Wang, Xuerui; Yan, Zheng; Zhang, Rui; Zhang, Peng

Attacks and defenses in user authentication systems: A survey

Published in:
Journal of Network and Computer Applications

DOI:
10.1016/j.jnca.2021.103080

Published: 15/08/2021

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Attacks and Defenses in User Authentication Systems: A Survey

Xuerui Wang[a], Zheng Yan[a,b,*], Rui Zhang[a] and Peng Zhang[c]

[a]The State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an 710071, China
[b]The Department of Communications and Networking, Aalto University, Espoo 02150, Finland
[c]Zalando, Finland

ARTICLE INFO

Keywords:
Authentication System
Attack Detection
Defense Mechanisms
Spoofing Attack
Liveness Detection
CAPTCHA
Biometric Authentication
Machine Learning
Deep Neural Networks

ABSTRACT

User authentication systems (in short authentication systems) have wide utilization in our daily life. Unfortunately, existing authentication systems are prone to various attacks while both system security and usability are expected to be satisfied. But the current research still lacks a thorough survey on various types of attacks and corresponding countermeasures regarding user authentication, including traditional password-based and emerging biometric-based systems. In this paper, we make a comprehensive review on attacks and defenses of the authentication systems. We firstly introduce a number of common attacks by classifying them into different categories based on attacker knowledge, attack target, attack form and attack strength. Then, we propose a set of evaluation criteria for evaluating different kinds of attack defense mechanisms. Furthermore, we review and evaluate the existing methods of detecting and resisting attacks in the authentication systems by employing the proposed evaluation criteria as a common measure. Specifically, we focus on comparing and analyzing the performance of different defense mechanisms in different types of authentication systems. Through serious review and analysis, we put forward a number of open issues and propose some promising future research directions, hoping to inspire further research in this field.

1. Introduction

In past decades, user authentication systems (in short authentication systems) have been widely used in our daily life to effectively block illegal access to services and sensitive data. Since the most primitive text-password authentication system is less secure and vulnerable to a variety of attacks [90], many biometric-based authentication systems have been used in many fields. Biometric-based authentication has improved performance on security and usability compared to traditional password-based authentication. However, the existing biometric systems need further improvement because new types of attacks appear quickly aiming at invade new systems of user authentication. Therefore, understanding these attacks and getting a holistic view on existing defense mechanisms become essentially important for developing an effective authentication system.

On the other hand, user requirements are much higher than before with the fast growth of the Internet and mobile applications. Users expect convenient and usable authentication while system security can be well ensured. However, high security usually means low usability. For example, complex passwords can reduce the risk of password guessing, but increase the difficulty of memory at the same time. This problem is getting worse when the users need to use different passwords for different services' access. Therefore, security and usability should be balanced. Motivated by this, many new authentication systems appeared. Unfortunately, existing systems are far from satisfactory. There are various new types of attacks on modern authentication systems and mobile services. It is necessary to overview existing attacks and their countermeasures, summarize recent advances, and discover open issues in order to drive further development in this field.

We notice that there are a number of surveys about authentication systems in the literature. But most existing surveys [129, 127, 22, 20, 6] only focus on a single type of authentication system. They lack comprehensive classification and comparative analysis on attacks and defenses in different types of authentication systems. For example, Meng et al. [129] focused on biometric user authentication in mobile phones. In [127, 22], authors reviewed fingerprint recognition systems. In [20], Blasco et al. provided a review on wearable biometric recognition systems. Alomar et al. [6] surveyed social authentication applications. They classified social authentication applications into knowledge-based social authentication and trust-based social authentication and evaluated them in terms of usability, security and deployementability. In [211], Zhang and Yan gave a thorough survey on biometric authentication, focusing on secure and privacy-preserving identification. In [175], Singh et al. gave a review on existing attacks in biometric systems and summarized liveness detection methods for fingerprint recognition and iris recognition. Based on our investigation, we saw a need of a comprehensive survey on attacks and defenses in authentication systems in order to give a thorough view on the current state and advance of user authentication.

In this paper, we provide a detailed overview on user authentication systems, mainly focusing on attacks and their countermeasures. We firstly introduce common attacks on authentication systems by classifying them into different categories based on attacker knowledge, attack scope, attack form and attack strength. Then, we propose a set of evaluation criteria in order to evaluate different kinds of attack defense mechanisms. Furthermore, we review and evaluate the

*Corresponding author
wangxueruimay@163.com (X. Wang); zyan@xidian.edu.cn (Z. Yan); cumt_zhangrui@126.com (R. Zhang); rishi@stmdocs.in (P. Zhang)
ORCID(s): 0000-0001-7511-2910 (Z. Yan)

existing methods of detecting and resisting attacks in authentication systems by employing the proposed evaluation criteria. Specifically, we focus on comparing and analyzing the performance of different defense mechanisms against attacks in different authentication systems. Through serious review and analysis, we put forward a number of open issues and propose some promising future research topics. The contributions of our paper can be summarized as below:

- We analyze the security vulnerabilities existing in two types of authentication systems: traditional password-based systems and biometric-based systems.
- We put forward a set of evaluation criteria for evaluating attack defense mechanisms in authentication systems.
- We review existing defense mechanisms against different types of attacks, and then we compare and analyze the advantages and disadvantages of the state-of-art defense mechanisms based on the proposed evaluation criteria.
- We particularly investigate novel attacks that are constructed by machine learning and deep learning. We review corresponding countermeasures based on deep learning technologies that were proposed in recent years.
- We propose some open issues and future research directions in this field to motivate future research efforts.

The structure of the remainder of the paper is as follows. Section II gives a brief review on existing attacks in authentication systems. Section III proposes a series of criteria for the purpose of evaluating different kinds of defense mechanisms. Section IV presents a comprehensive review on existing defense methods corresponding to different attacks, followed by comparison and analysis on the performance of different defense mechanisms in Section V. Some open issues and future research directions are pointed out in Section VI. Finally, and we provide our conclusion in the last section.

2. Attacks in Authentication Systems

In this section, we first introduce two main traditional user authentication systems: password-based and biometric-based. Then, we illustrate different types of attacks on them.

