk,
flin@zju.edu.cn, hanjinsong@zju.edu.cn, fuyxiao@126.com, kuiren@zju.edu.cn

***Abstract*—Current facial authentication (FA) systems are mostly based on the images of human faces, thus suffering from privacy leakage and spoofing attacks. Mainstream systems utilize facial geometry features for spoofing mitigation, which are still easy to deceive with the feature manipulation, *e.g.*, 3D-printed human faces. In this paper, we propose a novel privacy-preserving anti-spoofing FA system, named RFace, which extracts both the 3D geometry and inner biomaterial features of faces using a COTS RFID tag array. These features are difficult to obtain and forge, hence are resistant to spoofing attacks. RFace only requires users to pose their faces in front of a tag array for a few seconds, without leaking their visual facial information. We build a theoretical model to rigorously prove the feasibility of feature acquisition and the correlation between the facial features and RF signals. For practicality, we design an effective algorithm to mitigate the impact of unstable distance and angle deflection from the face to the array. Extensive experiments with 30 participants and three types of spoofing attacks show that RFace achieves an average authentication success rate of over 95.7% and an EER of 4.4%. More importantly, no spoofing attack succeeds in deceiving RFace in the experiments.**

I. Introduction

In recent years, facial authentication (FA) systems have been wildly applied to daily applications (*e.g.*, access control, online payment and individual identification [1, 2, 3]). FA is regarded as a promising alternative to traditional authentication approaches, such as PIN code [4], fingerprint [5] and token [6] thanks to its convenience and precision.

Existing FA systems are mostly camera-based and have some severe flaws, including privacy leakage risks and security problems. On the one hand, most current FA systems collect facial features of users by RGB cameras, which inevitably reveals complete visual facial information (VFI) and raises privacy concerns. On the other hand, these approaches perform authentications by extracting geometry features from VFI. Once the VFI of a user is leaked, an attacker can easily conduct a spoofing attack by reproducing the features [7]. Although more geometry information has been introduced to enhance the security, *e.g.*, the depth information of faces [8], camera-based FA systems are still vulnerable to spoofing attacks. This is because the information can still be captured remotely, *e.g.*, using depth cameras or infrared dot projectors [9]. Therefore, attackers can manipulate a 3D-printed mask based on the captured VFI to deceive FA systems [10]. To overcome these drawbacks, we explore a new facial feature based authentication technique, which can protect the visual privacy of users, and meanwhile resist spoofing attacks.

Jinsong Han and Yuanqing Zheng are the corresponding authors.

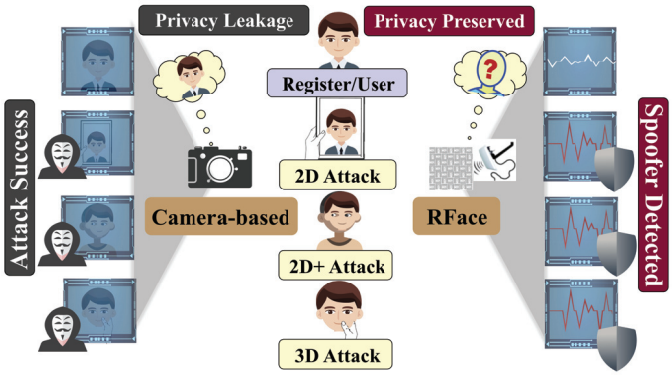


Fig. 1: Compared with camera-based systems, *RFace* is privacy-preserving and can effectively resist spoofing attacks.

It is worth noting that biomaterial-based FA has become more reliable against spoofing attacks [11]. Meanwhile, recent advances in wireless sensing reveal that radio frequency (RF) signals are sensitive to the material that they encounter during propagation [12]. Thus, by verifying the facial information captured in RF signals, we can determine the authenticity of users. Furthermore, researchers show that an array of commercial-off-the-shelf (COTS) radio frequency identification (RFID) tags can serve as a low-cost and sensitive sensor to support fine-grained wireless sensing [13, 14]. Motivated by the material-sensitive and fine-grained sensing capability of RFID systems, we attempt to develop an anti-spoofing FA system with COTS RFID devices.

In this paper, we propose a novel anti-spoofing privacy-preserving authentication system, named RFace. Specifically, RFace uses an RFID tag array to measure both RSS and phase of RF signals and extract 3D facial geometry and biomaterial features for spoofing attack resistant. The extracted features are then fed into a well-trained support vector machine (SVM) to conduct authentication. As shown in Fig. 1, compared with camera-based systems, RFace protects the VFI of users. RFace

is also resistant to spoofing attacks since the extracted features are difficult to be captured by attackers.

There are two main challenges in the design and development of RFace: (1) It is difficult to build the correlation model between real facial features and raw RF signals since RF signals are not as structured as images. (2) For each user, the distance and deflection from the face to the tag array may slightly vary in different authentication attempts, leading to undesirable degradation of the authentication accuracy due to the sensitivity of RF signals.

To address the first challenge, we build a theoretical model based on the principles of electromagnetism and RF signal propagation. The model rigorously proves the feasibility of leveraging RF signals to capture and extract the desired facial features from raw backscatter signals. For the second challenge, we try to explore a feature resistant to the variation of distance and deflection angle. Based on experiments and theoretical analysis, we find that in the tag array, the difference values of RSS and phase of two tags is related to the distance between the two tags. Specifically, the RSS and phase differences of two tags that are close to each other are more stable than that of two tags with a far distance, especially when the distance and deflection angle vary. Therefore, we take the RSS and phase differences of two tags within a tiny area as the final stable feature. We propose a novel algorithm, named DDDS, to split the array into minimum blocks, *i.e.*, a tag with its adjacent tags, in which the tags leverage their stable difference values of RF signals towards the variation to mitigate the degradation in the authentication accuracy.

RFace is implemented with COTS RFID devices. To perform user authentication, users are only required to pose their faces in front of a tag array for a few seconds. We evaluate RFace with 30 volunteers under various distance and deflection conditions. We also test RFace against three types of mainstream spoofing attacks, including 2D, 2D+ and 3D spoofing attacks. The results demonstrate the effectiveness of RFace with over 95.7% authentication success rates and around 4.4% equal error rates. More importantly, the results of defense experiments indicate that RFace is resistant to spoofing attacks, including 3D mask attacks. Our contributions can be summarized as follow:

- We propose a novel privacy-preserving anti-spoofing FA system, RFace, which can extract both 3D facial geometry and biomaterial features of users' faces from RF signals. In addition, we build a theoretical model to validate the feasibility of the feature extraction method.
- We propose a novel algorithm to enhance the flexibility of RFace by mitigating the impact of distance and deflection variations between human face and tag array.
- We build a prototype of RFace with COTS RFID devices. Extensive experiments demonstrate that RFace can achieve precise and robust authentication and defend against various spoofing attacks.

II. Preliminary

In this section, we start with some preliminary studies on two elemental indicators of RF signals and the layout of tag array that facilitates the feature collection. Then we introduce three types of typical attacks for existing FA systems.

A. Elemental Indicators of RF Signals and Tag Array Layout

RF Signal Indicators: A typical RFID system includes three parts, RFID tags, a reader and its antenna. The reader continuously transmits RF signals to activate tags. Then each tag responds its Electronic Product Code (EPC) by backscattering RF signals using ON-OFF keying [15]. By analyzing the backscatter signals, the reader can obtain the indicators, *i.e.*, received signal strength (RSS) and phase. Both indicators are influenced by the propagation distance and the materials encountered. In this paper, RFace measures the indicators to extract facial features. The concrete mathematical model will be presented in Section III-A.

