IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 25, 2020, accepted April 7, 2020, date of publication April 14, 2020, date of current version May 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2987966

Fake Identity Attributes Detection Based on Analysis of Natural and Human Behaviors

YAHAO ZHANG[1,3], RUIMIN HU[1,3], (Senior Member, IEEE), DENGSHI LI[2], (Member, IEEE), AND XIAOCHEN WANG[1,3], (Member, IEEE)

[1] National Engineering Research Center for Multimedia Software, School of Computer Science, Wuhan University, Wuhan 430072, China
[2] School of Mathematics and Computer Science, Jianghan University, Wuhan 430056, China
[3] Hubei Key Laboratory of Multimedia and Network Communication Engineering, Wuhan University, Wuhan 430072, China

Corresponding author: Ruimin Hu (hrm@whu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant U1803262, Grant U1736206, and Grant 61701194, and in part by the Basic Research Project of Science and Technology Plan of Shenzhen under Grant JCYJ20170818143246278.

ABSTRACT Under confrontational environment, individual can impersonate others by wearing masks or other skills to conceal real identity, which brings enormous challenges to physical identity recognition. Moreover, massive fake attributes seriously threaten identity management. Aiming at the existence of fake attributes during multimodal identification, we propose a novel method to detect fake attributes and compute real identity for security of systems. Most previous methods focused on the differences about features between fake and normal attributes, but each method generally targeted one type of fake attribute, and the results decreased a lot with unknown attacks. In this paper, we first explore the essential differences of data distribution caused by natural and human behaviors, then with order-of-consensus-calculation based on the differences, fake attributes are detected by analyzing the rank of consensus identity in recognition results, finally maximum-consensus-calculation is applied to compute real identity for evaluating detection performance. Experimental results on face, fingerprint, and voiceprint demonstrate that the proposed method can detect fake attributes effectively, which has a higher accuracy, and the accuracy of identity recognition is increased obviously by about 13.20% with forgery detection. The additional experiments further confirm the feasibility of the proposed method with increase of fake attributes. Furthermore, the proposed method can deal with different kinds of attacks, even with unknown attacks, and it is also significant to improve the security of identification with complex environment.

INDEX TERMS Fake attributes, natural and human behaviors, forgery detection, identification.

I. INTRODUCTION

The widespread use of biometric identification systems is severely limited by security threats arising from fake attributes [1], such as face masks [2], altered fingerprints [3]. Generally, individual can easily conceal real identity with fake attributes to evade identification systems, even if for multimodal systems. However, the use of fake attributes does not require advanced technical skills. Fig. 1 shows examples of fake attributes during recognition. Besides, some related events also happened, in December 2009, a woman successfully evaded the Japanese Immigration Automated Fingerprint Identification System (AFIS) by surgically swapping the fingerprint of her left and right hands, when arrested the scars on her hands made the police suspicious [4]. According to the report, financial losses due to fake identity reached to around 1.3 billion pounds each year in UK [5]. Such behavior is intentionally committed, which poses huge difficulty in computing real identity. Moreover, with the development of

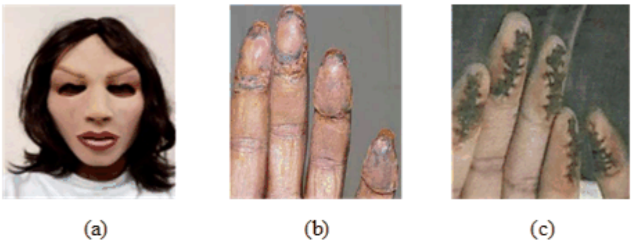

FIGURE 1. Examples of fake attributes during recognition. (a) Fake face with 3D mask. (b) Altered fingerprint, transplanted friction ridge skin from sole. (c) Switched finger by surgery.

The associate editor coordinating the review of this manuscript and approving it for publication was Chin-Feng Lai.

technology, the challenges for recognition are more severe, so some measures should be considered for solving fake attributes to improve security of systems.

Aiming at the causes of wrong recognition results in identification systems, we attribute them to two types, natural and human behaviors. For natural behavior, it mainly refers to recognition defects and other inevitable reasons, we can only improve technology to reduce the impact on recognition results. For example, when environment changes or acquired attributes with low quality, the recognition results may be wrong due to recognition defects, this kind of error is produced without human interference, and we call it as natural behavior. For human behavior, it mainly refers to malicious attacks, such as using masks to deceive face recognition system, this kind of error is produced with human interference, and we call it as human behavior. In real scenarios, criminals may forge their identity attributes with some skills, in addition, due to recognition defects, both will cause wrong results. In order to obtain real identity better, it is necessary to explore the differences between natural and human behaviors to detect fake attributes.

According to the analysis of the challenges and trends during identity recognition [6], [7], the trusted algorithms may focus on the following three key elements: the first is accurate, it means the method should acquire more accurate results when the first choice is not real identity; the second is robust, which means the algorithm should be less affected by external conditions such as environment changes, and it can provide more strong performance; the third is anti-attack, which shows the algorithm should be able to resist malicious attacks. Overall, the first two elements correspond to natural behaviors, and the last one corresponds to human behaviors.

In this work, aiming at the existence of fake attributes, we focus on the following topic: during recognition, when we acquire multiple attributes of an unknown person, in which may contain fake attributes, and the goal is to compute real identity. In actual applications, forging large-scale attributes is relatively hard, so we first study the problem with less than 49% of fake attributes. Due to natural behaviors, the recognition results may be wrong with normal attributes, and the experimental results show that majority voting [8] could not obtain better performance, so we need to study new methods to solve fake attributes and obtain real identity.

To date, despite a number of existing approaches are designed to detect fake attributes, most of them exploit the differences about features between fake and normal attributes [2], [9], and one method usually adapts only one kind of attack, besides, the detection performance decreases obviously with unknown attacks. In this paper, given that fake attributes seriously affect the accuracy of identification, we attempt to explore the differences between natural and human behaviors, and detect fake attributes with data analysis in multi-modal to make up for the shortcomings of previous methods, rather than improving the recognition accuracy of single attribute.

The major contributions of this paper can be summarized as follows:

1) We analyze the causes of wrong identification results and attribute them to the essential differences between natural behavior and human behavior, then propose to use proximity relationship to describe the differences of two behaviors;
2) The proposed method can detect different types of fake attributes, even with unknown attacks. Since we analyze the differences between two behaviors with data analysis instead of exploiting the differences about features between fake and normal attributes to detect fake attributes, so the proposed method can deal with different types of attacks.

The rest of the paper is organized as follows. Section II provides some approaches about detecting fake attributes. In section III, we introduce our method in detail. Section IV shows the experiments and some necessary analysis. Finally, section V concludes the paper.

