

Received October 13, 2021, accepted November 17, 2021, date of publication November 30, 2021, date of current version December 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3131408

Mobile Device Fingerprint Identification Using Gyroscope Resonance

JUNZE TIAN¹, JIANYI ZHANG^{1,2,3}, XIUYING LI¹, CHANGCHUN ZHOU¹,
RUILONG WU¹, YUCHEN WANG¹, AND SHENGYUAN HUANG¹

¹Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China

²School of Computing and Informatics, University of Louisiana at Lafayette, Louisiana, LA 70503, USA

³Key Laboratory of Network Assessment Technology, CAS, Beijing 100093, China

Corresponding author: Jianyi Zhang (zjy@besti.edu.cn)

This work was supported in part by the Key Laboratory of Network Assessment Technology, CAS, under Grant KFKT2019-004; in part by the National First-Class Undergraduate Major Construction Sites; and in part by the Beijing High-Precision Discipline Construction Program.

ABSTRACT Device fingerprint is information about the target computing device for the purpose of identification. The fingerprinting algorithm that how to assimilate the target into an identifier has been well studied for more than 20 years. However, the recent obfuscation method against device fingerprinting makes collecting this information more difficult. In order to solve these problems, this paper proposes a new type of fingerprinting method that relies on the resonant frequency response of the gyroscope. Our method first generates an ultrasonic as the trigger signal and obtains the sensor's output through the application program or the web browser as the response. After the sensor output being normalized during the data preprocessing, resonance features are extracted after frequency domain analysis. Finally, the mobile device is identified through these features matching. In the experiment, we test many types of mobile phones to demonstrate that our method is feasible while users are unaware of this process. For instance, we find that some features are stable when the posture of the mobile device or the time change. There are 10 features based on resonance frequency that can help us improve the classification accuracy to 96.5%. The comprehensive experiments demonstrate that our method can effectively distinguish different types of mobile devices. Even if it is the same model of mobile devices with the same type of gyroscopes, this method still has a good performance.

INDEX TERMS Device fingerprint, gyroscope resonance, mobile device.

I. INTRODUCTION

Device fingerprint [1], also known as a device ID or device identification, is information derived from various devices for the purpose of identification. It is calculated by analyzing different characteristics or combining certain attributes of a specific device. Nowadays, device fingerprint has become compelling information for marketers and advertisers in reaching potential customers. It could help deliver targeted ads to users based on their activity on their devices like computers, mobiles, or other devices. For example, IMEI (International Mobile Equipment Identity) is used to identify each independent mobile phone and other mobile communication equipment in the mobile phone network. MAC address (Media Access Control Address) used to locate network devices. In addition to these common device identifications,

browser fingerprints [2] can also be called device fingerprints. It obtains the user's hardware and software setting information through the browser or cookies to identify the device.

However, researchers have already built many successful countermeasures to device fingerprinting since the user can easily spoof the fingerprint data by faking attribute values and potentially change it with every request. At the browser level, in order to ensure the safety of local cookies, the client browser adopts unified Cookie encryption for different visited websites and even directly disables cookies [3]. At the operating system level, many tools for spoofing the device data have appeared in recent years. Most of the tools are based on the Xposed framework [4], which can modify device information, including phone model, IMEI, GPS location, MAC address, wireless name, phone number, etc. By constantly refreshing the forged device fingerprints, the purpose of deceiving the device manufacturer's device detection can be achieved so that one mobile phone can be split into

The associate editor coordinating the review of this manuscript and approving it for publication was Usama Mir.

multiple mobile phones. These countermeasures significantly reduce the feasibility of traditional device fingerprints.

Sensor fingerprints can avoid the problems that the traditional fingerprinting method faces. With the increase in the popularity of wearable devices among the general public, mobile devices are equipped with a large number of sensors (gyro [5], accelerometer, magnetometer, front and rear cameras [6], etc.). Since these sensors have inevitable process defects, these will be affected by some specific physical stimuli. For example, micro-electromechanical systems (MEMS) inertial sensors are known to be susceptible to resonant acoustic interferences [7]–[10]. These characteristics make the reaction of the sensors slightly different under specific physical stimuli even though they are the same model. After being converted into features, these differences can be seen as the identification information for device fingerprints. Although Apps may need to request specific permissions to use some sensors like a microphone or camera, the device can still access some sensors like accelerometer and gyroscope with lower permissions.

We propose a new fingerprinting method that relies on the resonant acoustic interferences of the inertial sensors. We select the gyroscope to reduce user perceptions since its resonance frequency is higher than the human hearing range. After sending the trigger signals from the ultrasonic transducer or some off-the-shelf speakers, the data of three axes of the gyroscope will be captured by the App or web browser to form a set of multi-dimensional data. Then we convert the data from the time domain to the frequency domain by the data preprocessing method we proposed and got a 10-dimensional feature matrix. Finally, the multi-dimensional feature matrix is used as the input of the decision tree to identify the specific mobile device. In the experiment, we collected 12 models of mobile phones, a total of 15 sets. The results show that the total classification accuracy rate reached 96.5%. We used five types of mobile phones to collect multiple sets of data at different times in a month to prove the time invariance of fingerprint features. Especially in the experiment, we set up two sets of comparative experiments on the same device. We find that even with the same model of mobile phone, the matching accuracy rate is still high. Therefore, the experiment proves that this method can solve the problem of difficulty in classifying mobile phones of the same type.

The main contributions of this work are summarized as follows:
















- 1) We find a clear difference in the reaction between the sensors for specific physical stimuli, even between the same model or the same type. This difference is a physical characteristic caused by the manufacturing process, which is unique and can be used as a fingerprint for the device.
- 2) We propose a mobile devices fingerprint recognition model and method based on finding the physical characteristic under the resonance. We can accurately distinguish devices of the same model through this method while maintaining stability during long-term testing.




- 3) We propose an independent data sampling and processing method for the device fingerprinting which regardless of the sampling rate, data interface, and application frameworks like App or web. And we design three sensor data collection architectures that can cover most user scenarios.
- 4) We set up a closed-cycle fingerprint scheme based on our proposed method and evaluate this method on 20 most popular mobiles. Our proof-of-concept device fingerprint method demonstrate the difference and stability over different models, different operating systems and even the same model, etc.

II. RELATED WORK

Nowadays, with the development of the Internet of Things, fingerprint research based on device sensors has attracted more and more attention from academia. Crister and Groza [18] studied fingerprint identification of mobile devices using ICMP timestamp through WiFi channels. The results show that it can identify the mobile phone in a few minutes, but the method will fail when the user changes the offset slope. Some studies have shown that each component of the mobile camera has the potential to become device fingerprints. Dirik *et al.* [19] studied the camera fingerprint recognition technology based on the features of dust particle detection and recognition. The experimental results show that the fingerprint extracted by this method cannot be maintained for a long time and will change. The fingerprint features are difficult to reuse, and the robustness is poor. Choi *et al.* [20] found that different camera models use different image compression algorithms. However, the same type of mobile phone has the same number of cameras, so the technology can only identify different types of mobile phones. Ling *et al.* [21] studied the classification model based on sparse representation for experiments and proved that this method could distinguish different brands and different models of the same brand and achieved good results. However, the identification problem of mobile phones with the same brand and the same model is still unresolved. Due to the limitations of this technology, researchers began to focus on other mobile phone sensors. Dey *et al.* [22] proposed a speaker-microphone fingerprint identification method, which needs to use the speaker as the fingerprint excitation device and distinguishes different mobile phones by sending audio at different frequencies and using the microphone to record the data for spectral analysis. However, calling camera sensors often require elevated user permissions, and data acquisition is complex. At the same time, the accelerometer has been widely studied [22], [23], [24], because of its high utilization rate in software and low access rights. Bojinov *et al.* [25] also proposed the use of accelerometer calibration error to construct sensor fingerprints. However, their method has limitations since they need to verify whether the device is horizontal and stationary before each work. Two years later, Das *et al.* [26] studied the working principles of gyroscopes and accelerometers, explained the causes of

TABLE 1. Motion sensors based mobile device fingerprints methods.