In this work, we utilize the *Impinj Speedway R420* reader which can achieve a phase resolution of 0.0015 radians in theory [16]. Thus, with the corresponding wavelength about $32cm$, it is capable of providing $\approx 320mm * 0.0015/(4 \times 3.14) = 0.038mm$ distance resolution, which suffices to capture the geometry feature of human face.

Tag Array Layout: We adopt a perpendicular orientation deployment of tags as in [14]. Additionally, for the purpose of avoiding two tags on a tag array from sharing the same phase, we ensure the maximum distance between any two tags on an array is less than half of the wavelength (approximates $16cm$). Specifically, we use the tiny RFID tag *AZ-9629* (only $2.25cm \times 2.25cm$) to arrange a compact 7×7 tag array with the geometry of $16cm \times 16cm$ square space, which is capable to cover whole faces in most cases.

B. Attacks

We mainly consider the following three types of attacks to FA systems.

2D Spoofing Attack: This attack includes both 2D static (photo) attack and dynamic (video) attack. 2D spoofing attacks aim to deceive an FA system with a 2D photo (video) of a legitimate user's face. Most traditional 2D feature based FA systems are vulnerable to this attack. As reported in [17], a 2D photo can deceive the face recognition systems of some mainstream smartphones.

2D+ Spoofing Attack: This attack constructs an uneven mask based on a precise 2D image plus rough depth measurements of a legitimate user's face. Such an attack can deceive many existing anti-spoofing FA systems[2] that only look for uneven surface rather than matching against the facial depth information exactly.

3D Spoofing Attack: This attack constructs a precise 3D-printed mask of a legitimate user. 3D spoofing attacks are hard to defeat, since current FA systems only extract the 3D structural features of face surface, while leaving the inner composition, *e.g.*, the biomaterial of faces, unexamined. In

this case, using a vivid 3D-printed mask can easily trick these FA systems [18].

III. Turning RFID Into Facial Features Extractor

In order to establish the correlation between RF signals and both the 3D geometry and inner biomaterial features of faces, we build a theoretical model based on the principles of electromagnetism and RF signal propagation. Besides, we conduct several experiments to test the feasibility of anti-spoofing face authentication.

A. Modeling Face Features upon RF Signal Propagation

Modeling Consideration: In our system, the received signals consist of three parts: the line-of-sight signal, the signal reflected from other surrounding objects and the signal reflected from face. The line-of-sight signal can be regarded as a consistent one when the distance between the antenna and the tag array remains static, In the FA scenario, the distance between other surrounding objects and the tag array is normally much larger than the one between the face and the tag array. As a result, the face would contribute the most of the impact on the tag array in terms of RF interaction. Therefore, we focus on the signal reflected from the face in our model. Moreover, we utilize the RSS and phase of received signals to extract the user's facial features. We demonstrate that the extracted features can represent both the unique *3D geometry* and *inner biomaterial* features of human face in the following.

As illustrated in Fig. 2, the human face is parallel and located directly in front of the tag array, and the user's chin is located on the vertical bisector of the bottom edge of the tag array. We utilize the lateral view of the 7×7 tag array to interpret the effect of the signal reflected from the face on the tag array. We denote the distance between the antenna and the tag array as L and the distance between the tag array and the chin as d. Our theoretical model involves three processes: 1) mapping tags to blocks on face, 2) extracting facial features by RSS and 3) extracting facial features by phase.

Mapping Tags to Blocks on Face: In order to precisely extract facial features, it is essential to map tags to their corresponding areas on a face. Due to the sensitivity of RF signal, each tag on the tag array backscatters the reflection signal from the entire face. Thus, each tag captures the features of the entire face. Nevertheless, the face will have a greater impact on those tags closer to the face [14]. Therefore, without losing the effectiveness of modeling, for each tag, we analyze the influence on the tag from the area on the face which is closest to the tag. In specific, we map each tag on the array to an area closest to the tag on the face, which can be regarded as a block. For ease of modeling, this reflection can be equivalent to the effect of the center point of this block on the tag. Taking tag T_i as an example, the corresponding reflection block is represented as the closest area (F_{u_i}, F_{c_i}, F_{l_i}), where F_{u_i}, F_{c_i}, F_{l_i} represent the upper vertex, center point and lower vertex of this block on the face, respectively. Therefore, the signal reflected from this block and received by tag T_i can be regarded as the signal reflected from the center point F_{c_i} and

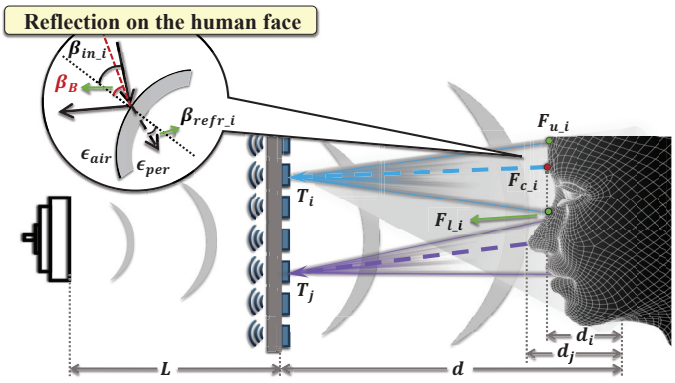


Fig. 2: RF signal propagation model.

we denote the incident angle of RF signal propagating into human face at F_{c_i} as β_{in_i}. In addition, for distinct human faces, each tag on tag array has different specific reflection area with corresponding center point and incident angle. Then we will take tag T_i and tag T_j as an instance to analyze the impact of RF signals reflected from human face on RSS and phase, and show how to extract facial features.

Facial Features Extracted by RSS: We divide the propagation of RF signals in our system into three stages: from antenna to face, reflection on face and from face to antenna. We analyze the change of RSS in each stage respectively to extract both 3D geometry and inner biomaterial features.

As for the first propagation stage, the RSS value is defined by the power P, which is proportional to the square of the amplitude A. The RSS can be formulated as:

$$RSS = 10 \log \frac{P}{10^{-3}} = 20 \log(DA) \quad (P \propto A^2), \tag{1}$$

where D is a constant. Generally, the amplitude A causes exponential loss in magnitude over a unit of propagation distance, which can be denoted as $e^{-\alpha}$. For the tag T_i in Fig. 2, the loss of amplitude A during the propagation of RF signal from antenna to the center point F_{c_i} of the corresponding reflection block (F_{u_i}, F_{c_i}, F_{l_i}) on face can be denoted as:

$$A_{in} = Ae^{-\alpha(L+d-d_i)}. \tag{2}$$

In this equation, A_{in} represents the amplitude of the RF signal when it reaches the surface of face. d_i denotes the horizontal distance between the center point F_{c_i} and chin, which indicates the 3D facial geometry feature of human face.