2.1. Authentication Systems

2.1.1. Password-based Systems

Text-based Password Systems Traditional text-based systems use a simple combination of alphanumeric and keyboard characters as passwords. Users only need to set a string of character combinations as their passwords. Text-based systems are familiar for users but they are vulnerable to such attacks as brute-force attack, shoulder-surfing attack and social engineering.

Graph-based Password Systems In practice, most users tend to set simple passwords that are easy to remember, which, however, makes them easy to guess. To solve this problem, graphical passwords become popular. Suo et al. gave a comprehensive review on existing graphical password systems [180]. There are many graphical passwords to enhance both security and usability. In general, there are three categories: recognition-based, recall-based and cued-recall.

In [180], Suo et al. listed some graphical password methods and summarized their advantages and disadvantages. The advantages include: 1) high usability because pictures are more memorable than texts; 2) a larger password space. So graphical passwords have better performance against dictionary attack than text-based passwords. However, the disadvantages are: 1) the registration and authentication in graph-based systems take a relatively longer time than text-based systems; 2) storing images usually requires a large storage space.

Token-based Password Systems Token-based systems improve authentication security, but require users to carry extra devices, which is inconvenient. In addition, according to [17], both graph-based and token-based systems take users more time to finish authentication, compared with the text-based password systems.

2.1.2. Biometric-based Systems

Nowadays, biometric authentication is often used in daily life. Physiological characteristics and behavioral characteristics are two forms of biological characteristics. Physiological characteristics include immutable features such as fingerprint, palm print, face, and DNA. Behavioral characteristics include voice, signature, walking posture, keystroke, etc. Table 1 lists the specific attributes of different biological characteristics, which are used for authentication.

In recent years, face recognition has been widely used in mobile devices. Researchers are still working to further improve its performance. As far as we know, a common method is to construct facial recognition based on deep neural networks [157], and its recognition accuracy can reach more than 98%. The principle of iris recognition is similar to face recognition, which realizes identity recognition based on iris images [15]. Its authentication accuracy can reach up to 97%. Although iris recognition is more secure than face recognition, it is not as widely used as face recognition because of its special requirement on data acquisition equipment. On the contrary, fingerprint recognition has been widely used even earlier than face recognition. It performs very well regarding accuracy, which can reach 99.2% [171]. Some other methods based on the characteristics of hand pattern were derived from fingerprint recognition, such as palmprint [89], and finger recognition [191], and their recognition accuracy can reach 98% and 96%, respectively."

With the development of intelligent systems and voice interaction, voiceprint based authentication has become popular. The recognition accuracy of voiceprint systems based on deep learning is more than 99% [21]. However, due to the open transmission of sound, the vulnerability of voiceprint system in face of adversarial attacks becomes obvious. In addition, identity verification can be implemented based on

Table 1
Specific Attributes of Different Biological Characteristics

Characteristics		Specific attributes
Physiological characteristics	Face [157]	The position of the five features of the face, facial expression
	Iris [15]	The size and image of iris
	Fingerprint [171]	Minutiae points: terminations and bifurcations of the ridge lines
	Palm print [89, 191]	Principal lines Wrinkles minutiae Delta point
Behavioral characteristics	Keystroke [21]	Duration for each letter typed Latency between keystrokes
	Signature [7]	Pen-down time Forward and backward time Pressure
	Voice [58]	Volume and Pitch

behavior features, such as keystrokes and signatures, which can also achieve relatively high accuracy [7, 58]. However, due to the need of additional device support, it has few applications on mobile devices.

2.1.3. Distributed Systems

With the development of Internet of Things and intelligent facilities, an authentication system is no longer limited to a client/server (C/S) structure widely used before. Distributed authentication becomes a new requirement. Researchers usually use blockchain, group signature, edge computing and other technologies to achieve it. Lin et al. designed a mutual authentication system based on blockchain, group signature and message verification code, which can be used in smart home scenarios [121]. Guo et al. designed a distributed trusted authentication system based on blockchain and edge computing [75]. It realizes activity tracking and offers trusted authentication. Its communication and computation costs are less than existing methods. It outperforms existing edge computing strategies by 8%-14% in hit ratio. In addition, Feng et al. noticed such a distributed authentication requirement in vehicular ad hoc networks (VANETs) and proposed a blockchain-assisted privacy-preserving authentication system (BPAS) [53] .

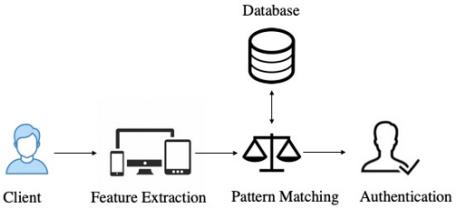

Figure 1: A generic biometric-based authentication system architecture.

2.2. Attacks in Authentication Systems

The attacks on the authentication systems can be classified based on four characteristics: attacker's knowledge, attack scope, attack form and attack strength.

Attacker's Knowledge Attacker's knowledge involves the attacker's understanding of a target system and a target user. It includes the structure of the system, the user's password dictionary, and biological characteristics in biometric-based systems, etc.

Table 2
Summary of Existing Attacks on Authentication Systems

Attacks	Knowledge	Target	Form	Strength
Brute force attack	Little	Password	-	Medium
Guess attack	Medium	Password	-	Medium
Shoulder-surfing	Medium	Password	-	Medium
Phishing Attack	Little	Password	-	Strong
Artificial Synthesis	More	Biometric	Direct	Medium
Replay Attack	Medium	Biometric	Indirect	Medium
Adversarial attack	More	Biometric	Indirect	Weak
Poisoning attack	More	Biometric	Indirect	Weak

Attack Target Attack target refers to the target of an attack. Obviously, an attack cannot attack all systems in the world, it can only work on a specific target or a kind of systems. Whether a system could be broken depends on the algorithm, architecture and even the physical devices used in the system.