Equipment	Sensors	Collection	Classification	Results	Paper
4170 devices	  	App	KNN, SVM, Bagging Tree, Random Forest	Accuracy:78%	[11]
3 smartphones	 	App	SVM	Accuracy:80%	[12]
20 smartphones	  	App	Random Forest	F1:0.9	[13]
15 devices		web	—	Accuracy:74.4%	[14]
117 smartphones	 	App	LSTM	Accuracy:93%	[15]
795 devices	  	App, Web	Clustering, Euclidean distance	—	[16]
9 smartphones		App	SVM	EER:0.0038	[17]

:Magnetometer :Accelerometer :Gyroscope.

a gyroscope fingerprint caused by production defects, and combined multiple motion sensors to influence the sensor fingerprint by using the invisible audio stimulation. These studies have proved the possibility of using inertial sensors to generate fingerprints. These related studies exposed the limitations of the current sensor device fingerprint. First, data acquisition is complex, and sensor calls need high permissions. Then, the fingerprint difference is low, resulting in a low classification recognition rate. Moreover, in the real world, we cannot stipulate that users can obtain fingerprint data in a specific way that we need to experiment with. For example, due to the different calling interfaces of applications or webpages, the settings that users can artificially change, such as sampling frequency, can usually affect the stability of the fingerprint extraction scheme, so the practicability of the method is not strong.

A. DEVICE FINGERPRINT DATA COLLECTIONS

Data collection is an important part of fingerprint identification. The acquisition target is usually the output of the sensor. It can be known from Section III that access to some sensors does not require user authorization [27], so motion sensors such as accelerometers, gyroscopes, and magnetometers are a suitable target for device fingerprint. Table 1 lists recent papers using motion sensors as device fingerprints. According to this table, their research only adopted one data collection approach, web or App, to get the sensors' output as the fundamental data of fingerprints recognition. There are a lot of differences, like sampling rates, permissions, or metric scales, between web and App. Hence, it isn't easy to collect data under the same conditions for the device fingerprint.

B. DEVICE FINGERPRINT COUNTERMEASURES

FaiKhademi *et al.* [28] proposed a method to prevent fingerprint recognition based on the web. This method prevents fingerprint tracking by adding randomization and filtering techniques. Das *et al.* [26] proposed an obfuscation technique. This technology uses the sensitivity of mean and root mean square to random numbers to randomize sensor fingerprints. Das *et al.* [29] developed a new fingerprint recognition strategy using data quantification in polar coordinates. The data in this method is quantified in the polar coordinate system, and then the sensor's output is changed. Khanna [30] proposed a method to timestamp TCP. The fingerprint identification method based on clock deviation is prevented.

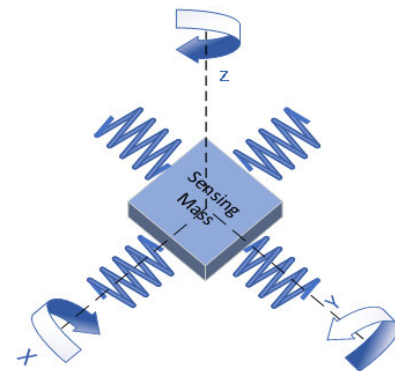


FIGURE 1. The working principle of gyroscope. The mass block inside the gyroscope oscillates back and forth. When it rotates, the Coriolis acceleration will be generated, and the distance between the capacitance plates changes. At this time, it can be measured.

III. BACKGROUND

Motion sensors in smartphones include gyroscopes and accelerometers. STMicroelectronics and Inven Sense are the top two companies in the market share of motion sensors. The motion sensors used by HUAWEI, Xiaomi Corporation, and vivo are all from the products produced by the above two companies.

A. PRINCIPLE OF GYROSCOPE

The physical principle that smartphone gyroscopes rely on is the Coriolis force, as shown in Figure 1. When the gyroscope rotates around any induction axes, the Coriolis effect causes a vibration detected by a capacitive pickup, which causes changes in capacitance and is proportional to the angular velocity. The obtained signal is amplified, demodulated, and filtered to generate a voltage proportional to the angular rate. The voltage is converted into angular velocity rad / s after digitization and then output.

The angular velocity is usually obtained by formula (1).

$$F_k = 2m\omega v \quad (1)$$

where m is the object's mass, ω is the angular velocity, and v is the linear velocity along the driving direction.

B. VULNERABILITY OF GYROSCOPE

The structure of the MEMS inertial sensor like accelerometer or gyroscope makes these sensors vulnerable to ultrasound. Attacks on them are known as out-of-band signal injections. The former research like [31]–[33] proved that the sensor

was vulnerable to the attacks such as EMI and ultrasonic waves. As early as 2014, inspired by the fact that gyroscope signal can identify speech [34], Son *et al.* [35] sent ultrasonic waves of different frequency bands to interfere with the gyroscope in the UAV based on the features of the gyroscope itself and induced the gyroscope to produce resonance, abnormal output data, mislead the direction of the UAV's action, and cause the UAV to crash. Khazaaleh *et al.* [36] assess the vulnerability of MEMS-based gyroscopes to targeted ultrasonic attacks. It points out that the misalignment between the gyroscope's sensing axis and the drive axis is the main reason why the gyroscope is vulnerable to ultrasonic attacks. In addition, [37], and [31] have proved that the attack of accelerometer resonance on gyroscope is effective. The frequency range of the injection signal to accelerometers is around 2kHz, while the frequency to gyroscopes is higher than 20kHz.

C. RESONANCE CHARACTERISTICS OF GYROSCOPE

The MEMS gyroscope in smartphones is generally a single degree of freedom system with a high damping ratio, which is highly susceptible to external stimuli to produce forced vibration. When this forced vibration is close to the natural frequency of the gyroscope itself, its amplitude can reach the maximum value. This is also why the gyroscope is susceptible to being affected by the sound wave signal and response. All the papers [7], [9], [10], [38], [39] proved that gyroscopes are highly sensitive to sound noise. Among them, [38] tested 24 ADXRS300 gyroscopes of the same model and concluded that many tested gyroscopes have low acoustic sensitivity to their resonant frequency at the first harmonic frequency. However, this test shows that the natural frequency of the same device varies greatly. The observed resonance frequency tends to be concentrated in the center of 14 kHz or 16 kHz. In the design, the different materials, structures, shapes, and quality of the gyroscope's manufacturing process affect the resonant frequency of different gyroscopes. Although the same type of gyroscope has the same structure and technology, it will be affected by subtle internal structural changes. As a result of the change in resonance frequency, even if the same batch of products is in mass production, there will inevitably be a difference in natural frequency, which provides a basis for using the difference in natural frequency between gyroscopes as a hardware fingerprint.

D. THE ESTABLISHMENT OF COVERT CHANNEL

The method proposed in this paper needs to use ultrasound as an external stimulus to affect the sensor output. In data collection using sound waves, the noise introduced by external equipment will cause the detection of the target object. It will also interfere with the production and life of the people in the external environment. Therefore, in this section, according to the features of gyroscope and acceleration sensors, the inertial sensors are analyzed from multiple perspectives: permission, physical characteristics, and inaudibility.

TABLE 2. Sensor permission table.

Sensor	Access Rights	Sensor	Access Rights
magnetometer	No	loudspeaker	YES
microphone	YES	GPS module	YES
accelerometer	NO	camera	YES
gyroscope	NO	optical sensor	NO

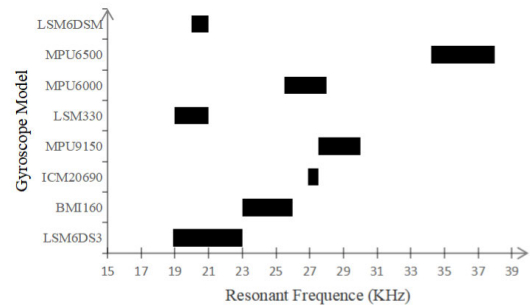


FIGURE 2. The resonance frequencies of the off-the-shelf gyroscopes.

1) FEW PERMISSION REQUIRED

Sensors are widely used in smartphones as hardware devices. In order to protect users' privacy of mobile phones before they leave the factory, technology companies provide users with the power to grant permission and permissions to sensors. In the Android 10.0 version, users have three permissions: always allowed, only allowed during the use, prohibited. Users can allocate the time and function of sensors for the App according to their own needs. Once the permissions are always allowed to be activated, the upload of the sensor data stream will be in a long-term active state, even if the application does not use apps to obtain sensor data without user permission. Once the permission is activated during the use period only, the sending and uploading of data flow do not require user authorization during the use of the application. Table 2 lists the current commonly used mobile phone sensor permissions. In order to facilitate the extraction and collection of large amounts of data, this study can select sensors such as gyroscopes and accelerometers that can collect data without high privileges as target sensors.