II. RELATED WORK

Identity attributes define who you are or any quality that you display that can be used to distinguish you from the other person. For biometric systems, an attacker can change his only one or a subset biometric traits to successfully evade identification systems [1], which threatens the security of identity recognition. Most researchers have already studied forgery detection in biometrics, with analysis of previous work, most of them addresses presentation attack detection, a brief review is given in this section.

A. TRADITIONAL FEATURE BASED METHODS

For visible spectrum images, several approaches such as detecting motion patterns [10], color texture, and histogram based methods in different color space and variants of LBP in color images [11], have shown good performance. Tan *et al.* [12] considered the task as a binary classification problem and proposed two strategies to extract the essential information about different surface properties of fake and real face, the results showed that the method could obtain preferable performance. For AFIS, individual could alter fingerprints easily by plastic surgery to access automatic border control. Feng *et al.* [13] presented that traditional image quality assessment software (e.g., NFIQ) cannot always detect altered fingerprints, they extracted features from ridge orientation field and used SVM to detect altered fingerprints. Yoon *et al.* [9] improved the method with a combination of orientation field and minutiae distribution, the results showed the feasibility of proposed approach in detecting fake fingerprints. Galbally *et al.* [14] presented a software-based fake detection method, they extracted 25 general image quality features to discern legitimate and imposter samples, and tested on fingerprint, iris, and 2D face databases, and acquired better performance. Raghavendra and Busch [15] proposed a detection scheme based on multi-scale binarized statistical image features and linear support vector machines to detect fake iris. Biggio *et al.* [1] proposed a statistical meta-model of face and fingerprint presentation attacks that characterized a wider family of fake score distributions, the results achieved reliable performance even under never-before-seen attacks. Sanchez-Reillo *et al.* [16] proposed the fusion of the number of strokes and signing time to detect fake signatures, the error rate lowered from about 20% to below 3% under operational conditions.

B. DEEP LEARNING BASED METHODS

With development of the technology, the methods based on traditional features to distinguish fake and real attributes performed not well, some researchers have reported good results using convolutional network (CNN). Yang *et al.* [17] used deep CNN to learn features of high discriminative ability in a supervised manner, and obtained good results on CASIA and Replay-Attack datasets. Menotti *et al.* [18] proposed a method based on two deep learning approaches, the first consisted of learning suitable convolutional network architectures for each domain, and the second focused on learning the weights of the network via back propagation, the results on iris, face and fingerprint showed the method could detect fake attributes well. Gan *et al.* [19] proposed a 3D CNN based approach, which utilized the spatial and temporal features of the video, and obtained good results. Atoum *et al.* [20] proposed a two-stream CNN method for 2D presentation attack detection by combining a patch-based model and holistic depth maps, and achieved better performance on CASIA-FASD, MSU-USSA, and Replay-Attack datasets. Manjani *et al.* [21] showed that individual could portray another identity easily with the help of masks, they proposed a novel multilevel deep dictionary learning-based algorithm to detect attacks. Shao *et al.* [22] presented a novel method based on deep convolutional dynamic texture learning to learn robust dynamic texture information from fine-grained deep convolutional features, the approach achieved an AUC (Area Under Curve) score of 99.99% in the 3DMAD dataset.

C. MULTI SPECTRUMS BASED METHODS

In general, most of methods based on visible spectrum try to detect the subtle differences in image quality when recaptured. However, the methods could fail as the counterfeiting improves, so some workers have suggested using multispectral to deal with this issue. Raghavendra *et al.* [23] proposed a method to detect attack using multiple spectral bands, they used different bands for complementary information and observed a wavelet-based feature level fusion and a score fusion methodology, and achieved better performance with score fusion. Agarwal *et al.* [2] exploited some experiments to present the effectiveness of face masks in obfuscating one's own identity, and the performance of face recognition dramatically decreased with an equal error rate (EER) of 44.9%. They observed that RDWT and Haralick features in the thermal spectrum demonstrated the highest performance for detecting face masks. Liu and Kumar [24] investigated a multispectral approach to detect face masks, they used two sensors to acquire real and masks faces under visible and near infrared, and the results showed that near infrared based imaging 3D face masks offered superior performance compared to visible illumination. Raghavendra *et al.* [25] presented a new approach based on using spectral signatures obtained from a spectral camera operating in eight narrow spectral bands across the visible and near infrared spectrum to detect fake faces. George *et al.* [26] proposed a multi-channel CNN-based approach for attack detection, they captured data images under color, depth, near-infrared and thermal four different channels, and obtained better results with an ACER of 0.3% compared to feature-based approaches. Tolosana *et al.* [27] presented a method by acquiring four short wave infrared spectrums, they combined both handcrafted and deep learning features to detect fake fingerprints, and results showed that the detection error rate as low as 1.35%.

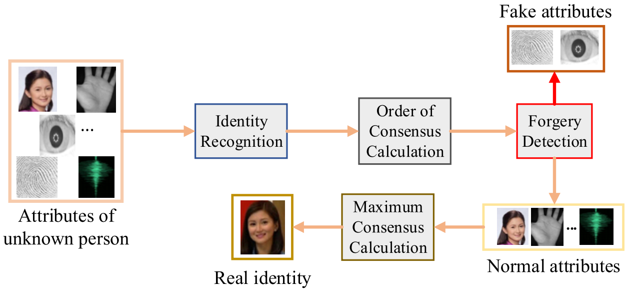
Fake attributes
Attributes of unknown person
Identity Recognition
Order of Consensus Calculation
Forgery Detection
Normal attributes
Maximum Consensus Calculation
Real identity

FIGURE 2. Flow chart of the proposed method.

Nonetheless, several problems are existed in previous work: (1) as the quality of attack instruments improves, it becomes difficult to discriminate real and fake attributes only under single spectral conditions. The trend of existing methods is to add more channels for acquiring more information, so the capture devices will become more and more complicated; (2) one detection approach is usually suitable for one type of attack, when another attack comes, the detection accuracy of the original method decreases a lot; (3) when a new type of attack (unknown attack) occurs, the performance of existing methods decreases obviously. In this paper, based on above problems, we extend our research to multimodality, and analyze the essential differences between natural and human behaviors to discern fake and real attributes, and then obtain real identity. The proposed method can deal with unknown attacks and improve security of recognition systems.

III. PROPOSED METHOD

In this part, a novel method is presented in detail for fake attributes detection and identity computing, Fig. 2 shows the procedure of our method. We first introduce some symbol definitions and then analyze the differences of wrong results caused by natural and human behaviors, finally use the differences to detect fake attributes and compute real identity.