Attack Form In biometric-based systems, direct attacks and indirect attacks are two categories of spoofing attacks [159]. The direct attacks usually occur in physical layer. A common form is to synthesize fake biometrics to cheat a target system [43]. However, the indirect attacks usually take place in transmission layer or application layer to obtain information indirectly. The targets of this kind of attacks are feature extractors and comparators, or communications channels.

Attack Strength Different kinds of attacks have different attack intensity. We divided them into strong attacks and weak attacks according to attack strength. Strong attacks mean that it is difficult to defend such attacks and their defense mechanisms are complex.

Based on the above aspects, we illustrate a number of typical existing attacks in authentication systems as follows. We also summary their classification characteristics in Table 2.

2.2.1. Brute Force Attack

Traditional password-based systems are vulnerable to brute force attack. Brute force and dictionary attacks are common attacks against password-based authentication systems. The brute force attack is such an attack that attackers need to enter all possible passwords (words or phrases) in a user-defined dictionary. There are two types of brute force attacks. The first one is that an attacker tries every combination of passwords based on the password space for specific user accounts. Another attack method tries to find a user who uses the password chosen by an attacker. This kind of attack exploits the vulnerability that most users often set up simple and easy to remember passwords.

2.2.2. Guess Attack

A guess attack can identify a user's password more efficiently than the brute force attack, because passwords depend on users' preferences, knowledge and experiences. The success rate of a guess attack depends on the attacker's knowl-

edge of the target user. It is easier for the attacker to guess the user's password when they have a lot of knowledge about the user. Specially, dictionary attacks [136] belong to guess attacks. Attackers try to attack the possible password (word or phrase) in the user-defined dictionary one by one. The difference between brute force attacks and dictionary attacks is that the former need to try all possible combination passwords, while the latter will use a pre-defined word list. In other words, guess attacks reduce the number of password attempts.

2.2.3. Shoulder-surfing Attack

Shoulder surfing is actually common in our daily lives. When we are inputting personal information into our computers or mobile phones, other people can easily observe our actions over our shoulders. Shoulder-surfing attack is easy to implement, and it almost costs nothing for intruders. This kind of attack can be divided into two types [114]. One is looking over a person's shoulder directly, and the other one is recording the process of entering passwords using a hidden camera.

2.2.4. Phishing Attack

Phishing induces users to visit fake websites by flooding them with fake emails. In this way, attackers can obtain sensitive information of users, such as user names, passwords, PIN codes or credit card information.

2.2.5. Spoofing Attack

Two main categories of spoofing attack are artificial synthesis and replay attack.

Artificial Synthesis Artificial synthesis can be regarded as direct attacks [2], these methods make use of original biometrics to create an artificial version. It is not difficult to imitate physiological features. Fingerprints left on doorknobs, personal photos posted on social media, and images from cameras in public places are all easily accessible to attackers. Attackers can use mature techniques such as facemasks and rubber fingerprint models to fake users' biological features.

Replay Attack In contrast to artificial synthesis, replay attack is one kind of indirect attacks, which take advantage of some ways to get original biometrics indirectly. An attacker tries to use a sample collected from a legal user to spoof the target system. For example, the adversary may record users' voice secretly or take photos posted by users from social media. In this way, the adversary resubmits these data to gain access control of the system. Figure 2.2.5 shows an overview of replay attacks in biometric-based authentication systems.

Articles [160, 101] gave an overview of the vulnerable points of existing biometric-based systems. The attacking points in an authentication system are shown in Figure 2.2.5 and listed below: artificial synthesis at point 1; replay attack at point 2; channel attack between databases and the pattern-matching module at point 3; tampering databases at point 4; modifying decision at point 5.

Artificial synthesis attacks usually take place at client side. At point 1 shown in Figure 2.2.5, attackers usually

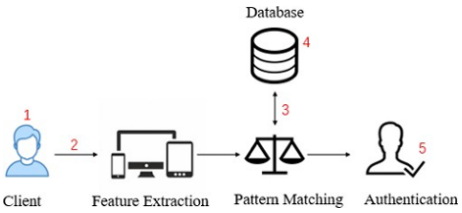

Figure 2: Possible attack points in a biometric-based authentication system.

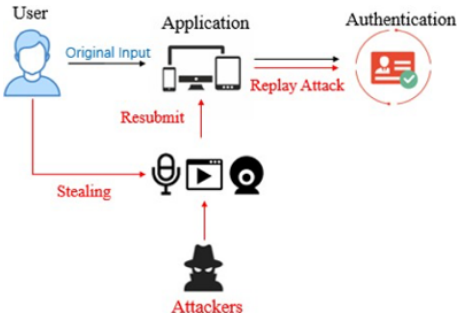

Figure 3: Replay attack in biometric-based authentication systems.

adopt fake fingerprints, face masks, and duplicate signatures [56] to cheat the system.

Replay attack usually occurs at the point 2 in Figure 2.2.5. Illegal users directly steal the information of legitimate users and resubmit it to the authentication system in order to obtain legal authority, e.g., a photo of a legal user or recorded his real audio [137, 196]. Attacks also occur between pattern matching modules and databases, as shown at point 3. An attacker who owns or steals administrator privileges can directly modify template data stored in the database and a final decision result at point 4 and point 5, respectively. Fortunately, for this kind of attacks, researchers have proposed many detection schemes to defend. The detection based on high frequency data proposed by Witkowski et al. [196] can directly screen out the input data with problems, reducing the error rate by 70%. The detection based on Deep Neural Network (DNN) proposed by Nagarsheth et al. [137] can distinguish different channels and achieve the purpose of distinguishing true and false audio.

Wolf Attack A Wolf attack is a kind of spoofing attacks. Wolf attacks use biometric samples that are similar to registered human templates and try to match these templates. Une et al. proposed a wolf attack and its probability in 2008 [189]. Wolf Attack Probability (WAP) is a novel measure to evaluate the security of biometric-based authentication systems. They found that the success probability of the wolf attack is larger than that of the brute force attack. In [189], one universal wolf in fingerprint pattern matching was found. This sample can match many fingerprint templates by mistake. In [144], Otsuka et al. made a synthesized wolf that gives a falsely accepted probability of 42.4% against a fingerprint authentication algorithm. Otsuka et al. proposed a wolf attack aimed at speaker verification systems. They

concluded that vulnerabilities in matching algorithms could cause most wolf attacks. In this paper, Otsuka et al. used a wolf for each gender to evaluate WAP of the speaker verification system proposed in [190]. The result shows that this wolf attack can achieve the WAP of 0.92, which means that it brings a big threat to the target system. In all, it is important to take an efficient method to resist wolf attacks on speaker verification in the future. In real authentication systems, liveness detection technologies can resist wolf attacks.