For the second propagation stage, the RF signal reaches the surface of human face. The signal can be divided into two parts: the part directly reflected and the part entering the face with refraction. The inner structure of human face consists of various biomaterials such as skin, fat, and muscle. For ease of illustration, we assume that each person's face is a unique hybrid material composed of multiple layers of materials, and the relative permittivity of the mixed biomaterial can be denoted as ϵ_{per}. According to [12], the RF signal refracted into the face has to traverse multi-layered tissue and go through multiple reflections before it can escape. Due to the exponential attenuation, there will be only very low power signal to escape the human face, which can be ignored. Then

we mainly analyze the power loss caused by reflection on the face surface. The power ratio of the signal before and after reflection on the face surface is the power reflection coefficient R_{per_i}, so the corresponding amplitude can be calculated as:

$$A_{\_after} = \sqrt{R_{per\_i}} A_{\_before}, \tag{3}$$

where $A_{\_before}$ and $A_{\_after}$ are the amplitudes of the corresponding before and after reflection signal. R_{per_i} is related to the mixed material of human face and the incident angle β_{in_i}. So R_{per_i} can reveal the facial features of human face. Then we analyze the factors that affect R_{per_i} in detail.

The reflection on an interface between two biomaterials is affected by the relative permittivity ϵ of them. Considering the RF signal arriving at the face surface which is the interface between the air (ϵ_{air}) and the face material (ϵ_{per}), the signal can be decomposed into transverse electric (TE) and transverse magnetic (TM) wave components, according to [19]. The power reflection coefficient R_{per_i} can be calculated by R_s and R_p, which are the power reflection coefficient of TE and TM wave components separately. Besides according to Fresnel formula [19], R_{per_i} can be represented as:

$$\begin{aligned} R_{per\_i} &= R_s R_p \\ &= \left| \frac{\sqrt{\epsilon_{per}} cos\beta_{refr\_i} - \sqrt{\epsilon_{air}} cos\beta_{in\_i}}{\sqrt{\epsilon_{per}} cos\beta_{refr\_i} + \sqrt{\epsilon_{air}} cos\beta_{in\_i}} \right|^2 \\ &\times \left| \frac{\sqrt{\epsilon_{per}} cos\beta_{in\_i} - \sqrt{\epsilon_{air}} cos\beta_{refr\_i}}{\sqrt{\epsilon_{per}} cos\beta_{in\_i} + \sqrt{\epsilon_{air}} cos\beta_{refr\_i}} \right|^2, \end{aligned} \tag{4}$$

where β_{refr_i} denotes the refraction angle. Furthermore, according to Snell's Law[19], R_{per_i} is only determined by ϵ_{per} and β_{in_i}. Therefore, in the propagation stage of reflection on face, the value of R_{per_i} involves both the inner biomaterial and 3D geometry features of human face.

Then for the last propagation stage from face to antenna, combining with Eq. 2 and Eq. 3, the amplitude of received signal A_r can be calculated as:

$$A_r = \sqrt{R_{per\_i}} A e^{-2\alpha(L+d-d_i)}. \tag{5}$$

According to Eq. 1, the RSS of the received signal RSS_i for tag T_i can be denoted as:

$$RSS_i = 20\log(DA_r) = 20\log\left[D\sqrt{R_{per\_i}} A e^{-2\alpha(L+d-d_i)}\right]. \tag{6}$$

We can find that the value of RSS is relevant to the distance (d) between the tag array and chin, and d is an unstable factor because of the movement of human face. In order to better extract stable facial features, we then subtract the RSS values of these two tags T_i and T_j to remove the impact of d, which is irrelevant to the structure of human face. Then we can gain:

$$\begin{aligned} RSS_i - RSS_j &= 20\log\frac{D\sqrt{R_{per\_i}} A e^{-2\alpha(L+d-d_i)}}{D\sqrt{R_{per\_j}} A e^{-2\alpha(L+d-d_j)}} \\ &= 20\log\left[\frac{\sqrt{R_{per\_i}}}{\sqrt{R_{per\_j}}} e^{-2\alpha(d_j-d_i)}\right]. \end{aligned} \tag{7}$$

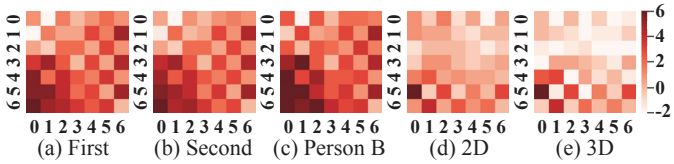


Fig. 3: RSS difference distributions of various sensing targets.

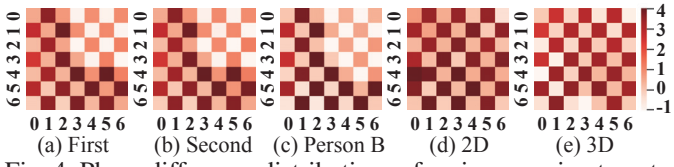


Fig. 4: Phase difference distributions of various sensing targets.

It can be observed that the factor d has been eliminated and the value of $RSS_i - RSS_j$ only related to R_{per_i}, R_{per_j} and $d_j - d_i$. Among these variables, R_{per_i} and R_{per_j} involve both the inner biomaterial feature and 3D geometry feature of human face which vary among persons. Meanwhile $d_j - d_i$ represents the horizontal distance between the center points of two different blocks on the human face, which also indicates the 3D geometry feature of human face. Therefore, we can conclude that the difference between the RSS values of the tags can reveal both distance-resistant 3D geometry and inner biomaterial features of human face.

Facial Features Extracted by Phase: Similar to RSS, we analyze the changes of phase according to the three stages of RF signal propagation in our model successively. Taking tag T_i as an example, the phase of the RF signal transmitted from the antenna before entering face ($\theta_{\_before}$) can be expressed as:

$$\theta_{\_before} = \theta_t + \frac{2\pi}{\lambda}(L + d - d_i), \tag{8}$$

where θ_t represents the initial phase value of the transmitter. As aforementioned, the signal is thought to be unable to escape once it enters the face, so only the reflections that occur on the surface of human face are considered. In this case, the phase of the RF signal ($\theta_{\_after}$) after reflection can be calculated as:

$$\theta_{\_after} = \theta_{\_before} + \theta_{per\_i}, \tag{9}$$

where θ_{per_i} denotes the phase variation caused by reflection at the human face. We then show that θ_{per_i} is also related to the facial features. According to[19], after reflections, there will be a phase change when the angle of incidence (β_{per_i}) is larger than Brewster angle (β_B):

$$\begin{cases} \theta_{per\_i} = 0, & \beta_{per\_i} \le \beta_B \\ \theta_{per\_i} = \pi, & \beta_{per\_i} > \beta_B \end{cases}, \beta_B = arctan\sqrt{\frac{\epsilon_{per\_i}}{\epsilon_{air}}}. \tag{10}$$

Therefore, θ_{per_i} is decided by ϵ_{per_i} and β_{per_i}, which means that the value of the phase variation (θ_{per_i}) caused by reflection on human face can reveal both the inner biomaterial and 3D facial geometry features of the face.