In multimodal identification system, we have collected N identity attributes of S known identities, and utilize $a, b, \ldots, n$ and $O_1, O_2, \ldots, O_S$ to represent different attributes and identities respectively. Under confrontational environment, supposing we have collected N attributes of an unknown person for identity recognition, in which may contain fake attributes. We first solve the problem: the number of fake attributes M satisfies the condition $M < 49\%N$. When the recognition algorithms are accurate enough, we find that it is simple to detect fake attributes and obtain real identity with majority voting method [8]. However, the performance is not well with experiments, so it is necessary to propose new methods for detecting fake attributes to improve the accuracy of identification. Moreover, we also make experiments with increase of the number of fake attributes to show whether the proposed method could work or not.

A. NATURAL AND HUMAN BEHAVIORS

To begin the procedure, we introduce the natural and human behaviors first. During recognition, the cause of wrong recognition results can be divided into two types, caused by natural and human behavior. For natural behavior, it mainly means the external factors that cannot be changed by human, such as illumination and posture changes; while for human behavior, it mainly refers to malicious attack, such as attackers use masks or other skills to deceive identification systems. In order to analyze the essential causes of wrong recognition results, we use proximity relationship to describe the differences of two behaviors, which can be expressed as the wrong results caused by natural behavior have proximity relationship, whereas caused by human behavior do not have proximity relationship. More generally, when the wrong result is caused by natural behavior, the first identity in the result is similar to the real identity; while the wrong result is caused by human behavior, the first identity in the result is dissimilar to the real identity. In the experimental part, we will design experiments to show the proximity relationship, with some necessary calculations and analysis, the results can clearly illustrate the differences between two behaviors.

B. IDENTITY RECOGNITION

The purpose of this step is to obtain identity for each attribute, we reuse the algorithms in literature for implementation directly. Due to proximity relationship, we choose top K of identities in result, and it is obtained by comparison with distances between unknown attribute and known identities, recorded as $R_i = \{O_1, O_3, O_7, \ldots, O_K\}$, where $K<S$, $i = a, b, \ldots, n$, and O_j represents one identity, $j = 1, 2, \ldots, S$. The identity in R_i is in order, such as the result is $R_b = \{O_3, O_1, \ldots, O_4\}$, the first identity is O_3 and secondary choice is O_1 of attribute b. The result of each attribute is expressed like R_i. In experiment, face, fingerprint, and voiceprint are used to illustrate the method. We use a, b, c and R_a, R_b, R_c, to indicate three attributes and corresponding recognition results. Next brief descriptions are given as follows:

For face, the open dlib deep learning library is used. Given an image, 68 facial landmarks are detected using DLIB implementation of Kazemi and Sullivan's [28] ensemble of regression trees method, then the image is normalized and passed to a network with a total of 27 convolution layers, and it is a version of ResNet-34 [29] with a few layers removed. The 128-dimensional output is used as feature vector, during training is fed into a fully connected layer with a structured metric loss. The result is obtained by calculating the distance between the feature vectors. SURF [30] descriptor is applied for fingerprint, first SURF is utilized to extract features with training data, then the same feature is extracted and calculated matching scores with known features with FLANN, and the result is acquired by the rank of scores [31]. Similar to fingerprint, MFCC and LPC are combined linearly for voiceprint recognition, DTW [32] is used to compute distances between two samples, and the result is obtained by the rank of distances.

C. ORDER-OF-CONSENSUS-CALCULATION

In order to make better use of the differences between natural and human behaviors, we will further explain the proximity relationship. Due to the different proximity relationship, the appearance of identity in results R_i will show different features. For normal attributes, due to the accuracy of recognition method cannot reach 100%, the first identity in R_i may not be the real identity, but the real identity will appear in R_i generally. Such as for normal attribute a of identity O_1, the result is $R_a = \{O_3, O_1, O_7, \ldots, O_4\}$ with recognition, it can be seen that the first identity is O_3 rather than real identity O_1.

In this case, the wrong result is mainly caused by natural behavior due to O_3 and O_1 are similar in attribute a level, but the real identity O_1 also appears in the second position in R_a. While for human behavior, supposing that an attacker O_1 attempts to impersonate others (such as identity O_4) by malicious attack with face masks, usually O_4 and O_1 are very dissimilar in face attribute level, otherwise O_1 cannot conceal his real identity, so the real identity will not appear in R_i. As correct rate at top choices drops, secondary choices often contain important information [33], so in our method, we use the sequence R_i to represent the result instead of only using the first identity in R_i. Based on this, for better mine the information in R_i, order-of-consensus-calculation is proposed to obtain consensus identity. The description is as follows:

For algorithm 1, the consensus value utilizes the number of identity in R_i to represent, and the consensus means that the algorithm should meet some conditions when it ends. In the above steps, O_j refers one identity, and d is used to record consensus identity and consensus value. The *identity* is used to record the calculation results, which contains consensus identity and consensus value. The purpose of step 7 is to avoid the appearance of multiple consensus identities. When the algorithm goes to end at step 2, it means that the consensus identity is not found, we ignore this situation in experiments

Algorithm 1 Order-of-Consensus-Calculation

```
Input: $R_i, N, S, K, i = a, b, \ldots, n$
Output: $identity$, $order$
1: Initialize consensus identity and value with $d[O_j] = 0$,
$j = 1, 2, \ldots, S$, set $flag$ = false, $order = 1$, $identity = \{\}$
2: while $flag$ = false and $order \leq K$ do
3: Update $d$ by traversing $R_i$ in order for each attribute
if identity of current $order$ in $R_i$ is $O_j$
    then $d[O_j] \leftarrow d[O_j]+1$
4: Traverse $d$
if exists identity $O_j$, satisfies $d[O_j] > N/2$
    then record $O_j$ and $d[O_j]$ in $identity = \{O_j\text{: } d[O_j]\}$,
    set $flag$ = true, $O_j$ is considered as consensus identity,
    goto step 7
5: Update $order$, $order \leftarrow order + 1$
6: end while
7: Revise $identity$, keep one identity $O_j$ in identity. Consensus identity $O_j$ meets:

$$\min\left(\sum_{i=a}^{n} r(O_j, R_i)\right) \quad (1)$$

Where $r(O_j, R_i)$ refers the rank of identity $O_j$ in $R_i$, when
$O_j$ does not appear in $R_i$, set $r(O_j, R_i) = S/2$
8: Return $identity$ and $order$
```

due to it basically does not happen; when happens, fake attributes are detected with a random number.