Spoofing attacks require attackers to be able to obtain biometric information about targeted users by specific means, while Online Social Network Facial Disclosure (OSNFD) are caused by users sharing personal photos in social networks. Liveness detection technologies can effectively defend such attack. By conducting a user study, Yan et al. classified three factors including security settings, target platforms, and user behaviors to evaluate the effectiveness of OSNFD attacks [119].

2.3. Attacks on Machine & Deep Learning

With the rapid development of machine learning technologies, deep learning and other related techniques, people are looking forward to a more intelligent authentication system than existing systems. Machine learning is a weapon to find security problems and has been applied into the field of vulnerability mining. At the same time, research on attacking machine learning models is on-going. Adversarial attacks make the difference between data and its original so subtle that the human cannot recognized by sensing. However, machine learning models may make a different classification decision for the two samples that look the same to humans.

Deep learning has made great outstanding achievements in the field of image recognition, speech synthesis and speech recognition. By using machine learning and deep learning, the ability of authentication systems to resist various kinds of attacks is greatly improved. However, researchers point out that deep neural networks still have the possibility of being attacked [205].

Different from the above attacks, attacks on machine & deep learning are a special type of attacks by making the machine & deep learning algorithms used in user authentication ineffective, which is being paid high attention in recent years. The target of this type of attacks is to interfere user authentication and make it produce wrong classification results. The attacker uses an optimization algorithm to construct adversarial noises carefully and adds them into normal data to achieve the goal of interfering classification with regard to user recognition.

Adversarial Attack Adversarial attacks can lead to final classification error of a deep learning model by adding a small change or perturbation in its input. Akhtar et al. reviewed the existing works about adversarial attacks in Computer Vision and proposed defenses against them [4]. Currently, the defense methods against the adversarial attacks are still under study. We will review the existing work for defending adversarial attacks in Section IV.

In the last decade, the development of deep neural networks let us perform many computational tasks, e.g., classic natural language understanding [125] and speech recognition tasks [30]. But the discovery of adversarial examples can fool well-trained neural networks. We call this problem as adversarial attacks. This attack has many applications and implications in identity recognition, autonomous driving, cyber security, etc. Some common terms about adversarial attacks are described below.

Adversarial example—A modified version of a clean image that is intentionally perturbed (e.g. by adding noises) to confuse or fool a deep neural network.

Adversarial perturbation—The noise that is added to the clean image to make it an adversarial example.

Adversarial training—Adversarial training uses both adversarial examples and the clean data to train machine learning models.

Black-box/White-box attacks—The attacker knows nothing about the internal structure of the attack model, training parameters, and defense methods. White-box attacks are in contrast to black-box attacks. Attackers can master the complete knowledge of the model. At present, most attack algorithms are white-box attacks.

Target/non-target attacks——Target attacks require model predicting a specific label. On the contrary, non-targeted attacks only cause a model to make a wrong judgment, rather than a specific result label. In terms of difficulty, it is more difficult to achieve target attacks than non-target attacks.

One-step methods——One-step methods perform one single step computation to generate adversarial examples.

Iterative methods—Iterative methods perform multiple times of computation. These kinds of methods usually cost more than the one-step methods.

In [4], Akhtar et al. introduced many forms of adversarial attacks on deep learning, such as one-pixel attack [178], Fast Gradient Sign Method (FGSM) [204], universal perturbations [134], and so on. In [205], Yuan et al. reviewed existing works on adversarial examples against deep neural networks. They reviewed adversarial examples on different applications, such as reinforcement learning [86, 109], face recognition [169], object detection [198], semantic segmentation [59, 80] and Natural Language Processing (NLP) [166, 118] .

Poisoning Attack Training data is a basic component of machine learning. Therefore, adding malicious data to the input data is one of frequently-used means for attackers to invade a machine learning system [177]. An attack that affects the accuracy of the model by injecting false training data into the deep neural networks is a kind of poisoning attack. In the poisoning attacks, attackers input modified data during the training stage. On the contrary, the adversarial attack means that attackers enter a modified example to cause the system to make a wrong classification decision.

There are two ways to achieve poisoning attacks: targeted attacks and non-targeted attacks. The goal of targeted attacks is to let the model output wrong labels chosen by adversaries previously. Non-targeted attacks only require mis-

Table 3
Summary of Adversarial Examples

Attacks	Target/ Non-target	Black/ White–box Attack	Attack Frequency	Attack Intensity
L-BFGS [4]	Target	White	Iterative	+++
FGSM [204]	Target	White	One-shot	+++
BIM and ILLC [113]	Non-target	White	Iterative	++++
JSMA [148]	Target	White	Iterative	+++
Deep Fool [135]	Non-target	White	Iterative	++++
CPPN EA Fool [138]	Target	White	Iterative	-
ATNs [13]	Target	White	Iterative	-
C&W Attacks [195]	Target	White	Iterative	+++++
Universal perturbations [134]	Non-target	White	Iterative	+++++
Feature Adversary [79]	Target	White	Iterative	-
Hot/Cold [194]	Target	White	One-shot	-
Model-based Resembling Attack[123]	Target/ Non-target	White	Iterative	-
Ground-Truth Attack [28]	Target	White	Iterative	-
One-pixel [179]	Non-target	Black	Iterative	++
Zero Order Optimization [203]	Target/ Non-target	Black	Iterative	-
Natural GAN [214]	Non-target	Black	Iterative	+++++
UPSET [44]	Target	Black	Iterative	++++
ANGRI [44]	Target	Black	Iterative	++++
Houdini [183]	Target	Black	Iterative	++++

+: The more symbols, the stronger the attack.
-: No evaluation on intensity.

leading neural networks to get wrong classification results. In Table 3, we summarize some adversarial examples and indicate attack types and their intensity.