Combining with the phase changes in the third stage and substituting Eq. 8 into Eq. 9, we can obtain the final phase of

the received RF signal for tag T_i as:

$$\begin{aligned}\theta_i &= \left[\theta_{\_after} + \theta_{tag\_i} + \frac{2\pi}{\lambda}(L + d - d_i)\right] \mod 2\pi \\ &= \left[\theta_t + \theta_{per\_i} + \theta_{tag\_i} + \frac{4\pi}{\lambda}(L + d - d_i)\right] \mod 2\pi,\end{aligned} \tag{11}$$

where θ_{tag_i} denotes the additional phase shift caused by the characteristic of tag. Similarly, to remove the factor d, we subtract θ_i with θ_j and the result can be denoted as:

$$\begin{aligned}\theta_i - \theta_j =&(\theta_{per\_i} - \theta_{per\_j}) + (\theta_{tag\_i} - \theta_{tag\_j}) \\ &+ \frac{4\pi}{\lambda}(d_j - d_i) + 2k\pi, k \in Z.\end{aligned} \tag{12}$$

It is worth noting that there is a term $2k\pi$ in theory since the phase of the received RF signal is a periodic function with a period of 2π. This uncertainty term can be eliminated when we apply a cosine function in Section IV. Similar to the analysis of RSS, we can conclude that the difference value of phase between tags $(\theta_i - \theta_j)$ can represent the 3D geometry and inner biomaterial features of human faces.

B. Feasibility of Anti-Spoofing Face Authentication

We conduct experiments to demonstrate that the 3D geometry and inner biomaterial features of human face have been indeed extracted for anti-spoofing FA purpose. Specifically, we ask two volunteers (Person A and Person B) to put their faces at a fixed distance in front of the tag array twice, and record the phase and RSS values of the tags. Then we hold the 2D photo and 3D printed mask of the two volunteers respectively, and collect the phase and RSS values. In Fig. 3 and Fig. 4, we calculate the phase difference and the RSS difference between the surrounding tags with the center one to analyze the impact of different targets on the tags. We can observe that the result of 2D photo is different from that of 3D mask, (Fig. 3(d) vs. Fig. 3(e) and Fig. 4(d) vs. Fig. 4(e)), which shows that the 3D geometry features of human face have been extracted. Besides, the result of 2D photo also varies severely to the real human face (Fig. 3(a) vs. Fig. 3(d) and Fig. 4(a) vs. Fig. 4(d)), which indicates that the traditional 2D static and dynamic attacks can be defended. Similarly, the result of 3D mask is distinct to the real face (Fig. 3(a) vs. Fig. 3(e) and Fig. 4(a) vs. Fig. 4(e)), indicating that the inner biomaterial features of human face have been extracted, and our system can resist 3D spoofing attacks. Additionally, the results of the same volunteer at different attempts are very similar (Fig. 3(a) vs. Fig. 3(b) and Fig. 4(a) vs. Fig. 4(b)), while they are different for two volunteers (Fig. 3(a) vs. Fig. 3(c) and Fig. 4(a) vs. Fig. 4(c)). Therefore, the features we extract are unique to everyone, so they can be utilized for authentication. Additionally, since these characteristics of a specific human face are difficult to imitate, our system can resist spoofing attacks.

IV. System Design

In this section, we present the design details of RFace. We first remove noise from raw RF signals and then suppress the impacts of distance and deflection variations between the face and the tag array to extract a stable fusion feature including both 3D geometry and inner biomaterial features. Finally, we utilize an SVM to realize anti-spoofing authentication.

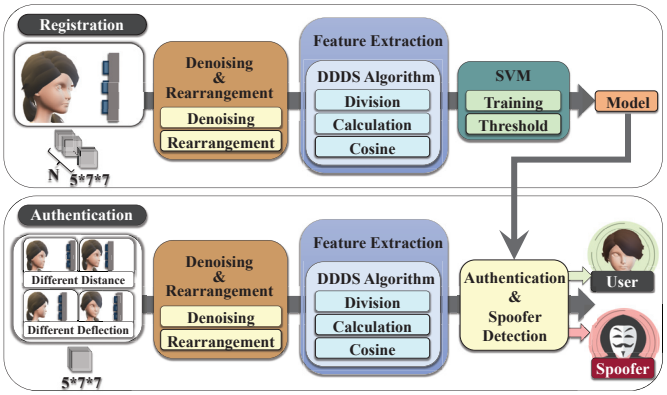


Fig. 5: System architecture of *RFace*.

A. System Overview

The architecture of RFace is illustrated in Fig. 5, which consists of two primary phases: registration phase and authentication phase. Users are required to pose their faces in front of a tag array for registration and authentication. In the registration phase, RFace collects the RSS and phase values of the RF signals reflected from human face, and feeds them into a denoising and rearrangement algorithm to construct a sequence of RSS and phase values. Then, this sequence goes through a distance-deflection disturbance resistant facial features extraction algorithm. Then a reliable fusion feature consisting of 3D geometry and inner biomaterial can be extracted by calculating the RSS and phase differences between the tags on the tag array. Finally, the extracted fusion feature is organized into feature blocks according to the time dimension and fed into an SVM for model training.

In the authentication phase, once a human face is detected, RFace collects a set of RSS and phase values for about 1.25 seconds, and then goes through denoising and face features extraction process. Then RFace leverages the extracted fusion feature to conduct authentication and spoofing attack defense.

B. Denoising and Rearrangement

The collected phase values from an RFID reader involve noise due to the involuntary movement of faces and imperfection of hardware. These inevitable defects may make RFace unreliable. We eliminate the noise by unwrapping successive phase values [20]. Moreover, we set a window with a size of five samples and filter out abnormal phase values in the window with the average of other normal values. Fig. 6 shows an instance of noise filtering, where abnormal phase values are filtered out. Additionally, for subsequent face features extraction, we rearrange both RSS and phase values (which can be represented as $N * 2 * M$, where N is the number of frames based on slot ALOHA [21], where M is the sum of tags) into a new sequence (whose shape is $N*2*R*C$, where R is the number of rows and C is the number of columns in tag array) according to the layout of the tag array.

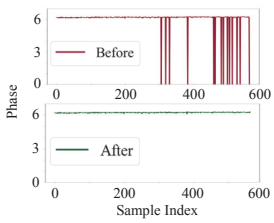


Fig. 6: Performance of denoising method.

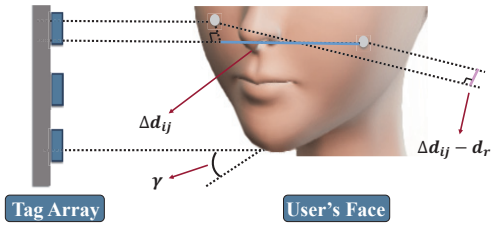


Fig. 7: The impact of deflection.

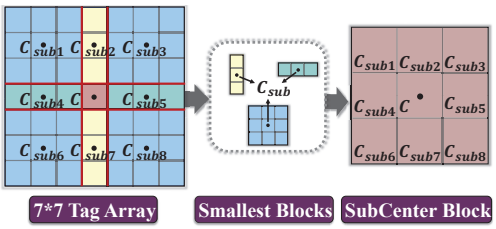


Fig. 8: A 7*7 example to represent the find-center-and-divide operation in *DDDS*.

C. Distance-Deflection Disturbance Resistant Feature

Based on the rearranged RSS and phase sequence, we start to extract the 3D geometry and inner biomaterial features (which can be represented as fusion feature in the following). As presented in Section III-A, the RSS difference and phase difference between tags can reveal the fusion feature of human faces and we can utilize these two kinds of difference values to extract a distance-resistant fusion feature. Nevertheless, in actual FA scenarios, it is hard to ensure that the user's face is always in a fixed position and deflection angle relative to the tag array for each authentication attempt. Moreover, due to the sensitivity of RF signals, the tiny variations in distance and angle to the tag array would cause non-trivial errors in the measurements of RSS and phase values [22]. In order to obtain more reliable features, we design a facial feature extraction algorithm resistant to distance and angle variations.