With results R_i, the purpose of this step is to calculate consensus identity. For each identity, we set consensus value with zero first, then traverse R_i to update the consensus value in order. If one identity exists in R_i, we increase its consensus value by one. When the consensus value of one identity is greater than $N/2$, the algorithm goes to end. By some necessary analysis, the consensus identity is obtained. Supposing that the R_i is:

$$\begin{aligned}R_a &= \{O_1, O_3, O_{71}, O_{15}, O_{43}, O_{21}, O_8, O_{37}, O_{66}, O_{54}\},\\ R_b &= \{O_{18}, O_4, O_{23}, O_{52}, O_{39}, O_5, O_{40}, O_7, O_{27}, O_{68}\},\\ R_c &= \{O_2, O_{33}, O_3, O_{45}, O_{31}, O_{10}, O_{90}, O_{87}, O_9, O_{72}\}.\end{aligned}$$

With order-of-consensus-calculation, when calculating to the third order, we find that the consensus value of identity O_3 is equal to 2, which meets the end condition, so the result is $identity = \{O_3\text{: } 2\}$, $order = 3$, it shows after third order calculation, the consensus identity is O_3 and its consensus value is 2.

D. FORGERY DETECTION

Fake attributes are detected with differences of the rank of real identity in R_i. By analyzing the wrong results caused by natural and human behaviors, with different proximity relationship, the appearance features of identity in result R_i are different, and we find that the rank of real identity in R_i is obviously different between fake and normal attributes.

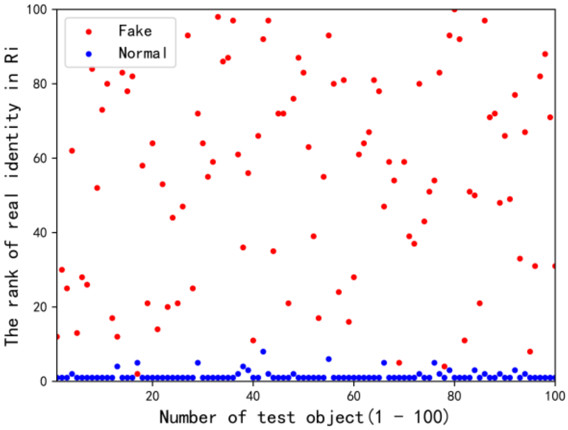

FIGURE 3. The rank of real identity in result R_i between fake and normal attributes. For normal attributes, the rank is small; but for fake attributes, the rank is relatively large.

In order to show the differences intuitively, experiments are designed with face attributes, after face recognition with method in previous section, we calculate the rank of real identity in R_i, Fig. 3 presents the results. It can be seen that for normal attributes, even if with wrong results, due to the wrong results caused by natural behavior have proximity relationship, so the rank of real identity is more advanced, as shown by the blue dots, the values are small; but for fake attributes, the purpose of the attacker is to conceal their real identity, so the real identity generally will not appear in result R_i, and then the rank of real identity is relatively large, as shown by the red dots, they are scattered randomly in the figure, and the values are big compared to the blue dots. Inspired by the differences about the rank of real identity in R_i caused by fake and normal attributes, fake attributes can be detected with suitable parameter. Based on the rank, we consider that if the consensus identity does not appear in the top p of R_i, the attribute corresponding to R_i is considered as fake attribute, otherwise as normal attribute. And parameter p is defined as follows:

$$p = min(order + \delta, K) \quad (2)$$

where p is dynamic as the parameter $order$ changes, and $min(\cdot)$ refers to the function of minimum. The meanings of parameter δ is to control the search range in R_i, and it can be estimated with some analysis. Considering the following two situations, for normal attributes, when the first choice in R_i is not real identity, the rank of real identity in R_i is recorded as a random variable V_n; for fake attributes, when the real identity appears in R_i, the rank of real identity in R_i is recorded as a random variable V_f.

$$V_n < order + \delta \quad (3)$$

$$V_f > order + \delta \quad (4)$$

The number of attributes satisfying conditions (3) and (4) are mutually inhibited, so as to discern fake and normal attributes, the value of δ should satisfy the following conditions: the ratio of attributes that meets inequalities (3) and (4) should

TABLE 1. An introduction of the dataset. It includes two types, type one is from public dataset and paired as real identity randomly; type two is from volunteers. Each attribute contains five samples.

type	face	fingerprint	voiceprint	objects
1	Vggface	CASIA	speech commands	300
	Each attribute contains 5 samples, and three attributes are paired as one identity			
2	HIKVISION	URU4000B	Lenovo b690	200
	Volunteers, each attribute contain 5 samples			

be maximized simultaneously. Like this, the detection effect will be the best. Generally, based on statistical analysis, the parameter δ can be calculated approximately with mathematical expectation of V_n and V_f, it can choose a value from the interval $(E(V_n), E(V_f))$, where $E(\cdot)$ stands for mathematical expectation of a random variable. In experiments, we use training data to acquire optimal value of the parameter δ. According to the previous example of R_i, we find that the consensus identity O_3 does not appear in R_b, so the attribute b is considered as fake.

E. MAXIMUM-CONSENSUS-CALCULATION

Maximum-consensus-calculation is utilized to compute the real identity after forgery detection, it is a variation of order-of-consensus-calculation. Due to the similarity with algorithm 1, detailed description of the algorithm is not given any more, only the different aspects are introduced as follows. First the input R_i is different from algorithm 1, for maximum-consensus-calculation, it should be removed the results obtained by fake attributes. For example, when $N = 3$, the attribute a is detected as fake with proposed method, so result R_a should be eliminated from R_i, it means that R_a is not used with calculation. On the other hand, the end condition is also different. For algorithm 1, it is that the consensus value of one identity is greater than $N/2$; but for this algorithm, we need to find consensus identities with the maximum consensus value. Assuming that the number of fake attributes detected is $\bar{M}$, if exists identity O_j satisfies the condition (5), the algorithm goes to end.

$$d[O_j] = N - \bar{M} \tag{5}$$

Then revise *identity* and keep one consensus identity O_j, O_j is considered as real identity; otherwise, the calculation process need continue until *order* equals K, then we choose consensus identities with maximum consensus value, and use the same revised rule to keep one consensus identity O_m in *identity*, finally O_m is recognized as real identity. The revised rule is same as step 7 of algorithm 1.

The key to maximum-consensus-calculation method is to record and update consensus value of each identity in order, the end conditions mainly focus on consensus value, one is when finding one identity satisfies condition (5); the other is that finding a consensus identity with the maximum consensus value, then real identity will be obtained with analysis. By using the previous example, attribute b is detected as fake, so the result R_b is removed. With calculation, we find that the consensus value of identity O_3 is equal to 2, the real identity is O_3.

IV. EXPERIMENTS AND RESULTS

In this section, we begin with an introduction of the dataset, then show several experiments and give necessary analysis of the results in detail, finally make a discussion about what these results may inspire us in identification.