3. Evaluation Criteria

In this section, we set up a list of criteria for comparing and analyzing the performance of different defense mechanisms against attacks in different authentication systems. A good defense mechanism should not only be able to successfully resist different kinds of attacks, but also ensure that it does not affect authentication efficiency and usability. Therefore, we mainly discuss from the following aspects: accuracy, efficiency, usability, security, privacy, user preferences, and cost/difficulty of defense. We divide these criteria into three categories: robustness, usability and reliability. For each criterion, we set three levels (high, medium and low) to judge performance level. The specific definitions are shown in Table 4.

3.1. Robustness (RO)

3.1.1. Accuracy (AC)

Authentication accuracy is a key criterion to evaluate the performance of an authentication system. Some widely used metrics for evaluating authentication accuracy are FAR, FRR, EER. The definition of these metrics is:

• False Acceptance Rate (FAR): FAR indicates the probability of accepting an invalid user.

• False Rejection Rate (FRR): FRR indicates the probability of rejecting a valid user.

• Equal Error Rate (EER): EER is the rate when FAR is equal to FRR. Obviously, an authentication system with lower EER has higher accuracy. In our paper, we use EER to indicate authentication accuracy. We divide EER into three levels according to its scores as shown in Table 4.

3.1.2. Efficiency (EF)

Time cost has always been a primary measure of system performance. Taking less time in the process of authentication means better efficiency. To evaluate the efficiency of existing defense mechanisms, we mark out three levels of efficiency according to the time of finishing one certification process, as shown in Table 4.

3.1.3. Security (SE)

Security is of key importance in authentication. It refers to the ability of resisting attacks. As mentioned above, traditional password-based systems and biometric-based systems are vulnerable to different types of attacks. In Table 4, we define three security levels: high, medium and low.

3.1.4. Privacy (PV)

Privacy is also an important evaluation criterion for authentication systems. With the wide use of biometric authentication systems, it is easy to compromise individual biometric features. The photos, fingerprints, voice and other biometric features of a user are easily accessible by others in real life. Privacy protection is becoming a serious problem. We denote privacy into two specific categories: Usage privacy and identity privacy.

Usage Privacy Usage privacy refers to the user's habits when using an authentication system, such as keystroke habits. In addition, some users are accustomed to operating phones with single hand, while others prefer to use both hands. These operating habits reflect the user's personal privacy and they are easy to expose to attackers. For mobile computing, privacy should be highly concerned [141]. Users tend to overlook privacy issues in public places. In addition, permission requests from apps pose a significant privacy risk.

Identity Privacy Identity privacy concerns user's personal identity information. It is a big security issue with the development of social applications like online banking,

online traction, shopping, etc. [40]. Moreover, most communications and transactions rely on online platforms nowadays. The privacy of a user's personal identity is particularly important, and identity theft can lead serious consequences [66]. An adversary can build comprehensive user profiles by obtaining identity information about individuals. Therefore, it is necessary to consider identity privacy in authentication. Considering that most authentication systems does not consider privacy protection, we choose to mark out those methods that emphasize privacy, instead of defining different levels like other criteria. See Table 4 for a detailed description.

3.2. Usability (UA)

One of the most important criteria is usability. Users tend to expect a convenient and practical authentication system while its security should be ensured. An authentication system must be user friendly so that any person can use with ease. A defense mechanism mostly increases system robustness at the cost of reducing usability. We further divide usability into the following aspects. We define the quality levels of different criteria in Table 4.

3.2.1. Universality (UV)

Universality means that every user can use this design; the mechanism is also suitable for the elderly or young children to use.

3.2.2. Learnability (LA)

While considering performance, learnability means ease of use, and users can get rid of the trouble of complex operation and instruction on system operation. Learnability refers to the ability to operate skillfully when a user is using the same system over a short period. Users can quickly get familiar with previous operations, which means that the system has memory points.

3.2.3. Adaptability (AD)

Adaptability means a defense mechanism can apply into many contexts, it is easy to install and use in different network environments or with different devices.

3.2.4. User preference (UP)

User preference is an important factor in evaluating whether an authentication system has high performance. User preference refers to the user's willingness in term of system UI design and system performance, etc. It is a comprehensive result of user cognition and psychological feeling. The following questions can evaluate user preferences: Is this system easy to use? Does this system meet your requirements? Do you like the UI design of the system? Do you think the system is secure enough? Usually, a user study answers all the above questions about user preferences. We give the definition of specific levels of user preference, as shown in Table 4.

3.2.5. Cost of defense (CO)

While the performance of a defense mechanism is important, we also need to consider its costs, e.g., the need of special extra equipment for collecting user information. Besides the cost, we should also consider the complexity of system deployment at the same time. A practical authentication system should be easily applied into various different application environments. Therefore, we define three levels in Table 4 in terms of different situations about the cost of defense.

3.3. Reliability (RA)

In practice, the choice of biological characteristics depends on application scenarios [76]. Reliability refers to the ability of the system to complete the authentication task in specific scenarios. At the same time, accidents do not make the system lose normal working ability. High reliability means a superior tradeoff between system robustness and usability. Obviously, we prefer authentication systems having high reliability.

In the following review and comparative analysis, not all criteria of defense mechanisms are used since different authentication approaches have different properties, structures and application scenarios. As a result, we use some of the evaluation criteria as listed here to finish comparison. The criteria that are not mentioned are normally not considered in the current work. Note that in the following review, we only measure the performance of defense in the same category, which usually refers to the same type of systems or attacks.

4. Defense against Attacks

Referring to the different attacks as described in Section II, we investigate corresponding defenses and review prior works in this section.