1) Challenges: Intuitively, we can calculate difference values between any two tags on the tag array to extract desired fusion feature. However, we have many practical challenges. Firstly, although arbitrary subtraction can potentially calculate more facial features, it requires about $2*C_M^2$ times of subtraction for each authentication, which is time-consuming. Additionally, the deflection of user's face could lead performance degradation of RFace. As shown in Fig. 7, when a user faces at a certain angle γ, the RSS and phase differences between the leftmost and rightmost tags not only involve the relative distance Δd_{ij}, but also the unexpected distance difference d_r due to facing direction. Δd_{ij} represents the difference of distances between the center points of their corresponding areas to tag array. This unexpected distance d_r may make RFace mistakenly authenticate a legitimate user as illegitimate. Finally, as shown in Eq. 12, there is an uncertainty term $2k\pi$ which makes the phase difference unstable with the impact of distance variation, thus making RFace unreliable as well.

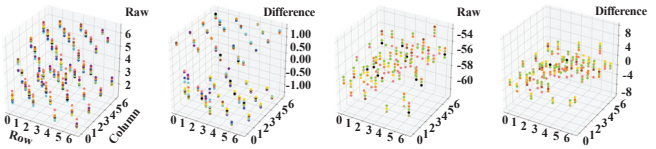
2) Distance-Deflection Disturbance Suppression Algorithm (DDDS): In order to tackle the challenges mentioned above, we propose a universal subtraction method that can suppress the disturbance of distance and deflection as well as achieve fast and accurate fusion feature extraction. As for deflection, it is vital to mitigate the unexpected distance difference d_r which may result in authentication deviation. Based on theoretical analysis, we can find that the closer the two tags are selected for subtraction, the smaller the d_r is. Therefore, the key idea of suppressing the impact of face deflection is to narrow the difference calculation range in the tag array. Besides, as for the $2k\pi$ term, the uncertainty of the value k is actually due to the variation of distance. Here, we can eliminate this uncertainty by calculating the cosine of the phase difference to obtain a stable distance-resistant feature.

Algorithm 1: Distance-Deflection Disturbance Suppression

Input: RSS and θ sequence of tags: $\{\{RSS_{r,c}\},\{\theta_{r,c}\}\}, r \in [1, Row], c \in [1, Column]$;
Output: Difference between RSS and θ sequence: $\{\{\Delta R_{r,c}\},\{cos(\Delta\phi_{r,c})\}\}, r \in [1, Row], c \in [1, Column]$;

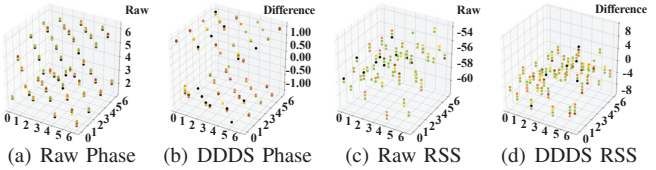
F1$(1, Row, 1, Column)$;
$\Delta R_{\frac{1+Row}{2},\frac{1+Column}{2}} \leftarrow 0$;
$cos(\Delta\phi_{\frac{1+Row}{2},\frac{1+Column}{2}}) \leftarrow cos(0)$;
Function F1 $(row1, row2, col1, col2)$:
  $C.r = \frac{row1+row2}{2}, C.c = \frac{col1+col2}{2}$;
  if $row2 - row1 > 2$ *and* $col2 - col1 > 2$ **then**
    $\Delta r = \frac{row1+row2}{4}, \Delta c = \frac{col1+col2}{4}$;
    for $r \leftarrow \{C.r - \Delta r, C.r, C.r + \Delta r\}$ **do**
      for $c \leftarrow \{C.c - \Delta c, C.c, C.c + \Delta c\}$ **do**
        if $r == C.r$ *and* $c == C.c$ **then**
          Continue;
        $\Delta R_{r,c} \leftarrow RSS_{r,c} - RSS_{C.r,C.c}$;
        $cos(\Delta\phi_{r,c}) \leftarrow cos(\theta_{r,c} - \theta_{C.r,C.c})$;
        if $r == C.r$ **then**
          F1$(r, r, c - (\Delta r - 1), c + (\Delta r - 1))$;
        else if $c == C.c$ **then**
          F1$(r - (\Delta r - 1), r + (\Delta r + 1), c, c)$;
        else
          F1$(r - (\Delta r - 1), r + (\Delta r + 1), c - (\Delta r - 1), c + (\Delta r - 1))$;
      end
    end
  else
    for $r \leftarrow [row1 : row2]$ **do**
      for $c \leftarrow [col1 : col2]$ **do**
        if $r == C.r$ *and* $c == C.c$ **then**
          Continue;
        else
          $\Delta R_{r,c} \leftarrow RSS_{r,c} - RSS_{C.r,C.c}$;
          $cos(\Delta\phi_{r,c}) \leftarrow cos(\theta_{r,c} - \theta_{C.r,C.c})$;
      end
    end
  end

According to the above analysis, we propose the distance-deflection disturbance suppression (DDDS) algorithm (as shown in Algorithm 1) to extract reliable fusion feature. The purpose of DDDS is to decrease the time for difference calculation and avoid the RSS subtraction and phase subtraction for a pair of tags that are far apart on the tag array (*e.g.,* the leftmost and rightmost, top and bottom). To this end, we first find the center point of the tag array (C) (as shown in Fig. 8 with a $7*7$ tag array as an example) and divide the tag array into smaller blocks based on the row and column where C



(a) Raw Phase (b) DDDS Phase (c) Raw RSS (d) DDDS RSS

Fig. 9: Distributions of raw RSS and phase and features extracted by DDDS in different distance conditions.



(a) Raw Phase (b) DDDS Phase (c) Raw RSS (d) DDDS RSS

Fig. 10: Distributions of raw RSS and phase and features extracted by DDDS in different deflection conditions.

locates. Then we repeat this find-center-and-divide operation until we obtain the smallest block whose rows and columns are both no more than 3. Next, for each smallest block, we first find the subcenter of it (C_{sub}), and then for each remaining tag (represented by $T_{r,c}$, with r and c as the row and column it locates) in this block, we get:

$$\Delta R_{r,c} = RSS_{r,c} - RSS_{C\_sub}, \tag{13}$$

$$\Delta \phi_{r,c} = \theta_{r,c} - \theta_{C\_sub}, \tag{14}$$

with $\Delta R_{r,c}$ and $\Delta \phi_{r,c}$ denoting the RSS difference and phase difference between $T_{r,c}$ and the corresponding subcenter point C_{sub} of the block. For the subcenters (C_{sub}) of these smallest blocks, we utilize the same method to get their $\Delta R_{r,c}$ and $\Delta \phi_{r,c}$ by calculating the RSS difference and phase difference between the subcenters (C_{sub}) and the center point of the whole tag array (C). So far, we have obtained ΔR and $\Delta \phi$ of all tags. In the end, as we have analyzed at the beginning, we have to substitute $\Delta \phi$ by $cos(\phi)$ in the phase part of our final fusion feature. Finally, combining the ΔR and $cos(\Delta \phi)$ of all tags in the tag array, we form a 3-dimension feature array with a shape of $(2 * R * C)$ with only $(2 * R * C)$ times of subtraction operations.