A. DATASETS

During experiments, since we need multiple attributes of each identity, and existing public dataset does not meet our requirements, so we build our own dataset to evaluate the effectiveness of the proposed method. Our dataset contains two types: one type is gathered from VGG [34], CASIA [35], and speech commands [36] of public datasets. For each kind of attribute, we collect about 300 objects, and each attribute contains five samples, then face-fingerprint-voiceprint are paired as one unique identity randomly; the other is gathered by about 200 volunteers. All of the volunteers are provided their face, fingerprint, and voiceprint, for each attribute, five samples are collected. The dataset contains 500 identities in total, since our method does not use the relationships of attributes from one identity, so combining three attributes into one specific identity in the first type meets our experimental conditions. In experiments, for each attribute, three samples are used for training during recognition; the first 200 objects are used to train the parameters and the remaining are used to evaluate performance of our method. Fake attributes are generated by replacement randomly with corresponding attributes of other objects. For example, we use face of O_1 to replace O_2, the face of O_2 is fake. The benefit of this is that O_2 can impersonate O_1 more realistic, which caused the detection is more challenging. Besides, it can represent different kinds of attacks. Therefore, the use of replacement to generate fake attributes is much better than a specific fake attributes.

B. EXPERIMENTS AND ANALYSIS

1) HYPOTHETICAL TEST EXPERIMENTS

First experiments are designed to verify the proximity relationship caused by natural and human behaviors. Two pairs of distances are calculated with face attribute, one is the test object with its recognition result object (it's abbreviated as recognition object in Figs. 4-5), and another is test object with its real identity object (it's abbreviated as real object in Figs. 4-5). The distance is obtained with the Euclidean distance between face feature vectors in equation (6).

$$d(v_1, v_2) = \sqrt{(v_1 - v_2)(v_1 - v_2)^{\mathrm{T}}} \tag{6}$$

where v_1 and v_2 represent the feature vectors of face images.

In order to illustrate the proximity relationship caused by natural behavior, we select 100 face images with wrong

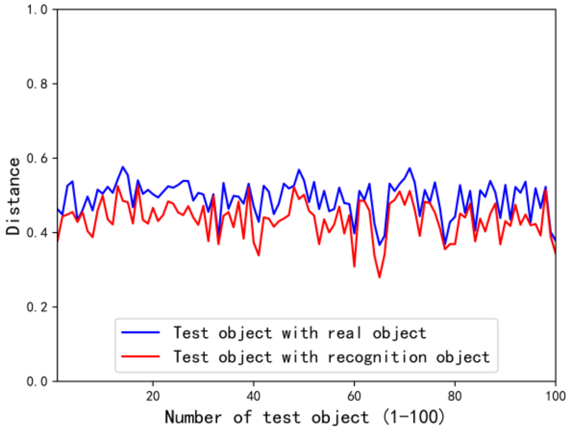

FIGURE 4. An illustration of distance with 100 objects caused by natural behavior. The distance of two lines is almost same, and the distance increment is about 9% on average, so we think that the wrong results caused by natural behavior have proximity relationship.

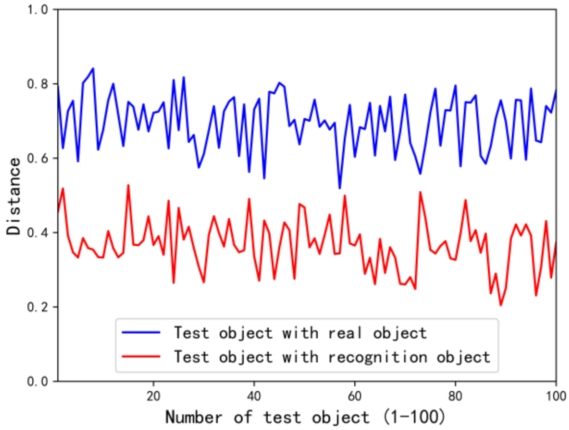

FIGURE 5. An illustration of distance with 100 objects caused by human behavior. The distance in blue line is obviously larger than distance in red line, and the distance increment is about 117% on average, so we think that the wrong results caused by human behavior do not have proximity relationship.

results due to recognition defects as test objects to represent natural behavior, and distance is shown in Fig. 4. With calculation, we can find that even with wrong recognition results, the distance in blue line is only about 9% larger than the distance in red line on average.

In order to illustrate the proximity relationship caused by human behavior, we choose 100 face images and then replace randomly with face images from different identity as test objects to represent human behavior, and the result of distance is shown in Fig. 5. With F-test, Student's t test of mathematical statistics, and necessary analysis, we have enough confidence to show that the distance in blue line is obviously larger than the distance in red line, and the average value is 117% larger.

Comparing two pairs of distances in Figs. 4-5, the distance distribution caused by two behaviors is significantly different. As can be seen that the distance increment in Fig. 5 is much larger than that in Fig. 4, so we make a conclusion that the wrong recognition results caused by natural behavior have proximity relationship, but caused by human behavior do not have proximity relationship. Furthermore, due to the differences of proximity relationship, we find that the rank of real identity in result R_i is obviously different, and it is presented in Fig. 3.

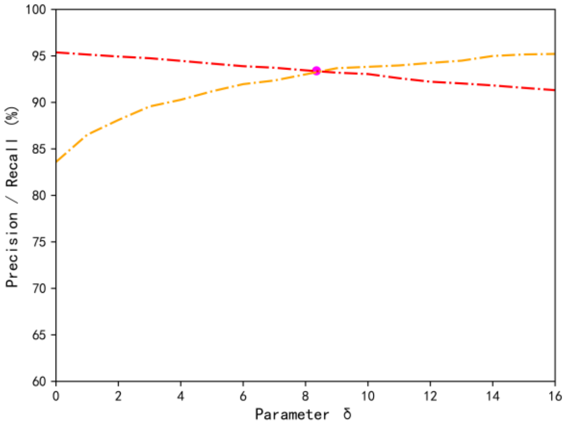

FIGURE 6. The change of precision and recall curves with parameter δ. At the intersection, the values of precision and recall reach maximum simultaneously, and detection performance reaches optimal.

2) EVALUATION METRICS

To evaluate the performance of our method, we calculate P, R, and F_1 values [37], the definitions are as follows:

$$P = \frac{number\ of\ fake\ attributes\ detected\ correctly}{num\ of\ fake\ attributes\ detected} \quad (7)$$

$$R = \frac{number\ of\ fake\ attributes\ detected\ correctly}{num\ of\ all\ fake\ attributes\ in\ dataset} \quad (8)$$

$$F_1 = \frac{2 * P * R}{P + R} \quad (9)$$

where P indicates whether the fake attributes detected by the method are accurate, R indicates whether the fake attributes detected by the method are comprehensive, and F_1 is the harmonic mean of P and R. So the P, R, and F_1 values could better reflect performance of the proposed method.