4.1. Defense against Brute Force Attack

Due to the vulnerability of the password-based systems, some defense mechanisms have been proposed, such as account locking and Automated Turing Test (ATT) [102]. Account locking means limiting the number of wrong login times. The most common mechanism is to limit the number of logins to three. However, due to the complexity of the password and the limit of input times, even legitimate users may lock their accounts by mistakes. But allowing more than three times attempts will reduce system security. Besides that, ATT is a kind of widely used mechanisms nowadays. ATT can distinguish between humans and machines. CAPTCHAs, SMS (Short Messaging Service) authentication codes and challenge questions are common forms of ATT tests.

4.1.1. CAPTCHA Technologies

The full name of CAPTCHA is completely automated public Turing test to tell computers and humans apart [63]. The emergence of CAPTCHA technologies based on the idea that people can pass some intelligent tests that computers cannot solve. CAPTCHA technologies mainly include the

Table 4
The Hierarchical Division of Evaluation Criteria

Criteria		Level		
		High(H)	Medium(M)	Low(L)
Robustness (RO)	Accuracy	EER is less than 2%.	EER is between 2% and 10%.	EER is more than 10%.
	Efficiency	It takes less than 1 second to complete one authentication process.	The time of one authentication process is between 1 second and 3 seconds.	The time of one authentication process is more than 3 seconds.
	Security	The system can resist almost any type of attack. System FAR and FRR are less than 2% when suffering attack.	The system is relatively difficult to attack and it can defend most of attacks. System FAR and FRR are between 2% and 10% when suffering attack.	This system is not secure and it's easy to attack. System FAR and FRR are more than 10% when suffering attack.
	Privacy (Usage privacy and Identity privacy)	The system pays attention to the protection of users' privacy information. It hardly exposes any private information to others.	The system can protect partial personal information of users, but there is still a possibility exposing some private information.	The system cannot protect users' privacy information. Personal information is easily stolen by other people.
Usability (UA)	Universality	Every user can use this design.The system is also suitable for the elderly or young children to use.	Most users can use the system. It is possible that older or younger children cannot use it very skillfully.	Many users are not proficient in using the system. This design does not make sense.
	Learnability	The system is easy to use, and users will not be bothered by complex instructions. When users use the system again, they can still use it skillfully. It means the uniqueness of a system.	The system is generally easy to operate. There may be some complex hints or operations involved in the authentication process. After not using the system for a long time, users can recall how to use the system in a short time.	This system is inconvenient to use and difficult to operate. The system design is not unique enough for users to quickly recall how to use the system.
	Adaptability	This design can apply to almost all contexts, it is easy to install and use in different network environments or mobile devices.	This design can be used in most scenarios and can be installed on most mobile devices. But it may not be applicable in some special cases.	This design is poor and cannot apply in any other scenario. It's also hard to use on different versions of mobile phone systems.
	User preferences	Users are very satisfied with the system, the UI design is good, and the user interface design is reasonable.	Users are satisfied with the overall design of the system and the details can be further improved.	The whole design of the system is not good and it needs to be changed greatly.
	Overhead	The design requires additional devices to gather information, and it costs more. And it requires complex user operations.	The design requires additional equipment, but it does not cost much.The system requires a certain amount of user cooperation, but the operation is not complicated.	The design does not need any special extra equipment. It costs less in practice and it does not require complex user interaction.
Reliability (RA)		This design can balance system robustness and usability very well.	This design is able to balance robustness and usability in some specific situations.	This design does not consider the tradeoff between robustness and usability. It cannot be well applied in practice.

following four categories: Text-based CAPTCHA, Graphics-based CAPTCHA, Audio-based CAPTCHA and Puzzle-based CAPTCHA. Different types of CAPTCHAs have their own advantages and disadvantages. We make a comparison of these technologies and show the results in Table 5. In addition, dynamic CAPTCHA technology combines a user's specific mobile phone number or email address with a random CAPTCHA at the time of registration, which enhances security.

A system called CaRP was proposed by Kolekar et al. [104]. It combines both a CAPTCHA technology and a graphical password method. This system uses graphical password to enhance system security. In addition, it uses a clicked-based CAPTCHA to realizes human-machine recognition and thus it can prevent guessing attacks. A system [94] called CAPTCHA-based Password Authentication (CbPA) protocol uses both CAPTCHA and password in an authentication protocol. CAPTCHA and text password are independent in CbPA. The protocol CaRP combines a CAPTCHA and a graphical password that provides better solution than CbPA for brute force attacks. CaRP can resist Key Logger Software attack effectively since users do not input information from keyboard. Experiments showed that CaRP can also effectively resist brute force attacks, well-studied attacks and shoulder-surfing attacks. These above schemes are robust against shoulder-surfing attack, as users get different chal-

Table 5
Comparative Analysis of Defenses Technologies Against Brute Force Attack

Scheme	References	RO			UA	RA
		AC	EF	SE		
Text CAPTCHA	[29]	H	L	H	M	M
Graphics CAPTCHA	[104][94][101]	M	M	M	M	M
Audio-based	[64][132]	M	L	M	M	M
Video-based	[103][158]	L	M	L	M	M
Puzzle-based	[65]	L	M	L	M	M
SMS	[142][126]	H	M	M	M	M
Challenge questions	[1][215]	H	H	L	H	L

lenge images and options for every login. This mechanism has a good performance on improving online system security. Due to images are easier to recognize and remember than text, CaRP also offers reasonable usability.

In [101], Kirushnaamoni proposed a protocol called Password Guessing Resistant Protocol (PGRP), which effectively prevents brute and dictionary attacks while improving user experience. The PGRP protocol limits login attempts to one and uses a distorted text to perform ATT. The ATT test starts while user inputs wrong usernames, passwords, or both. Only when a user passes the test can the user get access to the system. In order to analyze the performance of PGRP protocol, Kirushnaamoni did an experiment based on a number of successful login attempts, failed login attempts with invalid passwords and failed login attempts with invalid password and ATT test. PGRP is effective in defending brute force attacks. Few ATT challenges also bring convenience to legitimate users.

In [1], Adams et al. reviewed existing mechanisms against brute force attacks on web applications, and then they proposed a practical and simple defensive system to enhancs the level of security, which can be easily deployed in existing systems. The proposed solution in [66] can be split into three ideas: separate the subsystems, identify directions and sliding window.