Fig. 9 and Fig. 10 show the effect of our DDDS algorithm with the $7 * 7$ tag array, where the X-axis and Y-axis represent the row and column of the tag array respectively. Compared with the distribution of raw RSS and θ of each tag before, the values of ΔR and $cos(\Delta \phi)$ after applying the DDDS algorithm become more stable under varying distance and deflection conditions. Hence, we can obtain a reliable fusion feature based on the DDDS algorithm.

D. Anti-Spoofing Authentication

Based on the extracted face fusion feature, we next demonstrate how to perform face authentication and defend against spoofing attacks. In addition to the aforementioned RSS difference and phase difference, we also include the time series as a new dimension in the feature extraction. We take A ($A = 5$ in implementation) consecutive fusion feature arrays $(2 * R * C)$ in time series as a fusion feature block $(A * 2 * R * C)$, and reshape the fusion feature which we obtain from DDDS algorithm into a five-dimensional array $(N/A * A * 2 * R * C)$.

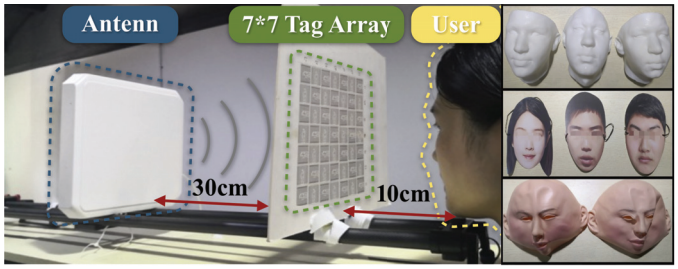


Fig. 11: Experimental setup.

Then the following anti-spoofing authentication and feature visualization are all based on this five-dimensional fusion feature array.

In RFace, we utilize an SVM as the classifier to implement face authentication and spoofing attack detection. Specifically, each user needs to provide a batch of signal samples to train the SVM for RFace registration. All feature blocks are reshaped as one-dimensional feature vectors to train the SVM. In the authentication stage, once receiving a login request, RFace feeds extracted features from the received signal samples into the pre-trained SVM model which outputs a series of confidence coefficients representing the similarity between the login user and the registered users in the database. Then RFace finds the largest one among these confidence coefficients and compare it with a pre-determined threshold. If it is larger than the threshold, the user will be accepted as a legitimate user. Otherwise, the user will be denied. Since the fusion feature of each person is distinct, unregistered users will fail the authentication owing to low similarity. Furthermore, as spoofing attackers cannot produce inner biomaterial features, attackers will be rejected by the threshold-confidence comparison mechanism.

V. Evaluation

We evaluate the performance of RFace in real environment on both authentication and anti-spoofing.

A. Implementation

Hardware: RFace is implemented with an *Impiji R420* reader connected to a directional antenna *Larid A9028*. Besides, we utilize 49 *Alien-9629* RFID tags to form a $7 * 7$ tag array in a perpendicular orientation deployment as shown in Section II. The working frequency of RFace is $920.625MHz$.

Software: The collection of RF signals is implemented by *C#* based on slot-ALOHA protocol and EPC Gen2 standard to avoid collision and control the communication respectively. The processing algorithms of RFace are implemented by *Python* which runs on a personal computer (PC) with Intel(R) Core(TM) *i5-8250U* 1.6 GHz CPU and 8 GB RAM.

Experimental Setup: We conduct our experiments in a typical laboratory environment. Fig. 11 shows the default setup of RFace. The directional antenna is placed $30cm$ behind the tag array to transmit interrogative RF signals, and users place their faces around $10cm$ in front of the tag array for authentication. Then RF signals reflected from human faces are collected and further sent to PC via Ethernet for processing.

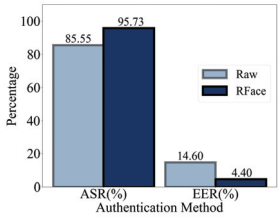


Fig. 12: ASR and EER with raw data and RFace.

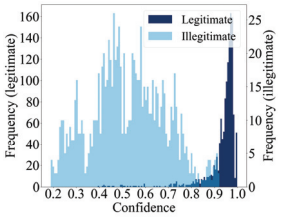


Fig. 13: Confidence distributions for users.

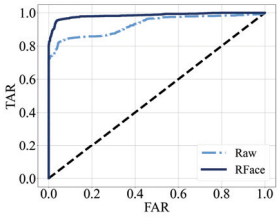


Fig. 14: ROC curves for RFace and raw data.

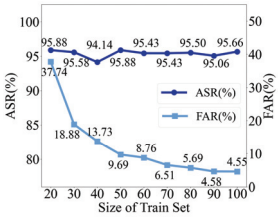


Fig. 15: The effect of the training set size.

Data Collection: We invite 30 volunteers (10 females and 20 males) aged from 18 to 30 in our experiments. Among the 30 volunteers, we randomly choose 5 volunteers as spoofers and the rest 25 volunteers register as legitimate users. In the registration phase, we collect three groups of RF signals (each group contains 60 fusion feature blocks) for each legitimate user, which takes about 225 seconds. Then in the authentication phase, each legitimate volunteer performs authentication for 120 times and each illegitimate volunteer performs 360 times authentication to test the performance of RFace. Each authentication attempt takes about 1.25 seconds.

Metrics: We define six metrics to evaluate RFace: Authentication Success Rate (ASR), False Accept Rate (FAR), False Reject Rate (FRR), Receiver Operating Characteristic (ROC), Equal Error Rate (EER) and Defense Success Rate (DSR). ASR is the probability that the system authenticates a legitimate user correctly and can be represented as: $ASR = \frac{N_{acc}}{N_all}$, where N_{acc} is the number of correct authentication times for legitimate users and N_{all} is the number of all authentication times for legitimate users. FAR is the probability that the system mistakenly authenticates an illegitimate user as a legitimate one and can be represented as: $FAR = \frac{N_{wr}}{N_{il}}$, where N_{wr} is the number of wrong accepted times for illegitimate users and N_{il} is the number of all authentication times for illegitimate users. FRR is the probability that the system mistakenly authenticates a legitimate user as an illegitimate one. ROC curve indicates the relationship between the ASR and FAR under various threshold. Additionally EER describes the rate where FAR equals FRR. Finally, we define the DSR to measure the performance of RFace on anti-spoofing. DSR is the probability that a spoofing attack is successfully detected, and the higher DSR indicates that RFace is more secure. DSR can be formulated by: $DSR = \frac{N_{def}}{N_{att}}$, where N_{def} is the number of successfully detected spoofing attacks and N_{att} is the number of all spoofing attacks.

B. Overall Performance

We first compare the overall performance of RFace with/without our DDDS algorithm. As shown in Fig. 12, the ASRs for RFace and raw data are 95.73% and 85.55%, respectively. Meanwhile, with the threshold of 0.8, the EERs of RFace and raw data are 4.40% and 14.60%, respectively. These comparison results demonstrate that our denoising and feature extraction method can effectively remove noise and improve feature quality. To show if RFace is able to reject illegitimate users, we plot the confidence distributions of legitimate users and illegitimate users in Fig. 13. This result indicates that RFace can effectively reject illegitimate users with a high probability. Therefore, as shown in Fig. 14, RFace can achieve a low FAR of 4.48% while the FAR of raw data is as high as 16.52%. These results demonstrate that RFace can authenticate users accurately and securely. In addition, our experiments show that every authentication only takes 1.26 seconds on average, indicating that RFace performs well in real-time authentication.