3) FAKE ATTRIBUTES DETECTION

In order to obtain optimal value of parameter δ, we use 200 objects to train with calculation of precision and recall. Fig. 6 shows the result of precision and recall curves with δ changes, from Fig. 6 we can see that when δ is too small, some normal attributes are detected as fake attributes; but when δ is too large, some fake attributes are detected as normal attributes, so it is not reasonable to set δ value too larger or too small, it will directly affect the performance. As shown in Fig. 6, when δ equals to the approximate value at the intersection, the values of precision and recall achieve best at the same time, and the detection results reach optimal, so the value of parameter δ equals to 8 in the following experiments.

In experiments, we set different situations which contain different proportions of fake attributes, and fake attributes are generated with random numbers for many times. We use Q to describe the situations:

$$Q = \frac{\textit{numof}\text{ objects contain } \textit{fake attributes}}{\textit{num of all unknown objects}} \tag{10}$$

And Q is set with 0, 1/5, 2/5, 3/5, 4/5 and 1, the process is repeated several times in order to obtain the average of the results. Since existing forgery detection methods introduced in related work use the differences between fake and normal attributes, so it is not feasible to make comparisons with our method directly, we only make comparison of performance with majority voting method. Table 2 shows results with P, R, and F_1 values, the parameters are with $K = 20$, $\delta = 8$.

TABLE 2. Performance comparison between proposed method and the majority voting.

Method	P/%	R/%	F_1
Majority voting	71.84	75.24	0.735
Our method	**93.38**	**93.91**	**0.936**

Comparing the results in Table 2, it can be seen that the detection of proposed method performs well, and F_1 value reaches 0.936; while for majority voting, the performance drops drastically, because it can only detect a part of fake attributes, and F_1 value is only 0.735. It is apparent from this table that the proposed method is better than majority voting.

To further verify the effectiveness of our method, we design experiments which contain only one type of fake attribute. Table 3 presents the results of P, R, and F_1 values with only fake fingerprints are included. From this table, the F_1 value of proposed method is 0.917, it is much higher than 0.722 with majority voting, and the detection performance is increased by about 27% with simple calculation, which also demonstrates that our method is effective even with a single type of fake attributes.

TABLE 3. Performance comparison between proposed method and the majority voting when only fake fingerprints are included.

Method	P/%	R/%	F_1
Majority voting	70.34	74.12	0.722
Our method	**91.25**	**92.06**	**0.917**

In order to make comparisons with some approaches in section II, we calculate the same metrics of APCER, BPCER, and ACER with definitions in [27], the results are as follows: with proposed method, APCER is about 5.4%, BPCER is about 2.0%, and ACER is about 3.7%. According to results of the methods listed in [26], our method has a lower APCER compared to most methods, the value of BPCER is only much larger than some methods, it shows that the system with our method is more security, and ACER is also very competitive with other methods. Due to slight differences with our research issue, we cannot only compare the absolute values directly. From above comparisons, we know that the performance of our method has been very good overall, and it can deal with different types of attacks, even with unknown attacks and also obtain real identity with fake attributes.

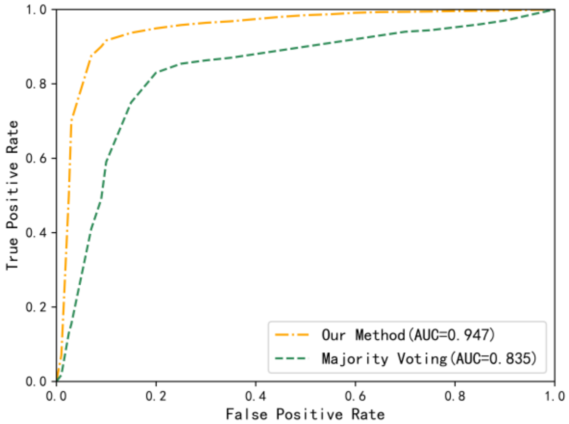

FIGURE 7. ROC curve with comparison of majority voting method.

To compare the detection performance directly between majority voting and proposed method, the ROC (Receiver Operating Characteristic) curve is shown in Fig. 7. True positive rate (TPR) represents the proportion of the number of fake attributes detected correctly in the number of fake attributes in dataset, false positive rate (FPR) indicates the proportion of the number of fake attributes detected wrongly in the number of normal attributes in dataset. The formulas are as follows:

$$TPR = \frac{TP}{TP + FN} \tag{11}$$

$$FPR = \frac{FP}{FP + TN} \tag{12}$$

In our paper, TP indicates the number of fake attributes predicted as fake attributes, and FN represents the number of fake attributes predicated as normal attributes; FP indicates the number of normal attributes predicated as fake attributes, and TN represents the number of normal attributes predicated as normal attributes.

As Fig. 7 shows, there is a significant difference between the two line. The AUC (Area Under Curve) can illustrate the effect of different method. From this figure, the AUC of our method is 0.947, while the majority voting method is only 0.835. With comparison, it can be seen that the effect of proposed method is better than majority voting. Under complicated situation, the performance of majority voting decreases obviously, because it can only detect a part of fake attributes, while the proposed method can effectively detect fake attributes.

Moreover, we also make some analysis about the detection results. In experiments, fake attributes are generated by replacement randomly. By analyzing the wrong detection results, it shows that about 74% is mainly caused by unreasonable replacement, such as an attacker O_1 attempts to impersonate O_2 with mask, while O_1 and O_2 are similar originally at face attribute. So in real scenarios, our method will obtain much better performance.

4) REAL IDENTITY COMPUTING

To further evaluate the effectiveness and necessity of forgery detection during recognition, the real identity of unknown person is acquired to compute the accuracy of identity recognition. Based on the above experiments, we compute real identity with maximum-consensus-calculation after forgery detection. The results are listed in Table 4. It can be seen that the recognition accuracy increases about 13% with the proposed method, and also shows the importance of forgery detection during recognition.

TABLE 4. Accuracy of identity recognition after forgery detection.

Method	Accuracy/%
Without forgery detection	82.39
Ours	**95.57**

Corresponding to the results in Table 3, we also compute real identity with only fake fingerprints are included, the results are presented in Table 5. From this table, we can see that our method can still get better results with single fake attributes.

As can been seen from Tables 4-5, while without forgery detection, we combine the recognition results of each attribute in decision level with majority voting to obtain real identity, the accuracy is only about 80%, which confirms that fake attributes seriously affect the accuracy of recognition. But with proposed method, the accuracy of real identity is about 95%, which improves a lot. In identification systems, it is relatively easy to forge attributes to conceal real identity, with proposed method, we can also obtain real identity even with the existence of fake attributes. Under confrontational environment, forgery detection may play an important role in computing real identity with the existence of fake attributes, and it can also improve the security of recognition systems.