2) PHYSICAL CHARACTERISTICS OF SENSORS

Figure 2 shows the resonant frequencies of all gyroscopes tested in this article. Eight gyroscope sensors which occupy 90 % of the current market, also have noticeable differences in response to ultrasonic because of their different internal features. It can be concluded from Figure 2 that this difference is reflected in the length of the resonance frequency band and the difference between the starting and stopping frequencies. The subdivision of the above features makes it possible to use gyroscope resonance features as a new hardware fingerprint.

3) INAUDIBLE COLLECTION PROCESS

According to the features of acoustic waves, between 20Hz and 20kHz is the human ear can hear the frequency range, more than 20kHz ultrasonic is the human ear cannot perceive. The resonance frequency bands of most gyroscopes and accelerometers are shown in Figure 2. Gyroscope resonance

TABLE 3. Ultrasonic characteristics causing resonance of gyroscope and accelerometer. The distance between the speaker and the smartphone is from near to far, and the minimum sound required to make the sensor resonance is recorded. Even if the sound decibel required for accelerometer resonance is 5 m apart, the sound can still reach 65 dB, significantly higher than the environmental noise. The sound decibel required for gyroscope resonance is consistent with the environmental noise decibel, achieving silent data extraction.

Chip Type	Sensor	Distance	Resonant Frequency	Hearable Decibels	Environmental Noise Decibels	Whether People Can Hear
lsm6ds3	accelerometer	5cm	1600Hz	94db	43db	YES
		1m	1600Hz	80db	43db	YES
		5m	1600Hz	65db	43db	YES
	gyroscope	5cm	20200Hz	44db	43db	NO
		1m	20200Hz	43db	43db	NO
		5m	20200Hz	43db	43db	NO
lcm20690	accelerometer	5cm	900Hz	93db	43db	YES
		1m	900Hz	84db	43db	YES
		5m	900Hz	73db	43db	YES
	gyroscope	5cm	27400Hz	43db	43db	NO
		1m	27400Hz	43db	43db	NO
		5m	27400Hz	43db	43db	NO



FIGURE 3. Mobile phone classification workflow based on gyroscope.

frequency tends to be more than 18kHz, almost cannot be perceived by a human, and the accelerometer resonance frequency is below 3kHz chiefly, in the range of human perception. To demonstrate the rigor, we tested two types of chips for a total of four to excite more than twice the average amplitude of the sound wave as a control variable. When the amplitude of the two accelerometer sensors is affected by the resonance frequency, the sound decibels emitted by the loudspeaker are more than 90 decibels, which belongs to the maximum noise value and does not conform to the covert channel. Under the same laboratory experimental environment, the decibels of the audio signal in the range of apparent resonance frequency of gyroscope is approximately equal to the decibels of the environment at that time, which humans ears cannot detect in any range. So gyroscope sensors can be used as the research object of smartphone hardware fingerprints.

IV. OVERVIEW & DESIGN OF THE FINGERPRINT IDENTIFYING

In this section, we present our research motivation, and discuss the design of fingerprint identifying.

A. INTUITION & OVERVIEW

The core intuition behind our fingerprint recognition is to use the fragility of the gyroscope in the ultrasonic environment to identify mobile devices. We found that when there is ultrasound in the environment, the gyroscope's readings will fluctuate differently than usual. We found that this reaction is regular, reflecting that different gyroscopes' resonance bands are unique. Moreover, for gyroscopes, this response is universal and stable. Not only that, many other resonance-related reactions can be used as fingerprints. Because these fingerprints are not based on statistics, they can bypass confusion

and quantification attacks. Considering these advantages, we designed a mobile fingerprint based on resonance.

B. DESIGN OF THE FINGERPRINT IDENTIFYING

This article aims to obtain a stable digital fingerprint from the smartphone's built-in gyroscope sensor. The process of the whole method is shown in Figure 3, which is to collect the test cases of the digital output of the gyroscope. Then we convert the time domain data into frequency domain data through preprocessing, and finally generate the fingerprint feature set and perform the classification decision tree machine learning. The algorithm gets the classification model. Let us take the X-axis of the gyroscope as an example and use the formula to express it as:

$$[X_1, X_2, X_3 \cdots X_n] \rightarrow [F_1, F_2, F_3 \cdots F_i] \rightarrow A \quad (2)$$

where X_n represents the response data of the X-axis of the gyroscope to ultrasound, F_i corresponds to the 19-dimensional feature vector. A is the classification accuracy obtained by the machine learning equipment matching. The steps of this method will be described in sequence in the following subsections. However, before starting the research, some prerequisites need to be put forward first. We assume that users will actively install our designated gyroscope data acquisition application or visit a website designed by us. In addition, we assume that the software embedded in the application or web page can communicate with a remote server under our control. Finally, there are only two positional relationships between the intelligent device and the horizontal plane in the data collection process: parallel and vertical. Moreover, the smart device is static. Most users do not move it violently when using a smart device. Most of the time,

the smart device will be steadily placed on the desktop, test bench, and other relatively stable environments.

C. DATA ACQUISITION AND PROCESSING

With the increase of application scenarios and audiences of motion sensors in the Internet of Things, it has formed a mature industry ecology to obtain many stable motion sensor data streams through mobile applications. It then provides a series of data analysis services for users to control their health. However, two independent application systems are formed due to the difference between the mobile phone iOS and Android operating systems. Forming a cross-platform data collection method for mobile phone users of different systems is more conducive to research development. So we built a lightweight JavaScript (JS) that runs entirely on the web. Relying on the online open-source editing page [40], the code integrates audio playback, frequency sweep, gyro data recording, and file download. The ultrasonic frequency sweep function is realized by AudioNode [41], and the x, y, z-axis angular velocity of the digital output of the mobile gyroscope is obtained by calling the gyroscope API for page monitoring. The event trigger mechanism is used to connect the two modules. Finally, the gyroscope data is transferred to the local database.

In the process of experimental data acquisition, this research needs an auxiliary hardware speaker to generate external ultrasonic signals. So we connect the DG5300 signal generator to the vifa external speaker and transmit the ultrasonic wave to the gyroscope inside the mobile phone. In particular, the smartphone itself also has a built-in speaker. Since the built-in speaker and the gyroscope in the mobile phone are in close contact, if the ultrasonic wave is emitted from the inside to stimulate the motion sensor, it is beneficial to extract the fingerprint of the motion sensor with the minimum energy. Therefore, three data collection architectures are designed, as shown in Figure 4.

External speaker + APP. After the signal generator connects the external speaker, the frequency sweep ultrasonic signal is output. The external speaker and the smartphone are in the same plane, and the data are collected through the application program inside the mobile phone and uploaded to the server background.

External speaker + Web. The signal generator connects the external speaker to output the frequency sweep ultrasonic signal. The external speaker and the smartphone are on the same plane. The data are collected through the online webpage in the browser and uploaded to the user's mobile phone.

Built-in speaker + Web. By developing the JS code, the smartphone's internal speaker is controlled to output the swept ultrasonic wave, and the energy is fed back to the internal chip, which causes the resonance of the motion sensor and collects data. Due to the limitations of the performance of the mobile phone loudspeaker itself, the maximum output audio of the tested mobile phone loudspeaker is 24kHz, which can only cause the resonance of some mobile phone models.

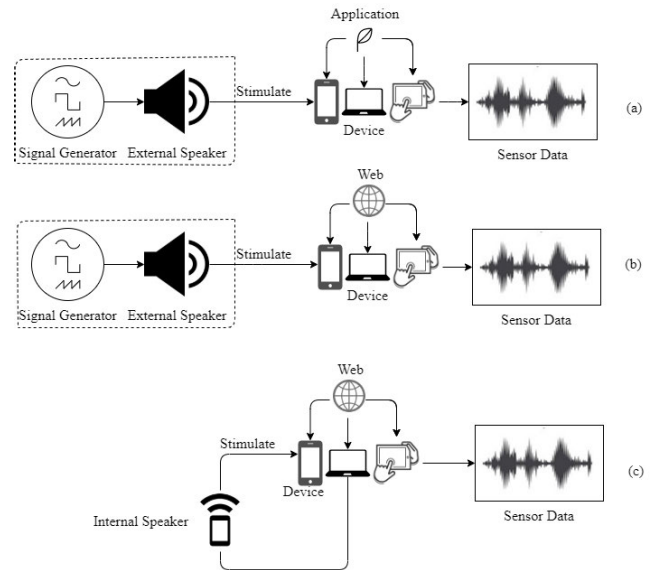


FIGURE 4. Three collection architectures. (a), (b) stimulate smart devices (smartphones, two-in-one computers, tablets) through external speakers, and collect gyroscope data using online webpages and applications, respectively. (c) stimulate smart devices through the speaker of smartphones, and collect data through online web pages.