4.1.2. Short Messaging Service (SMS)

With the development of mobile communication devices such as smart phones and iPads, SMS authentication codes are already widely used to verify a legitimate user. It is convenient for users to purchase goods, take public transportation and do many other tasks by carrying their mobile phones. SMS authentication codes proposed in [142] contain activation message and an encrypted value timestamp using a cryptographic algorithm. This kind of method called One Time Password (OTP) that limits the use of timestamp and the generated authentication code. OTP provides high security because of the uniqueness of one password. In [142], the first step of generating the authentication code is to generate an activation message and then combine it with the timestamp. The next step is to encrypt the authentication code generated in the first step. The first six digits of cipher text are then used as the authentication code.

However, when a user's mobile phone is lost or stolen, using the authentication codes is not safe at all. To resolve this problem, it is particularly important to lock users' accounts remotely to prevent illegal appropriation. Some personal information such as photos, address books and chat history need protection when users' mobile phones are lost. It is necessary for users to remotely lock their smartphones and wipe/clean all data contained in them. These protective modes refer to a remote lock and a remote wipe service, respectively [126]. Gunil et al. [126] proposed a scheme that can lock users' mobile phones and wipe user data remotely. This system consists of two independent modules: a control module that is installed in another device and a command processing module usually appears in the user's mobile phone. By sending an SMS message to the lost mobile phone from the remote-control module, a command processing module inside the phone gets the message and performs corresponding actions. Gunil et al. highlighted that message integrity checking and message reply prevention should be highly considered. These two considerations ensure that it is the legal users who have sent the message and attackers do not listen to or intercept the message during message delivery. This scheme [74] performs better than other solutions from memory usage, time and bandwidth usage. It is faster than digital signature-based authentication and symmetry key-based authentication regarding average processing time. It is unnecessary to store a secret key separately, so the scheme proposed in [74] can save more storage and only require 32 bytes to transmit a message. Comparing with the digital signature-based systems that cost at least 80 bytes for message transmission, this scheme also saves bandwidth. Combined with the above advantages, the efficiency of the scheme [74] is relatively high.

4.1.3. Challenge Questions

Adams et al. pointed out that in order to solve the problem of memorizing passwords, some authentication systems tend to use security questions to challenge users [1]. However, these "challenge-response" systems are still vulnerable to brute force attacks because security questions are usually very simple, such as only asking your parents' first names.

An online password mechanism named "Combined-PWD" that inserts blanks into passwords can resist brute force attacks and dictionary attacks effectively [215]. During registration, users can choose to set specified characters or blanks anywhere in the passwords string. For example, the password is "a..p.pl.e", the server will record the number of separators as a string 2101 while storing the password. Then they only need to enter the passwords and the number of separators correctly during authentication. Users can insert more blanks in passwords rather than one or two. In this way, the number of blanks combinations is greatly increased. Even though attackers obtain the correct password, they still do not ensure where to insert blanks and the number of blanks.

In other words, this "Combined-PWD" mechanism increases the difficulty of guessing and enhances the password strength. Experimental results show that this system is easy to use and has low cost. High usability and security make widely used in various applications.

4.2. Defense against Shoulder-surfing Attack

There are several authentication methods to prevent shoulder surfing attacks. Teddy et al. [168] compared different schemes against shoulder-surfing attacks. They introduced well-known secure keypad schemes including qwerty-based, ABC based, Touch and Slide Secure Keypad, etc. However, traditional keypad solutions are not secure enough. The rest of this paper gives some suggestion to overcome shortcomings of existing methods. The core of one efficient scheme is to prevent attackers from guessing correct passwords or complete contents even if they obtain users' information by shoulder surfing.

In recent years, some defense mechanisms against shoulder-surfing attacks are secure but difficult to use. They usually need complex operations, which means low usability. For example, shoulder-surfing attacks bring risks to Personal Identification Number (PIN), which is a secure and usable scheme for user authentication. Normally, PIN is consisting of four or six digits that cannot ensure the security of the password. One defense proposed by Roth et al. [164] is black-and-white method (BW). The BW method requires users input each password number with colored button. Half of the keys of the digit keypad shown to users are black and others are white. Users need to respond the color of the digit by choosing the separate color key shown below. Roth et al. evaluated both security and usability of the proposed method. The proposed method performs better than regular PIN methods. Long execution time and large numbers of entries are two disadvantages of normal PIN methods. Roth et al. pointed out that security, usability and accuracy have great improvement in their method. This method has high accuracy and security, and this also improves the usability. Tic-Toc PIN, a colored PIN entry scheme, uses four colors white, black, blue and red [114]. Kwon and Hong [114] analyzed security and usability of Tic-Toc PIN method. Comparing with normal PIN methods, Tic-Toc PIN has higher security but lower usability.

A new attack called convert attentional shoulder surfing developed by Taekyoung et al. [115]. They proposed Revolving Flywheel PIN Entry Scheme, which contains outside layer, middle layer and inner layer. From the usability perspective, a system using Revolving Flywheel PIN Scheme is user-friendly and every person can use it with ease and fun.

As each time the user logs in, the challenge images received is different in CaRP [104]. CaRP is robust against shoulder-surfing attacks in practical applications, thus CaRP has sound security and usability. It provides various authentication schemes to users and these schemes protect a system from unauthorized access.

4.3. Defense against Phishing Attack

There are many effective ways to defend against phishing attacks. First, it is necessary to tell users to be vigilant about the Internet junk emails. There are several technical defense methods as follows [37].

- Monitor phishing networks and send warning message timely.
- Use spam filters to prevent spam emails.
- Improve web security using hardware devices or biometrics characteristics (e.g., face, voice, iris, etc.)
- Install anti-phishing software on client sides.

Juan et al. [31] reviewed approaches mentioned above. DNS scanning periodically is one method for phishing monitoring. However, it faces the problem of increasing the overhead of DNS systems.