C. Effect of Training Set Size

To explore the effect of training set size, *i.e.*, the number of feature blocks of each user in the training set, we vary the size from 20 to 90. The experiment results shown in Fig. 15 indicate that with 90 feature blocks for each user, RFace can achieve a FAR that is lower than 5.0% while retaining a high ASR of about 95.5%. This result also shows that RFace is user-friendly in user registration because collecting 90 feature blocks only takes 112.5 seconds approximately.

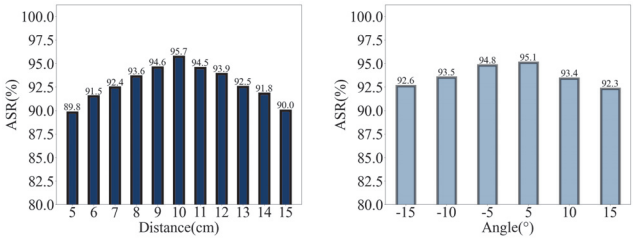
D. Performance Towards Distance and Deflection Variations

In the distance experiment, we use the feature blocks collected in 10 centimeters distance as the training set. Then we vary the distance from 5 centimeters to 15 centimeters to evaluate the impact of distance. The authentication results are shown in Fig. 16(a), in which we find that large distance variation (*i.e.*, far from 10 centimeters) would cause ASR reduction. However, even if the difference is 5 centimeters, the reduction scale is still acceptable (less than 6%), which proves that DDDS algorithm is effective at distance disturbance suppression and RFace is robust to distance variation.

In the deflection experiment, we use the normal feature blocks without deflection as the training data. Then we collected testing data of two orientations (*i.e.*, leaning left or right of cheeks) of deflections. Specifically, we vary the deflection angles from 5 degrees to 15 degrees. As in Fig. 16(b), it can be observed that even if the left or right deflection is 15 degrees, RFace can still achieve a high ASR. Therefore, DDDS is also effective in deflection impact suppression.

E. Attack and Defense

Attack Realizations: We evaluate our system against three types of spoofing attacks: 2D spoofing attack, 2D+ spoofing attack and 3D spoofing attack. For the 2D spoofing attack, there are two attack methods including static and dynamic attacks, which are respectively realized with photos and videos of three victims (each authenticates 60 times) in front of



(a) Distance (b) Angle

Fig. 16: The impact of distance and deflection on ASR.

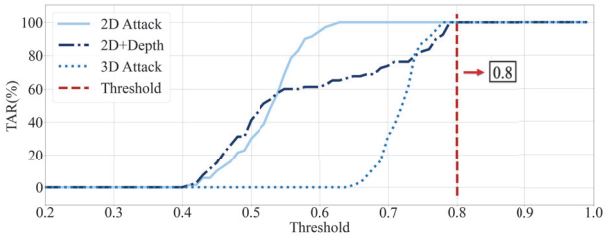


Fig. 17: The change of DSR of three attacks with threshold.

the tag array. For the 2D+ spoofing attack, we recruited five unregistered volunteers as attackers, each wearing a soft PVC mask printed with victim's photo respectively. We make three soft PVC masks with three victims' photos and each attacker wears each mask to attack RFace 60 times. For the most challenging 3D spoofing attack, we launch attacks by utilizing photosensitive resin to build three $1:1$ scale 3D masks of victims which simulate both 2D features and precise depth features of the victim. Specifically, we also pose each 3D printed mask in front of the tag array to perform 3D spoofing attack 60 times. The setup of these three types of attack is presented in Fig. 11.

Defense Performance: We calculate the DSRs of three types of attacks. The results are shown in Fig. 17, which indicate that the DSRs for all three types of attacks are 100%. This is because the confidence coefficients of the features provided by attackers cannot reach our empirical threshold of 0.8. The results indicate that the extracted inner biomaterial feature is effective in defending against the spoofing attacks. Table I compares RFace with four advanced FA systems. The results show that, compared with other FA systems, RFace can protect users' privacy and defeat various spoofing attacks.

VI. Related Work

Facial Feature-based Authentication: Over the past decades, FA has been extensively studied in literature. For instance, Alfalou *et al.* [26] leverage a nonlinear function to increase the correlation peak to make the face recognition application more robust. However, traditional FA systems, which only capture user's two-dimensional facial features, are vulnerable to spoofing attacks. To solve this problem, many solutions were proposed to verify if a user is alive, i.e., liveness detection [1, 3, 27]. For example, EchoPrint [27] employs inaudible voice emitted by a smartphone to sense the 3D contour of human face to check the liveness. Nevertheless, existing anti-spoofing techniques only sense the 3D structure of human face, which makes them vulnerable to 3D-printed faces [28]. In this paper, we try to defeat this spoofing attack problem by extracting both the 3D geometry and inner biomaterial features from RFID backscatter signals using COTS RFID systems.

RFID Sensing Techniques: Recently, RFID has been developed in many application fields, such as user authentication [20, 29], activity recognition [30, 31], localization [32, 33], and so on [34]. RF-Mehndi [20] is an RFID-based user authentication system. It leverages the coupling effect of a tag array to amplify user's impedance feature to achieve biometric acquisition. DU *et al.* [30] design a novel in-library activity recognition system to facilitate readers and book managers. 3DLRA [32] develops a 3D indoor localization system with RFID tags. It uses deep learning to analyze the variation characteristic of signal indicators to localize tags in 3D space.

TABLE I: Comparison with previous work

System	2D Attack Resistance	2D+ Attack Resistance	3D Attack Resistance	Privacy Preserved
Samsung FR [23]	×	×	×	×
EchoFace [24]	✓	✓	×	×
FaceHeart [25]	✓	✓	×	×
Face Flashing[3]	✓	✓	×	×
RFace	✓	✓	✓	✓

VII. Conclusions

In this paper, we build a novel facial authentication system named RFace with COTS RFID devices. RFace ensures privacy-preserving and spoofing-resistant simultaneously. We build a rigorous theoretical model to prove the feasibility of extracting both 3D geometry and biomaterial features from backscatter RFID signals. In order to alleviate the impact caused by position difference in real scenarios, we design a novel distance and deflection disturbance suppression algorithm. We conduct comprehensive evaluations with 30 participants in various experiment settings. The results show that RFace achieves an ASR of 95.73% and an EER of 4.4%. More importantly, RFace can effectively defeat spoofing attacks by jointly considering 3D geometry and biomaterial features.

Acknowledgment

This work is supported in part by National Natural Science Foundation of China under grant 62032021, 61872285, 61702437, 61972348 and the major project of the National Social Science Foundation under Grant 20ZDA062, Alibaba-Zhejiang University Joint Institute of Frontier Technologies, Research Institute of Cyberspace Governance in Zhejiang University, Leading Innovative and Entrepreneur Team Introduction Program of Zhejiang (Grant No. 2018R01005), Zhejiang Key R&D Plan (Grant No. 2019C03133), Hong Kong GRF under grant PolyU 152165/19E.