The collected data is the time series data output by the gyroscope, in the form of X, Y, Z-axis angular velocity output based on its spatial coordinate system. Data are as follows.

$$\begin{bmatrix} X_1 & X_2 & X_3 & \dots & X_n \\ Y_1 & Y_2 & Y_3 & \dots & Y_n \\ Z_1 & Z_2 & Z_3 & \dots & Z_n \end{bmatrix} \quad (3)$$

We get the speed of rotating alpha with the Z-axis as the center. Moreover, the speed of rotating beta with the X-axis as the center. And the speed of rotating gamma with the Y-axis as the center. Their unit is deg/s. Deg is the angle. The unit of data collected by Android is deg/s, and the unit of data collected by the web is rad/s. In order to unify the standard with the angular velocity data collected by the Android application, we convert the angular data into radians. The conversion formula is as follows:

$$R_g = D_g \times (\pi/180) \quad (4)$$

where R_g is radian data and D_g is angle data.

In addition, because the browser limits the sampling rate for security reasons, but the application does not, the dimensions of the data collected through the web are different from the application. In order to achieve the unity of the two, we convert the data to the frequency domain. The formula is as follows:

$$F_g = \frac{X_g}{f} \times S + f_0 \quad (5)$$

Among them, F_g is the final frequency, X_g is the number of sampling points, f is the total sampling times, s is a broad sweep range, here is 10kHz, f_0 is the reference frequency, here is 20kHz. This method normalizes the data to frequency points. This method does not require data alignment.

At the same time, it can avoid data unavailability caused by different sampling rates of web and applications.

D. FEATURE EXTRACTION

Unlike natural language processing and speech recognition, there are mature feature extraction algorithms such as the Mel cepstrum coefficient and machine learning. There are few types of research on fingerprint recognition features based on gyroscope resonance in mobile hardware fingerprint recognition, so this part analyzes the coarse-grained and fine-grained data to determine the feature extraction part with the most significant amount of information. The data samples collected from the above section show that the feature dimension is higher for each sample between three thousand and thirty thousand. If all data are regarded as feature points, irrelevant feature points and noise points will be introduced. In order to facilitate subsequent research and classification, feature points need to be extracted and dimensions reduced. According to the analysis of the existing sample data, it is found that there are more obvious data features by converting each data set into a line graph. These features are extracted as follows.

1) FEATURES OF RESONANCE PEAK

In a resonant frequency band, there is a frequency that makes the forced vibration amplitude reach the peak, and the amplitude corresponding to this frequency is called the energy peak. The peak fluctuates in a particular range, but the magnitude is stable. Three peak features of the X, Y, and Z axis can be used as additional features.

2) POSITION FEATURES OF RESONANCE PEAK

Since gyroscope the differential sensitivity of gyroscope to ultrasonic signals with different frequencies, in the frequency domain, different frequencies correspond to different amplitudes, forming the corresponding envelope. To better describe the envelope, the proportional relationship between the frequency of X, Y, Z-axis resonant peaks and the whole resonant frequency band is extracted as the position representation, and the position relationship is relatively fixed.

3) FEATURES OF RESONANCE BANDWIDTH

The resonant frequency band refers to the gyroscope with different degrees of response to ultrasonic waves. After quantifying the range of response frequency, it is found that this value is stable, and multiple measurements have controllable changes. Therefore, the resonant frequency bandwidths of the X, Y, Z axis are extracted.

4) QUANTITATIVE FEATURES OF RESONANT FREQUENCY BANDS

According to the analysis of the collected data, there is a phenomenon that the resonant frequency band of the gyroscope is discontinuous. Between 20,000–30,000 Hz frequency bands, some sensors have more than one resonant frequency band. Therefore, the 4-fold average is used as the sign of the initial

response, and the 4-fold average is used as the sign of the end response to screen the resonance band, and the number of X, Y, and Z triaxial resonance bands of the sensor is calculated and used as a recognition feature.

5) FREQUENCY FEATURES OF STARTING AND STOPPING VIBRATIONS

The 4-fold average was used as the sign of the beginning response, and the 4-fold average was used as the sign of the end response. The scale of the two positions was recorded and quantified as frequency. The uniqueness of studied that the uniqueness of this feature exists in X, Y, and Z axis. However, since the outliers and noise points in the data acquisition process will affect the extraction of the starting and stopping vibration frequencies, the sliding window is introduced to determine the starting and stopping vibration frequencies when the amplitude of the fixed frequency band after the starting vibration frequency is compared with the average amplitude if there are multiple growths.

6) SAMPLING RATE FEATURES

In Android mobile phones, the sensor sampling rate has four call attributes SENSOR _ DELAY _ NORMAL, SENSOR _ DELAY _ UI, SENSOR _ DELAY _ GAME, SENSOR _ DELAY _ FASTEST from low to high corresponding to four sensitivity. Because of the differences in hardware support and underlying definitions, the acquisition frequency of different phones will be different even if the same attribute sensitivity is called.

E. RECOGNITION BASED ON DECISION TREE

The tree structure algorithm of the decision tree type is often used to construct a classification model. Its essence is a set of rules. It is a typical non-parametric structure algorithm. It does not need logical regression and Naive Bayes algorithm to consider the linear separable problem of outliers and data. Especially in the hardware classification problem studied in this paper, there are 19 features simultaneously. The tree model will pick out the independent variables from all the independent variables according to the contribution so that many independent variables can be automatically processed. Through the analysis of the above section, the data features extracted in this paper have noticeable value differences, and the features are generally continuous variables. The algorithm considers all possible continuous value intervals for multi-channel division and converts them into a fixed discrete interval for model construction. It is more appropriate to use a decision tree for the multi-classification of multiple mobile phones.

Chi-square Automatic Interaction Detector (CHAID) [42] conditional reasoning decision tree. The chi-square statistics used by the CHAID decision tree in node splitting have the strongest interaction between selection and classification categories. If the categories and features of each prediction classification are not significantly different, these categories are merged, and the parent class can branch out

multiple trees. First, do expectation hypothesis, classification independent variables, and classification variables have no relationship. Then do the card test calculation, the formula is as follows [43].

$$\chi^2 = \sum \frac{(A - E)^2}{E} = \sum_k \frac{(A_i - E_i)^2}{E_i} = \sum_k \frac{(A_i - np_i)^2}{np_i} \quad (6)$$

A is the observed value, E is the theoretical value, k is the number of observed values, n is the total frequency, p is the theoretical frequency, $n \times p$ is the theoretical frequency. After calculating the chi-square value of each feature, the greater the χ means, the greater the gap between the predicted situation and the actual situation, which proves the greater the correlation between the independent variables and the classification variables. Then the optimal chi-square value is used as the priority classification basis for category prediction.

CRT classification regression tree. The algorithm can consider all possible division points in binary division and select the division point that produces the best structure. The Gini coefficient judges it. The smaller the Gini coefficient, the purer the node and thus split the node.

Assuming that the collected overall data sample is set D , the Gini coefficient [44] is:

$$Gini(D) = 1 - \sum_k \left(\frac{|C_k|}{|D|} \right)^2 \quad (7)$$

C_k is the sample subset of the K class. For the Gini coefficient of feature A , the sample is divided into two parts D_1 and D_2 of $A = a$ and $A \neq a$, and the Gini coefficient of feature A is [44]:

$$Gini(D, A) = \frac{D_1}{D} Gini(D_1) + \frac{D_2}{D} Gini(D_2) \quad (8)$$

The smaller the Gini index of feature A is, the smaller the sampling uncertainty is. Select the binary classification that minimizes $Gini(D, A)$ and perform hierarchical recursion to meet the termination conditions. This paper establishes the classification model based on the above two decision tree algorithms, obtained good results.