TABLE 5. Accuracy of identity recognition after forgery detection when only fake fingerprints are included.

Method	Accuracy/%
Without forgery detection	78.36
Ours	**95.12**

5) ADDITIONAL EXPERIMENTS

Furthermore, we extend the attributes to four types with iris, and iris is gathered from CASIA dataset, and set the condition with $M = 50\%N$ to investigate the performance of our method. We modify the condition in step 4 of algorithm 1 with $d[O_j] \geq N/2$, and obtain consensus identity. Table 6 shows the P, R, and F_1 values with increase of fake attributes, since the proportion of fake attributes is equal to 50%, so the results of majority voting are not given any more in the table.

TABLE 6. Performance comparison between proposed method and the majority voting with increase of fake attributes.

Method	P/%	R/%	F_1
Majority voting	/	/	/
Our method	90.08	84.82	0.874

The F_1 of our method is 0.874, it can be compared with the data in Table 2, despite the performances decrease slightly, the results also provide further support for forgery detection with the proportion of fake attributes increases. For further study, we will explore what conditions that the number of fake attributes should meet under calculation can be realized, and study methods for fake attributes detection.

C. DISCUSSION

Overall, these results indicate that the proposed method performs better than majority voting, the main cause is as follows: for majority voting, it focuses on the first identity in recognition result to calculate real identity. When the first identity in R_i is not real identity caused by natural behavior, the consensus identity cannot be obtained correctly, so the detection effect decreases obviously; while for proposed method, we choose top K identities in the result instead of only relying on the first identity. As the first identity is incorrect caused by natural behavior, based on differences of proximity relationship caused by two behaviors, it could also obtain consensus identity with top K identities by using order-of-consensus-calculation, therefore fake attributes can also be detected correctly. In summary, our method is better than majority voting.

With above results, one interesting finding is that the differences of proximity relationship caused by natural and human behaviors, and maybe this finding is particularly useful in solving fake attributes during identification. As shown in Tables 2-3, it can be seen that the proposed method is better than majority voting. The method can also deal with different kinds of fake attributes, even with unseen attacks, it can still work and obtain better performance. Interestingly, our method is effective with a single kind of fake attributes, which means that it may provide a new solution for single fake attributes detection. Comparing the results in Tables 4-5, it shows the significance of forgery detection in identification. The results in Table 6 illustrate the feasibility of detection with the proportion of fake attributes increases. Most importantly, the results of differences between natural and human behaviors are vital to understand the process of recognition. To sum up, these results mean that the real identity could also be obtained better with existence of fake attributes under confrontational environment.

In conclusion, we attempt to analyze the causes of errors in recognition results, and summarize them as the differences between natural and human behaviors. In real life, we may use the two behaviors to solve practical problems. For example, in criminal investigation, we need to identify the suspect quickly. Supposing that in the information obtained at the scene, we find that the video is covered by a 3D face mask, and fingerprint extracted from the scene is blurred, and other evidence information may also with low quality. During identification, the results acquired by face and fingerprint may be wrong due to natural and human behavior, which will bring difficulties in determining real identity of suspect for law enforcement agency, so it is critical to realize the differences of wrong results caused by two behaviors. Based on the concepts proposed in this paper, we could analyze the differences of proximity relationship caused by the wrong results, and detect fake attributes and obtain real identity of the suspect. Therefore, it is significant to explore the essential differences between natural and human behaviors, with understanding of the differences, we can better detect fake attributes to further improve the security of identification systems.

V. CONCLUSION

Aiming at the existence of fake attributes during identity recognition, a novel method is proposed for detecting fake attributes and computing real identity in this paper. We start by exploring the wrong results caused by natural and human behaviors, and use proximity relationship to show the differences between two behaviors, by analyzing the rank of real identity, order-of-consensus-calculation is presented to detect fake attributes, and experimental results on dataset demonstrate that our method can obtain better performance compared to majority voting method. Moreover, maximum-consensus-calculation is used to calculate real identity, the accuracy improves a lot, which indicates that the method has possessed the robustness to obtain real identity while with existence of fake attributes. More importantly, the proposed method can detect different kinds of fake attributes, even with unknown attacks, instead of one special attack.

Further research should be focused on the boundary of fake attributes with expansion of the types of attributes. As the proportion of fake attributes increases, we will verify the effectiveness of proposed method, and investigate in what conditions forgery detection can be achieved, and study novel methods further for improving the security of identity recognition systems under complicated environment.

REFERENCES

[1] B. Biggio, G. Fumera, G. L. Marcialis, and F. Roli, "Statistical meta-analysis of presentation attacks for secure multibiometric systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 3, pp. 561–575, Mar. 2017.

[2] A. Agarwal, D. Yadav, N. Kohli, R. Singh, M. Vatsa, and A. Noore, "Face presentation attack with latex masks in multispectral videos," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jul. 2017, pp. 81–89.

[3] E. Tabassi, T. Chugh, D. Deb, and A. K. Jain, "Altered fingerprints: Detection and localization," in *Proc. IEEE 9th Int. Conf. Biometrics, Appl. Syst. (BTAS)*, Redondo Beach, CA, USA, Oct. 2018, pp. 1–9.

[4] K. M. Heussner. (Dec. 2009). *Surgically Altered Fingerprints Help Woman Evade Immigration*. ABC News. [Online]. Available: https://abcnews.go.com/Technology/GadgetGuide/surgicallyaltered-fingerprints-woman-evade-immigration/story?id=%209302505

[5] G. A. Wang, H. Chen, J. J. Xu, and H. Atabakhsh, "Automatically detecting criminal identity deception: An adaptive detection algorithm," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 36, no. 5, pp. 988–999, Sep. 2006.

[6] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognit. Lett.*, vol. 79, pp. 80–105, Aug. 2016.

[7] J. Fierrez, A. Morales, R. Vera-Rodriguez, and D. Camacho, "Multiple classifiers in biometrics. Part 2: Trends and challenges," *Inf. Fusion*, vol. 44, pp. 103–112, Nov. 2018.

[8] A. F. R. Rahman, H. Alam, and M. C. Fairhurst, "Multiple classifier combination for character recognition: Revisiting the majority voting system and its variations," in *Proc. Int. Workshop Doc. Anal. Syst.*, Princeton, NJ, USA, Aug. 2002, pp. 167–178.

[9] S. Yoon, J. Feng, and A. K. Jain, "Altered fingerprints: Analysis and detection," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 3, pp. 451–464, Mar. 2012.