REFERENCES

[1] H. Chen, W. Wang, J. Zhang, and Q. Zhang, "Echoface: Acoustic sensor-based media attack detection for face authentication," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2152–2159, 2020.

[2] B. Zhou, J. Lohokare, R. Gao, and F. Ye, "Echoprint: Two-factor authentication using acoustics and vision on smartphones," in *ACM International Conference on Mobile Computing and Networking, MobiCom*, 2018.

[3] D. Tang, Z. Zhou, Y. Zhang, and K. Zhang, "Face flashing: a secure liveness detection protocol based on light reflections," in *Annual Network and Distributed System Security Symposium, NDSS*, 2018.

[4] S. Rajarajan and P. Priyadarsini, "UTP: a novel PIN number based user authentication scheme," *International Arab Journal of Information Technology*, vol. 16, no. 5, pp. 904–913, 2019.

[5] A. S. Rathore, W. Zhu, A. Daiyan, C. Xu, K. Wang, F. Lin, K. Ren, and W. Xu, "Sonicprint: a generally adoptable and secure fingerprint biometrics in smart devices," in *ACM International Conference on Mobile Systems, Applications, and Services, MobiSys*, 2020.

[6] S. Mare, M. Baker, and J. Gummeson, "A study of authentication in daily life," in *USENIX Symposium on Usable Privacy and Security, SOUPS*, 2016.

[7] R. AMADEO, "Galaxy s8 face recognition already defeated with a simple picture," https://arstechnica.com/gadgets/2017/03/video-shows-galaxy-s8-face-recognition-can-be-defeated-with-a-picture/, 2017.

[8] K. Kollreider, H. Fronthaler, and J. Bigun, "Non-intrusive liveness detection by face images," *Journal of Image and Vision Computing*, vol. 27, no. 3, pp. 233–244, 2009.

[9] A. Wyatt, "What exactly is the dot projector? why it is used in iphone x?" https://www.thebestintech.com/what-is-dot-projector/.

[10] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3d masks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1084–1097, 2014.

[11] F. Wang, J. Han, F. Lin, and K. Ren, "Wipin: Operation-free passive person identification using wi-fi signals," in *IEEE Global Communications Conference (GLOBECOM)*, 2019.

[12] D. Vasisht, G. Zhang, O. Abari, H. Lu, J. Flanz, and D. Katabi, "In-body backscatter communication and localization," in *International Conference of the ACM Special Interest Group on Data Communication, SIGCOMM*, 2018.

[13] L. Yang, Q. Lin, X. Li, T. Liu, and Y. Liu, "See through walls with cots rfid system!" in *ACM International Conference on Mobile Computing and Networking, MobiCom*, 2015.

[14] C. Wang, J. Liu, Y. Chen, H. Liu, L. Xie, W. Wang, B. He, and S. Lu, "Multi-touch in the air: Device-free finger tracking and gesture recognition via COTS RFID," in *IEEE International Conference on Computer Communications, INFOCOM*, 2018.

[15] L. Yang, Y. Chen, X.-Y. Li, C. Xiao, M. Li, and Y. Liu, "Tagoram: Real-time tracking of mobile rfid tags to high precision using cots devices," in *ACM International Conference on Mobile Computing and Networking, MobiCom*, 2014.

[16] Impinj, "R420 readers," https://www.impinj.com/library, 2010.

[18] A. Greenberg, "Hackers say they've broken face id a week after

[17] T. Foltýn, "Face unlock on many android smartphones falls for a photo," https://www.welivesecurity.com/2019/01/10/face-unlock-many-android-smartphones-falls-photo/, 2019.

iphone x release," https://www.wired.com/story/hackers-say-broke-face-id-security/, 2017.

[19] L. Tsang, J. A. Kong, and R. T. Shin, "Theory of microwave remote sensing," 1985.

[20] C. Zhao, Z. Li, T. Liu, H. Ding, J. Han, W. Xi, and R. Gui, "Rf-mehndi: A fingertip profiled RF identifier," in *IEEE International Conference on Computer Communications, INFOCOM*, 2019.

[21] X. Lei and L. Sanglu, *Principle, Protocol and System Design of RFID*. Science Press, 2016.

[22] L. Yang, Y. Li, Q. Lin, H. Jia, X.-Y. Li, and Y. Liu, "Tagbeat: Sensing mechanical vibration period with cots rfid systems," *IEEE/ACM Transactions on Networking, TON*, vol. 25, no. 6, pp. 3823–3835, 2017.

[23] SAMSUNG, "How does face recognition work on galaxy s20, s20+, s20 ultra, and z flip?" https://www.samsung.com/global/galaxy/what-is/face-recognition/.

[24] H. Chen, W. Wang, J. Zhang, and Q. Zhang, "Echoface: Acoustic sensor-based media attack detection for face authentication," *Internet of Things Journal*, vol. 7, no. 3, pp. 2152–2159, 2019.

[25] Y. Chen, J. Sun, X. Jin, T. Li, R. Zhang, and Y. Zhang, "Your face your heart: Secure mobile face authentication with photoplethysmograms," in *IEEE INTERNATIONAL Conference on Computer Communications, INFOCOM*, 2017.

[26] A. Alfalou, C. Brosseau, and W. Kaddah, "Optimization of decision making for face recognition based on nonlinear correlation plane," *Optics Communications*, vol. 343, 2015.

[27] B. Zhou, J. Lohokare, R. Gao, and F. Ye, "Echoprint: Two-factor authentication using acoustics and vision on smartphones," in *ACM International Conference on Mobile Computing and Networking, MobiCom*, 2018.

[28] Y. Gao, W. Wang, V. V. Phoha, W. Sun, and Z. Jin, "Earecho: Using ear canal echo for wearable authentication," *Journal of Interactive, Mobile, Wearable and Ubiquitous Technologies, IMWUT*, vol. 3, no. 3, pp. 81:1–81:24, 2019.

[29] J. Liu, X. Zou, J. Han, F. Lin, and K. Ren, "BioDraw: Reliable multi-factor user authentication with one single finger swipe," in *IEEE/ACM International Symposium on Quality of Service, IWQoS*, 2020.

[30] Y. Du, Y. Lim, and Y. Tan, "Activity recognition using RFID phase profiling in smart library," *ACM Transactions on Information Systems, TOIS*, vol. 102-D, no. 4, pp. 768–776, 2019.

[31] R. Liang, S. Yang, and B. Chen, "Indexmo: exploring finger-worn RFID motion tracking for activity recognition on tagged objects," in *ACM International Symposium on Wearable Computers*, K. Farrahi, R. Harle, and N. D. Lane, Eds., 2019.

[32] S. Cheng, S. Wang, W. Guan, H. Xu, and P. Li, "3dlra: An RFID 3d indoor localization method based on deep learning," *Journal of Sensors*, vol. 20, no. 9, p. 2731, 2020.

[33] Y. Ma, B. Wang, X. Gao, and W. Ning, "The gray analysis and machine learning for device-free multitarget localization in passive UHF RFID environments," *Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 802–813, 2020.

[34] C. Duan, L. Yang, Q. Lin, Y. Liu, and L. Xie, "Robust spinning sensing with dual-rfid-tags in noisy settings," *IEEE Transactions on Mobile Computing, TMC*, vol. 18, no. 11, pp. 2647–2659, 2019.