V. EXPERIMENT AND RESULT ANALYSIS

We used 5 gyroscope chips and 20 smartphones to evaluate the performance of gyroscope fingerprints. The key issues we investigated and the corresponding research results are summarized as follows.

- 1) It only takes 60 seconds to generate a reliable fingerprint.
- 2) Whether it is placed on the desktop horizontally or vertically, its characteristics remain stable. In a stationary situation, there is no need to consider the posture of the device.
- 3) Whether it is a short-term continuous measurement or a long-term interval measurement, the fingerprint remains stable.
- 4) Fingerprints have an excellent effect on the identification of iOS and Android phones.



FIGURE 5. Experimental equipment placement status. The intelligent equipment is placed on the experimental platform at the level of Figure 5. The Vifa speaker is placed in the Y-axis direction of the device, 5 cm away from the device. An ultrasonic sweep signal is generated in the signal generator, which affects the intelligent equipment through the Vifa speaker and observes the output.

- 5) It is feasible to integrate data between App and the web. The data processing method proposed in this article allows data from different data sources to form unified features.

A. EXPERIMENTAL DEVICE

Figure 5 shows the experimental setup. The experimental equipment includes: 1. DG5300 signal generator is used to generate sweep frequency ultrasonically. Here the output amplitude is set to 5v. 2. Power amplifier is used to enhance signal power. 3. Vifa speaker is responsible for outputting ultrasound. 4. 20 mobile phones that have downloaded the gyroscope App. As shown in Table 4, Android devices include Huawei's mainstream models: mate series and p series. And Xiaomi, Redmi, vivo, Honor, OnePlus, and other products. iOS devices include Apple's mainstream models: Apple 12 pro, Apple 11, and Apple XR. Before starting the experiment, we fixed the sweep time interval of the signal generator to 60s, the starting frequency is 20kHz, and the ending frequency is 30kHz.

B. OVERALL FINGERPRINT VERIFICATION

The first experiment. We chose 15 Android phones of 12 models. The number of Huawei Mate 30 phones of the same model is three, and the number of Honor 8 phones is two. We measured 25 groups of gyroscope outputs using web and App, and a total of 750 data constitute a data set. Using these raw gyroscope data, we generated 19 features. We found that all three axes of mobile phones have resonance features. The resonance of the Z-axis of the Mi 8 and the Y-axis of the Huawei P10 is extremely weak, and the resonance amplitude is confused with the amplitude fluctuation of the gyroscope when it is stationary, so we set its feature value to 0.

TABLE 4. The three axes resonance frequency and sampling frequency of gyroscope in 15 smartphones. When the sensor chip is installed inside the mobile phone, the resonant frequencies of the gyroscopes are significantly different from each other, and the sampling frequencies are different.

Chip Enterprises	Chip Type	Equipment Type	Gyroscope Resonance Frequency(10^4 Hz)			Sampling Frequency(Hz)
			X-axis	Y-axis	Z-axis	
Invensense	ICM20690	Huawei Mate 30	2.702-2.754	2.704-2.758	2.702-2.752	507
	ICM20690	Mi 8	2.664-2.727	2.668-2.723	-	407
	ICM20690	Huawei P10	2.669-2.741	-	2.673-2.736	505
	ICM20690	Huawei Mate 10 Pro	2.672-2.747	2.679-2.744	2.698-2.735	506
	ICM4X6XX	Redmi K20	2.584-2.801	2.446-2.582	2.511-2.659	506
STMicroelectronics	LSM6DS3	Honor 8	2-2.066	2-2.065	2-2.075	102
	LSM6DS3	vivo X9	2.008-2.024	2.01-2.024	2.01-2.025	105
	LSM6DS3	Huawei nova 2S	2-2.02	2-2.023	2-2.025	200
	LSM6DSM	Huawei Mate10	2-2.078	2-2.082	2-2.072	504
	LSM6DSM	OnePlus 8 Pro	2-2.081	2-2.112	2-2.032	423
	LSM6DSM	Porsche Design Huawei Mate 30 RS	2-2.099	2-2.119	2-2.114	503
	LSM6DSM	Huawei Mate 20	2-2.076	2-2.075	2-2.077	506
Bosch	BMI282AA	iPhone 12 Pro	2.51-2.583	2.499-2.55	-	100
	BMI282AA	iPhone 11	2.67-2.74	2.67-2.74	2.68-2.72	100
	BMI282AA	iPhone SE (2nd generation)	2.41-2.55	2.43-2.5	-	100
	BMI282AA	iPhone XR	2.5-2.55	2.51-2.54	-	100

TABLE 5. Three decision tree classification accuracy comparison. SF_y : Y-axis stop frequency. $RFBW_y$: Y-axis resonance frequency bandwidth. $RFBN_y$: Y-axis resonance frequency band number. STF_x : X-axis start frequency. SF_x : X-axis stop frequency. SF_z : Z-axis stop frequency. $RFBW_z$: Z-axis resonance frequency bandwidth. $RFBW_x$: X-axis resonance frequency bandwidth. $RFBN_x$: X-axis resonance frequency band number. $RFBN_z$: Z-axis resonance frequency band number. CF_y : Y-axis cutoff frequency.

Recognition Algorithm	Optimal Features	Splitting Node	Accuracy
Chaid Decision Tree	$RFBW_y + CF_y$	Chi-square Test	70%
Classification Regression Tree	$SF_y + RFBN_y + STF_x + SF_x + STF_z + SF_z + RFBN_z + RFBN_x$	Gini Index	82.3%
Classification Regression Tree	$SF_y + RFBW_y + RFBN_y + STF_x + SF_x + SF_z + RFBW_z + RFBW_x + RFBN_x + RFBN_z$	Dichotomic Division	96.5%

There is a big difference between mobile phones equipped with different chips with only one feature of the resonance frequency. For example, the X-axis resonance frequency range of the ICM20690 chip is about 26640Hz-27540Hz, the ICM4 × 6XX chip is 25840Hz-28010Hz, and the LSM6DSM series chip is 20000Hz-20990Hz. The three types of chips can be distinguished by only one feature.

However, only one feature cannot complete fingerprint recognition for mobile phones equipped with the same chip. In particular, Huawei Mate 30, Mi 8, Huawei P10, and Huawei Mate 30 Pro equipped with the ICM20690 chip have similar resonance bands. However, the classification results show that these four are still well distinguished. After our research, we found that Mi 8 was distinguished due to the 25% difference between the sampling rate and the other three mobile phones. The starting frequencies of the three axes of Huawei Mate 30 all exceed 27kHz. The Y-axis ultrasonic stimulation response of Huawei P10 is invalid. The resonance frequency range of the Huawei Mate 10 Pro is about 20% higher than that of the two mobile phones except Huawei Mate 30.

The classification results of these 15 mobile phones are obtained from Table 5. The accuracy rate of the classification model using the CHAID decision tree is 70%, and it only uses two features. Then, the two types of CRT classification and regression trees used 8 and 10 features, respectively, and the classification accuracy rates increased sequentially. We found that the more features the input model has, the higher the recognition rate. This also allows us to select 10 types of

features from the 19-dimensional features, which better affect the recognition model.

In the CHAID decision tree based on the chi-square test, the tree is divided into three layers, forming 16 leaf nodes. The classification judgments of the second and third layers are based on the Y-axis resonance bandwidth and the Y-axis cutoff frequency, respectively. Each feature has the most considerable chi-square value. The Y-axis resonance bandwidth is subdivided into 14 leaf nodes, which proves that the device fingerprint Y-axis resonance bandwidth contributes to the mobile phone classification problem. In the other two CRT classification regression trees, it can be seen that the final used features are the same 12. The decision tree model that uses Gain as the basis for discrimination has a lower final overall classification accuracy rate instead of using a simple dichotomy as the basis for bifurcation discrimination. The accuracy of the model differs by 14.2%. Both methods select the best binary segmentation in each branch. The simple dichotomy is close to 99% because it traverses all the binary classification methods based on training data and finally finds the highest accuracy of the binary classification method. It also proves that the features extracted in this paper and the device fingerprint identification method are feasible and can finally completely distinguish all mobile phone models.