[10] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Washington, DC, USA, Oct. 2011, pp. 1–7.

[11] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Washington, DC, USA, Oct. 2011, pp. 1–7.

[12] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in *Proc. 11th Euro. Conf. Comput. Vis.*, Crete, Greece, Sep 2010, pp. 504–517.

[13] J. Feng, A. K. Jain, and A. Ross, "Detecting altered fingerprints," in *Proc. 20th Int. Conf. Pattern Recognit.*, Istanbul, Turkey, Aug. 2010, pp. 1622–1625.

[14] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," *IEEE Trans. Image Process.*, vol. 23, no. 2, pp. 710–724, Feb. 2014.

[15] R. Raghavendra and C. Busch, "Robust scheme for iris presentation attack detection using multiscale binarized statistical image features," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 4, pp. 703–715, Apr. 2015.

[16] R. Sanchez-Reillo, H. C. Quiros-Sandoval, I. Goicoechea-Telleria, and W. Ponce-Hernandez, "Improving presentation attack detection in dynamic handwritten signature biometrics," *IEEE Access*, vol. 5, pp. 20463–20469, 2017.

[17] J. Yang, Z. Lei, and S. Z. Li, "Learn convolutional neural network for face anti-spoofing," 2014, *arXiv:1408.5601*. [Online]. Available: http://arxiv.org/abs/1408.5601

[18] D. Menotti, G. Chiachia, A. Pinto, W. Robson Schwartz, H. Pedrini, A. X. Falcao, and A. Rocha, "Deep representations for iris, face, and fingerprint spoofing detection," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 4, pp. 864–879, Apr. 2015.

[19] J. Gan, S. Li, Y. Zhai, and C. Liu, "3D convolutional neural network based on face anti-spoofing," in *Proc. 2nd Int. Conf. Multimedia Image Process. (ICMIP)*, Wuhan, China, Mar. 2017, pp. 1–5.

[20] Y. Atoum, Y. Liu, A. Jourabloo, and X. Liu, "Face anti-spoofing using patch and depth-based CNNs," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Denver, CO, USA, Oct. 2017, pp. 319–328.

[21] I. Manjani, S. Tariyal, M. Vatsa, R. Singh, and A. Majumdar, "Detecting silicone mask-based presentation attack via deep dictionary learning," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1713–1723, Jul. 2017.

[22] R. Shao, X. Lan, and P. C. Yuen, "Deep convolutional dynamic texture learning with adaptive channel-discriminability for 3D mask face anti-spoofing," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Denver, CO, USA, Oct. 2017, pp. 748–755.

[23] R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch, "Extended multispectral face presentation attack detection: An approach based on fusing information from individual spectral bands," in *Proc. 20th Int. Conf. Inf. Fusion*, Xi'an, China, Jul. 2017, pp. 1–6.

[24] J. Liu and A. Kumar, "Detecting presentation attacks from 3D face masks under multispectral imaging," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Salt Lake City, UT, USA, Jun. 2018, pp. 47–52.

[25] R. Raghavendra, N. Vetrekar, K. B. Raja, R. S. Gad, and C. Busch, "Detecting disguise attacks on multi-spectral face recognition through spectral signatures," in *Proc. 24th Int. Conf. Pattern Recognit. (ICPR)*, Beijing, China, Aug. 2018, pp. 3371–3377.

[26] A. George, Z. Mostaani, D. Geissenbuhler, O. Nikisins, A. Anjos, and S. Marcel, "Biometric face presentation attack detection with multi-channel convolutional neural network," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 42–55, May 2020.

[27] R. Tolosana, M. Gomez-Barrero, C. Busch, and J. Ortega-Garcia, "Biometric presentation attack detection: Beyond the visible spectrum," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1261–1275, Aug. 2020.

[28] V. Kazemi and J. Sullivan, "One millisecond face alignment with an ensemble of regression trees," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Columbus, OH, USA, Jun. 2014, pp. 1867–1874.

[29] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Las Vegas, NV, USA, Jun. 2016, pp. 770–778.

[30] H. Bay, T. Tuytelaars, and L. V. Gool, "Surf: Speeded up robust features," in *Proc. 9th Eur. Conf. Comput. Vis.*, Graz, Austria, May 2006, pp. 404–417.

[31] M. Muja and D. G. Lowe, "Scalable nearest neighbor algorithms for high dimensional data," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 36, no. 11, pp. 2227–2240, Nov. 2014.

[32] N. Chauhan, T. Isshiki, and D. Li, "Speaker recognition using LPC, MFCC, ZCR features with ANN and SVM classifier for large input database," in *Proc. IEEE 4th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Vellore, India, Feb. 2019, pp. 1–4.

[33] T. Kam Ho, J. J. Hull, and S. N. Srihari, "Decision combination in multiple classifier systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 16, no. 1, pp. 66–75, Jan. 1994.

[34] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep face recognition," in *Proc. Brit. Mach. Vis. Conf.*, Swansea, U.K., Sep. 2015, pp. 1–12.

[35] T. Tan. *CASIA-FingerprintV5*. Accessed: Aug. 2010. [Online]. Available: http://biometrics.idealtest.org/

[36] P. Warden, "Speech commands: A dataset for limited-vocabulary speech recognition," Apr. 2018, *arXiv:1804.03209*. [Online]. Available: http://arxiv.org/abs/1804.03209

[37] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.

YAHAO ZHANG received the B.S. degree in computer science and technology from the Ocean University of China, Qingdao, China, in 2017. He is currently pursuing the M.S. degree with the National Engineering Research Center for Multimedia Software, Wuhan University. His research interests include fake attributes detection and trusted computing.

RUIMIN HU (Senior Member, IEEE) received the B.S. and M.S. degrees in communication and electronic system from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 1984 and 1990, respectively, and the Ph.D. degree in communication and electronic system from the Huazhong University of Science and Technology, Wuhan, China, in 1994. He is currently the Director of the Hubei Key Laboratory of Multimedia and Network Communication Engineering and the National Engineering Research Center for Multimedia Software, Wuhan University, Wuhan, Hubei. His research interests include multimedia understanding and image/video processing.

DENGSHI LI (Member, IEEE) received the Ph.D. degree in communication and information system from Wuhan University, Wuhan, China, in 2018. She is currently an Associate Professor with Jianghan University. Her research interests include sound field reproduction, audio and video coding, signal processing, and so on.

XIAOCHEN WANG (Member, IEEE) received the B.S. degree in cartography and geography information system and the Ph.D. degree in communication and information system from Wuhan University, in 2003 and 2011, respectively. Since 2011, he has been with Wuhan University. His research interests include speech/video coding and rendering.