C. FINGERPRINT ON ANDROID AND iOS

In the second experiment, in order to discuss the impact of the operating system on fingerprints. We collected 11 mobile phones produced in the last three years, of which six are Android phones, and five are iOS phones. Through

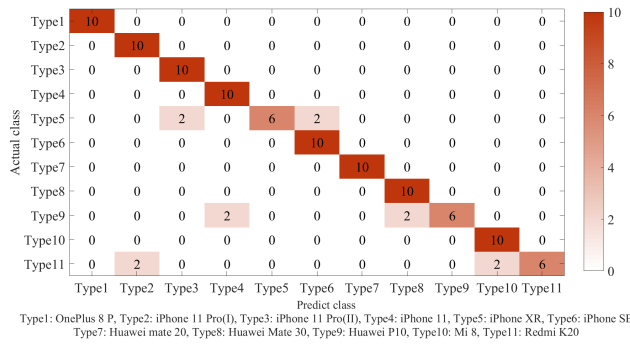


FIGURE 6. Classification confusion matrix. The X-axis is the actual value in the confusion matrix, and the Y-axis is the predicted classification. The darker the diagonal color represents, the higher the percentage of the correct result. In other areas, the darker the color, the higher the number of classification errors. As we can see from the figure, eight phones are classified correctly, and three of them have a 60% correct rate.

Experiment 1, we identified 10 features that are beneficial to improve the results of the experiment. In this experiment, we used them. From the extracted iOS devices, we found that the Z-axis resonance phenomenon of the device equipped with the BMI282AA chip does not exist or is particularly weak, which may be caused by the low Z-axis sensitivity during the chip's manufacturing process. The data is modeled and matched through a decision tree, and the classification accuracy is 90.2%. The generated confusion matrix is shown in Figure 6. iPhone XR was mistakenly divided into iPhone 12 pro twice, and the other two were mistakenly divided into iPhone se2. The reason is that their X-axis and Y-axis resonance frequency bands overlap more than 80%, and the Z-axis has no response. In the follow-up experiments, we added three features as X, Y, Z-axis peak ratio. There is no false distinction. The wrong distinction between Huawei P10 and Redmi K20 is also related to the overlap of the resonance frequency band by more than 50%. After the peak position feature is added, the accuracy rate has been greatly improved.

D. TIME-CONSISTENCY OF SENSOR FINGERPRINT

In the third experiment, to evaluate the impact of the sampling interval on the features, we selected 5 models of Android phones from four companies, namely OnePlus 8 pro, vivo X9, Redmi K20, Huawei Mate 10, and Huawei Mate 10 Pro. In a month, we randomly selected ten days, collected a set of data every day, extracted the features of the data, and produced Figure 7. It can be concluded from Figure 7 that the performance of the fingerprint feature at ten-time points is approximately a straight line, which shows that the feature is stable in the collection experiment at a longer time interval. Moreover, in Figure 7 (a), the gray line, the Red Mi K20 feature, has an abnormal peak. This may indicate that the time non-deformation feature is not universal. In order to solve this problem, we extracted the other three features to make a line graph. Abnormal peaks generally existed at time 4. Since mechanical vibrations will cause the output of the gyroscope to fluctuate, we checked the laboratory log. The log showed laboratory construction on the day at time 4,

and severe vibrations caused by electric drills would affect data collection and feature extraction. In summary, this feature is stable for long time intervals.

Then we conducted a short-term continuous measurement experiment. Using the same experimental environment as above, each mobile phone continuously measured complete data. It can be seen from Figure 8 that the performance of the fingerprint feature at ten-time points is approximately a straight line, which shows that the feature is still stable in the case of a short time interval. Moreover, the Redmi K20 feature is similar to a parallel line, which verifies our conjecture that external factors cause feature mutations. In summary, the fingerprint feature proposed in this paper has time stability.

E. ATTITUDE-CONSISTENCY OF SENSOR FINGERPRINT

The fourth experiment. We hope to explore the impact of equipment attitude on data collection. In the process of data collection, a series of time series data of gyroscope output is obtained, which is represented by X, Y, Z-axis angular velocity output based on its spatial coordinate system. When a gyroscope is used as a UAV and gait recognition, the attitude factor of equipment is a significant factor to be considered in the construction of the system. Because the gyro reference plane of the carrier changes with the user's behavior, it is necessary to analyze the relationship between the current coordinate system and the reference plane coordinate system when obtaining attitude data. In the two experimental environments designed in this paper, the location of the mobile phone is shown in the Figure 9, showing a 0-degree angle and 90-degree angle with the horizontal plane.

$$G_{X0} = G_{X90} \quad (9)$$

$$G_{Y0} = -G_{Z90} \quad (10)$$

$$G_{Z0} = G_{Y90} \quad (11)$$

The X, Y, and Z axis conversion form of the mobile phone constructed in the two placement states shown in Figure 9 from the reference coordinate system is obtained by formulas (9), (10), (11). Here we take the Huawei mate20 mobile phone as an example. Under the premise of ensuring that other environmental factors are precisely the same, we have collected the gyroscope output data of the same mobile phone in different postures. As shown in Figure 9 (c), the two data types are very similar, and the difference in features such as resonance frequency bands is within an acceptable range. Therefore, the placement posture of the two mobile phones will not change the resonance features. Therefore, there is no need to change the fixed device extraction algorithm with the placement angle when the device placement state changes.

VI. LIMITATION AND DISCUSSION

A. FREQUENCY DRIFT

As mentioned in Section III, the inertial sensors are vulnerable to acoustic signals. These out-of-band signals are injected at resonant frequencies and sampled by the analog-to-digital converter (ADC) with an insufficient sample rate. Therefore,

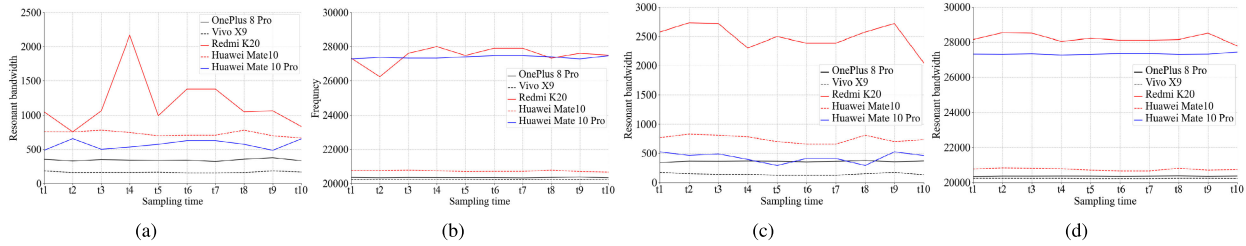


FIGURE 7. Features time invariance experiment. We randomly selected five mobile phones, namely OnePlus 8 Pro, vivo X9, Redmi K20, Huawei Mate10, Huawei Mate 10 Pro. Within a month, we randomly selected ten days and tested ten data sets on each mobile phone. We convert the data into frequency domain features and draw it into a line graph. (a) is X-axis resonance. (b) is X-axis vibration stop frequency. (c) is Y-axis resonance bandwidth. (d) is Y-axis vibration stop frequency.

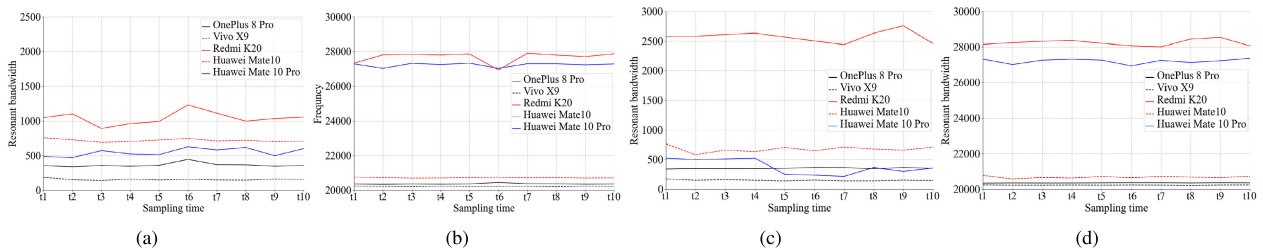


FIGURE 8. Features time invariance experiment. We randomly selected five mobile phones, namely OnePlus 8 Pro, vivo X9, Redmi K20, Huawei Mate10, Huawei Mate 10 Pro. We continuously tested ten sets of data on each mobile phone. We convert the data into frequency domain features and draw it into a line graph. (a) is X-axis resonance. (b) is X-axis vibration stop frequency. (c) is Y-axis resonance bandwidth. (d) is Y-axis vibration stop frequency.

TABLE 6. Gyro resonance range table at different temperatures.

We choose three temperatures to simulate the common temperature in spring, summer, and autumn. Under different temperature conditions, the difference in resonance range is small. It can be concluded that the difference in resonance frequency will not affect the effectiveness of this method.

Equipment Type	Temperature(°C)	X(kHz)	Y(kHz)	Z(kHz)
Huawei Mate 30	13.8	27.15-27.52	27.21-27.5	27.24-27.56
	25.7	27.21-27.55	27.17-27.57	27.19-27.55
	34.6	27.19-27.56	27.2-27.58	27.24-27.57
Huawei nova 7	13.8	23.38-23.62	23.39-23.66	23.43-23.77
	25.7	23.45-23.63	23.44-23.66	23.49-23.7
	34.6	23.45-23.68	23.45-23.67	23.43-23.76

slight frequency drift or sample rate jitter could be amplified and cause significant deviation in the digital output of the sensors [31]. Due to this drift, the frequency of the induced output is not a constant. Hence, we do not use the signal of sensors' output as our method's feature, which will not affect the recognition accuracy of our fingerprints.

In addition, as we use the resonance bandwidth and starting/stopping vibration frequency as the features in our method, the influence of the resonant frequency drift should be considered. However, the degree of this effect is very tiny since the MEMS gyroscope is located inside the phone case which the external environment has limited impact on them. Besides, the feature extraction of our method is to extract a range rather than an exact value. We take temperature as an example, as shown in Table 6, we can see the frequency drift with the temperature is slight and much more minor than the value range of our feature extraction.

B. ULTRASONIC TRANSDUCER

At present, some of the built-in speakers of mobile phones cannot reach the corresponding resonance frequency

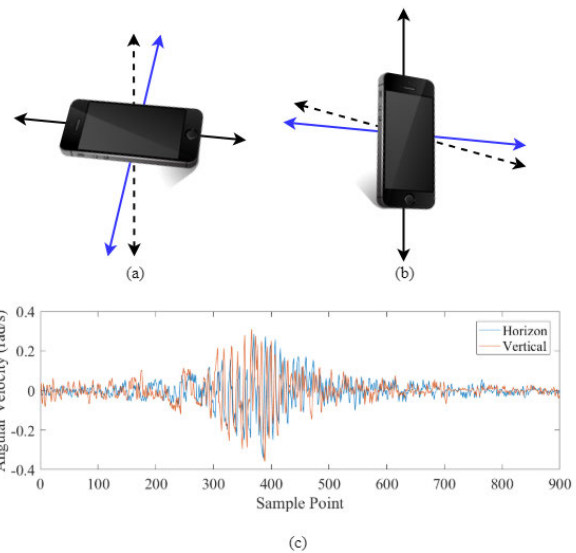


FIGURE 9. Characteristic attitude stability experiment. (a) and (b) show the self-reference coordinate system of the horizontal and vertical positions of the equipment. The blue line is the X-axis direction of the equipment, the solid black line is the Y-axis direction of the equipment, and the black dashed line is the Z-axis direction of the equipment. (c) shows the performance of the gyroscope data collected in the two postures in the exact figure.

of some types of gyroscopes, like higher than 20kHz. Therefore, transmission and conducting ultrasound higher than 20kHz is challenging, especially for the built-in speaker. Our solution will be limited in specific scenarios since whether the data collection in Figure 4 (c) can be succeed

depends on the frequency range of the built-in speaker. Nowadays, as the demand for high-fidelity audio increases, many speakers today can provide a wide frequency range higher than 25Hz, such as [45] and [46]. These speakers will provide more opportunities for our fingerprint method in the future.

C. PHONES' MOVEMENT

In reality, the mobile phone cannot remain stationary at all the time. Generally speaking, the amplitude of the motion signal is much bigger than the resonance signal. It is challenging to distinguish the signals generated by users' movements. However, the people's regular movements, such as jogging, running, or walking, can be modeled and predicted [22]. Hence, after modeling the user data, we can filter these periodic signals by the digital filter.

D. PERMISSION ISSUES

The operating system has different permissions for the browser to read the sensors. For example, some high versions of iOS are equipped with high permissions for the browser to get sensor data. By default, Apple removed motion sensor access permissions from mobile Safari and removed WebKit's motion sensor access permissions in later versions. Under the Android system, the browser can read sensor data without restrictions. However, some privacy-enhancing browsers (such as the Brave browser) are an exception, which blocks Android's access to the motion sensor. For iOS, the gyroscope as the target of the fingerprint is still the least restrictive among many solutions, and the App can still directly get the gyroscope data without any notifications. For Android, the usage of privacy-enhancing browsers is still a tiny number, and it is not difficult to obtain gyroscope data from standard Apps or webs.

VII. CONCLUSION

In this paper, we introduced a new type of fingerprint method for the mobile device using gyroscope resonance. Based on the finding that there is a clear difference in the responses to specific physical stimuli between sensors, we utilise ultrasonic as the trigger signal and calculate the different reactions as the fingerprint information between the mobile devices. After a series of experiments, the results demonstrate that our method can effectively distinguish mobile devices clearly and stably.

Nowadays, sensors are deeply integrated into our lives. As one of the essential user interfaces, inertial sensors will be used more and more commonly. In future work, it would be interesting to flesh out how to filter the phones' movement. Furthermore, it could also focus on other devices that contain gyroscopes.

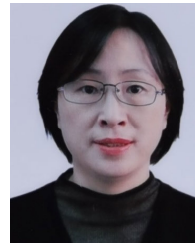
REFERENCES

- [1] G. Baldini and G. Steri, "A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1761–1789, 3rd Quart., 2017.
- [2] K. Mowery, "Pixel perfect: Fingerprinting canvas in HTML5," in *Proc. W2SP*, 2013, pp. 1–2.
- [3] J. C. Sipior, B. T. Ward, and R. A. Mendoza, "Online privacy concerns associated with cookies, flash cookies, and web beacons," *J. Internet Commerce*, vol. 10, no. 1, pp. 1–16, Mar. 2011.
- [4] *Xposed Module Repository*. Accessed: Aug. 2, 2021. [Online]. Available: <https://repo.xposed.info/>
- [5] Q. Zheng and Z. Gao, "Disturbance rejection in MEMS gyroscope: Problems and solutions," in *Proc. 30th Chin. Control Conf.*, 2011, pp. 6334–6339.
- [6] D. Freire-Obrigón, F. Narducci, S. Barra, and M. Castrillón-Santana, "Deep learning for source camera identification on mobile devices," *Pattern Recognit. Lett.*, vol. 126, pp. 86–91, Sep. 2019.
- [7] S. Castro, R. Dean, G. Roth, G. T. Flowers, and B. Grantham, "Influence of acoustic noise on the dynamic performance of MEMS gyroscopes," in *Proc. ASME Int. Mech. Eng. Congr. Expo.*, 2007, pp. 1825–1831.
- [8] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, "A study of Android application security," in *Proc. USENIX Assoc.*, 2011, pp. 1–4.
- [9] R. N. Dean, G. T. Flowers, A. S. Hodel, G. Roth, S. Castro, R. Zhou, A. Moreira, A. Ahmed, R. Rifki, B. E. Grantham, D. Bittle, and J. Brunsch, "On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise," in *Proc. IEEE Int. Symp. Ind. Electron.*, Jun. 2007, pp. 1435–1440.
- [10] W. N. Yunker, P. Soobramaney, M. Black, R. N. Dean, G. T. Flowers, and A. Ahmed, "The underwater effects of high power, high frequency acoustic noise on MEMS gyroscopes," in *Proc. 23rd Biennial Conf. Mech. Vibrat. Noise*, Jan. 2011, pp. 1–14.
- [11] T. Hupperich, H. Hosseini, and T. Holz, "Leveraging sensor fingerprinting for mobile device authentication," in *Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment*, 2016, pp. 377–396.
- [12] G. Baldini, G. Steri, F. Dimc, R. Giuliani, and R. Kamnik, "Experimental identification of smartphones using fingerprints of built-in micro-electro mechanical systems (MEMS)," *Sensors*, vol. 16, no. 6, p. 818, Jun. 2016.
- [13] I. Amerini, R. Becarelli, R. Caldelli, A. Melani, and M. Niccolai, "Smartphone fingerprinting combining features of on-board sensors," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2457–2466, Oct. 2017.
- [14] T. V. Goethem, W. Scheepers, D. Preuveneers, and W. Joosen, *Accelerometer-Based Device Fingerprinting for Multi-Factor Mobile Authentication*. Cham, Switzerland: Springer, 2016.
- [15] X.-Y. Li, H. Liu, L. Zhang, Z. Wu, Y. Xie, G. Chen, C. Wan, and Z. Liang, "Finding the stars in the fireworks: Deep understanding of motion sensor fingerprint," *IEEE/ACM Trans. Netw.*, vol. 27, no. 5, pp. 1945–1958, Oct. 2019.
- [16] J. Zhang, A. R. Beresford, and I. Sheret, "Factory calibration fingerprinting of sensors," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1626–1639, 2021.
- [17] G. Baldini, G. Steri, R. Giuliani, and V. Kyovtorov, "Mobile phone identification through the built-in magnetometers," 2017, *arXiv:1701.07676*.
- [18] M. Cristea and B. Groza, "Fingerprinting smartphones remotely via ICMP timestamps," *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1081–1083, Jun. 2013.
- [19] A. E. Dirik, H. T. Sencar, and N. Memon, "Digital single lens reflex camera identification from traces of sensor dust," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 539–552, Sep. 2008.
- [20] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Source camera identification using footprints from lens aberration," in *Digital Photography*, vol. 6069, N. Sampat, J. M. DiCarlo, and R. A. Martin, Eds. Bellingham, WA, USA: SPIE, 2006, pp. 172–179.
- [21] L. Zou, Q. He, and X. Feng, "Cell phone verification from speech recordings using sparse representation," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2015, pp. 1787–1791.
- [22] S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi, "AccelPrint: Imperfections of accelerometers make smartphones trackable," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2014, pp. 1–4.
- [23] Z. Ba, T. Zheng, X. Zhang, Z. Qin, B. Li, X. Liu, and K. Ren, "Learning-based practical smartphone eavesdropping with built-in accelerometer," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2020, pp. 1–18.
- [24] A. Primo, V. V. Phoha, R. Kumar, and A. Serwadda, "Context-aware active authentication using smartphone accelerometer measurements," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2014, pp. 98–105.
- [25] H. Bojinov, Y. Michalevsky, G. Nakibly, and D. Boneh, "Mobile device identification via sensor fingerprinting," 2014, *arXiv:1408.1416*.
- [26] A. Das, N. Borisov, and M. Caesar, "Tracking mobile web users through motion sensors: Attacks and defenses," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2016, pp. 1–15.

- [27] A. Das, G. Acar, N. Borisov, and A. Pradeep, "The web's sixth sense: A study of scripts accessing smartphone sensors," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2018, pp. 1515–1532.
- [28] A. Faizkhademi, M. Zulkernine, and K. Woldemariam, *FPGUARD: Detection and Prevention of Browser Fingerprinting*. Springer, 2015.
- [29] A. Das, N. Borisov, and E. Chou, "Every move you make: Exploring practical issues in smartphone motion sensor fingerprinting and countermeasures," *Proc. Privacy Enhancing Technol.*, vol. 2018, no. 1, pp. 88–108, Jan. 2018.
- [30] V. K. Khanna, "Remote fingerprinting of mobile phones," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 106–113, Dec. 2015.
- [31] Y. Tu, Z. Lin, I. Lee, and X. Hei, "Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors," in *Proc. Secur. Symp.*, 2018, pp. 1545–1562.
- [32] I. Giechaskiel and K. Rasmussen, "Taxonomy and challenges of Out-of-Band signal injection attacks and defenses," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 645–670, 1st Quart., 2020.
- [33] D. Arp, E. Quiring, C. Wressnegger, and K. Rieck, "Privacy threats through ultrasonic side channels on mobile devices," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2017, pp. 35–47.
- [34] Y. Michalevsky, D. Boneh, and G. Nakibly, "GyroPhone: Recognizing speech from gyroscope signals," in *Proc. 23rd USENIX Secur. Symp.*, 2014, pp. 1053–1067.
- [35] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," in *Proc. USENIX Assoc.*, 2015, pp. 881–896.
- [36] S. Khazaaleh, G. Korres, M. Eid, M. Rasras, and M. F. Daqaq, "Vulnerability of MEMS gyroscopes to targeted acoustic attacks," *IEEE Access*, vol. 7, pp. 89534–89543, 2019.
- [37] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2017, pp. 3–18.
- [38] R. N. Dean, S. T. Castro, G. T. Flowers, G. Roth, A. Ahmed, A. S. Hodel, B. E. Grantham, D. A. Bittle, and J. P. Brunsh, "A characterization of the performance of a MEMS gyroscope in acoustically harsh environments," *IEEE Trans. Ind. Electron.*, vol. 58, no. 7, pp. 2591–2596, Jul. 2011.
- [39] P. Soobramaney, "Mitigation of the effects of high levels of high-frequency noise on MEMS gyroscopes," Ph.D. dissertation, Auburn Univ., Auburn, AL, USA, 2013.
- [40] *Codepen*. Accessed: Jun. 2, 2021. [Online]. Available: <https://codepen.io/accounts/signup/user/free/>
- [41] *Audionode*. Accessed: Jun. 6, 2021. [Online]. Available: <https://developer.mozilla.org/en-US/docs/Web/API/AudioNode/>
- [42] G. Ritschard, *CHAID and Earlier Supervised Tree Methods*. Routledge, 2013.
- [43] J. Ouyang, N. Patel, and I. K. Sethi, "Chi-square test based decision trees induction in distributed environment," in *Proc. IEEE Int. Conf. Data Mining Workshops*, Dec. 2008, pp. 477–485.
- [44] G. Wang and J. Xu, "A decision tree algorithm based on coordination degree and gini-coefficient," in *Proc. Int. Conf. MultiMedia Inf. Technol.*, Dec. 2008, pp. 822–824.
- [45] *Pioneer Multimedia Se-MJ721-BRWH Design Headphones Brown*. Accessed: Aug. 30, 2021. [Online]. Available: <https://www.bax-shop.co.U.K/headphones/pioneer-multimedia-se-mj721-brwh-design-headphones-brown>
- [46] *Car Audio Speaker Tweeter*. Accessed: Oct. 5, 2021. [Online]. Available: <https://www.amazon.com/gp/product/B002UL7ZKA>



JIANYI ZHANG received the Ph.D. degree in computer security from the Beijing University of Posts and Telecommunications (BUPT). From 2009 to 2012, he was a Security Researcher with Huawei Digital Technologies, Beijing, China. Since 2012, he has been with the Faculty of Computer Science, Beijing Electronics Science and Technology Institute (BESTI). His research interests include internet security, data security, and privacy.



XIUYING LI was born in China, in 1975. She received the master's degree from Beijing Jiaotong University, in 2005. She is currently an Associate Professor with Beijing Electronic Science and Technology Institute. Her main research interest includes embedded system security.



CHANGCHUN ZHOU was born in China, in 1963. He is currently a Professor with Beijing Electronic Science and Technology Institute.



RUILONG WU is currently pursuing the master's degree in cyberspace security with Beijing Electronic Science and Technology Institute. His main research interests include sensor security and embedded systems.



YUCHEN WANG was born in China, in 1997. He received the bachelor's degree in communication engineering from Beijing Jiaotong University. He is currently pursuing the master's degree with Beijing Electronic Science and Technology Institute. His research interests include embedded systems and hardware security.



SHENGYUAN HUANG was born in China, in 1996. He is currently pursuing the master's degree with Beijing Electronic Science and Technology Institute. His research interests include the Internet of Things security and privacy protection.

...



JUNZE TIAN was born in China, in 1997. He received the bachelor's degree in communication engineering from Xiangtan University. He is currently pursuing the master's degree with Beijing Electronic Science and Technology Institute. His main research interests include the Internet of Things in safety and privacy protection.