Spam filters use blacklist, whitelist, keyword filters, Bayesian filters with self-learning abilities, and E-Mail Stamp, etc. to filter phishing e-mails. Blacklist and whitelist need to know attackers' names in advance. Probabilities of false positives and false negatives still exist when using keyword filters and Bayesian filters.

Installing software on client sides is the last defense. Some tools like ScamBlocker [188], PhishGuard [95], and Netcraft [25] can be included as blacklist/whitelist based category. Another category is rule-based tools. Examples include SpoofGuard [124] and TrustWatch that check the website security according certain rules such as domain names, port numbers, and so on.

All of these defense mechanisms have their pros and cons. An algorithm named Link-Guard designed in [31] can achieve high detection accuracy. Link-Guard belongs to the fourth type of methods mentioned above. It can detect known and unknown phishing attacks. Juan et al. [31] performed their experiments in Windows XP and this method shows high accuracy and high efficiency on preventing phishing attacks. The scheme takes less than 1% CPU time and less than 7 MB memory.

4.4. Defense against Spoofing Attacks in Biometric-based Systems

Spoofing defense approaches usually refer to liveness detection techniques, especially in the biometric-based systems. In many scenarios, both anti-spoofing and liveness detection are regarded as the same [62]. A good defense method should be effective to all types of spoofing attacks, including artificial synthesis and replay attacks. From a general perspective, there are three group of spoofing defenses techniques for biometric-based authentication systems: hardware-based, software-based and multi-model.

Hardware-based Approaches Hardware-based methods require some hardware devices to detect particular properties of different biometric traits like facial expression [62, 173], blood pressure [174], finger sweat [176], etc.

Software-based Approaches Software-based approaches normally refer to feature extraction from biometric samples rather than from human beings directly. Static methods and dynamic methods are two different types of software approaches

[62]. They can differentiate by identifying that the input is one biometric sample or a time sequence of samples.

Both hardware-based and software-based methods have their pros and cons. In Table 6, we make a comparison of these two types of methods about their performance and usability. In general, the hardware-based methods usually have high detection accuracy, which means these approaches have good performance in practice. But the cost of extra devices may be a problem, which may cause low usability. Sometimes the hardware methods are not applicable in practice. The software-based methods cost less and more user-friendly, but they present lower performance than the hardware-based ones. Therefore, a combination of both advantages would be a good way to improve the performance of biometric-based systems.

Multi-model Approaches It is easy to associate that multi-model biometric systems are more robust than the above two kinds of systems since attackers need to forge multiple biometrics in this kind of systems [173]. In practice, multi-model approaches fuse different biometrics in order to increase the difficulty of authentication intrusion.

Combining multiple defense mechanisms can significantly improve the security of the system, such as combining more than two kinds of biometric features, combining biometrics and verification codes, etc. The two-factor authentication methods use cards or tokens with passwords to improve the security. Nevertheless, there are additional costs associated with purchasing and issuing cards. Meanwhile, carrying a card becomes a burden to users and cards are easy to be lost. It was shown that systems based on audio-visual fusion gain better robustness [153]. Such as, in a low Signal-to-Noise Ratio (SNR) environment, only acoustic feature does not acquire high performance. In [154], experimental results showed that correlation features do improve performance. In [67], the fusion system that combines face and keystroke dynamics acquired a good EER of 2.22%. This result is lower than the EER of any single feature system, means better performance. In the meantime, this kind of method does not need extra user interactions. Obviously, it improves usability and reduces cost.

A multi-factor biometric authentication system for cloud computing was proposed in [216] by adopting palm vein and fingerprint as features. This system stores palm vein data in smart cards and fingerprint data in a central database of a cloud server. The use of smart cards in this method enhances the security but it also increases cost.

However, multi-modal biometric systems cannot completely resist spoofing attacks [163]. This conclusion based on the assumption that attackers can submit perfect replicated biometric traits refers to a "worst case" scenario. Attackers can replicate biometric features perfectly in worst case. In [18], Biggio et al. analyzed the robustness of multimodal biometric systems that consist of face and fingerprints modules. They investigated three attack scenarios including fingerprint spoofing only, face spoofing only and both fingerprint and face spoofing. FAR was tested to assess the performance of the fusion system. Biggio et al. noticed that FAR of multimodal systems is similar than FAR of face or fingerprint system alone. The results pointed out that multi-model systems are not always more robust than a single model system in a worst-case assumption, as they can be attacked by spoofing only one biometric. This leads us to develop a novel score fusion model or design robust fusion rules.

In what follows, we summarize existing defense methods, including their performance analysis. Face and fingerprint are two types of widely used biometric information [177]. There already have some surveys about face and fingerprint recognition [4, 54, 193]. Herein, we focus on spoofing defense approaches. It is worth noting that the dataset and experimental process used by different methods are different, and the results mentioned here are only for reference.

4.4.1. Artificial Synthesis Defense

With the continuous progress of science and technology, advanced scientific techniques can detect synthetic biological features. Baldisseri et al. proposed using odor analysis to detect artificial fingerprint samples [88].

4.4.2. Replay Attack Defense

Biometric authentication systems are vulnerable to spoofing attacks. Liveness Detection (LVD) has achieved good performance in resisting replay attacks [174]. It refers to the techniques that can detect physical spoofing samples. Liveness detection can efficiently distinguish between humans and machines by sensing living features such as facial expression changes, lip movements and speech. Some methods also detect physical properties like spectral reflection, density and visual color [43]. We review liveness detection for face anti-spoofing, speech anti-spoofing, fingerprint anti-spoofing, iris anti-spoofing and other approaches as below.

Face Anti-spoofing Using Convolutional Neural Networks (CNNs) [193] can enhance the accuracy of face recognition. But even if recognition accuracy has improved, face authentication based systems are still vulnerable to attack. In recent years, a number of liveness detection methods were proposed for face recognition.

A system proposed in [173] uses pupil tracking to detect spoofing attack. This system achieves high accuracy but it needs a hardware equipment for eye region detection. According the analysis of [120], existing face authentication systems have low security, so they are vulnerable to Online Social Network Facial Disclosure (OSNFD) attacks. While liveness detection is a good method against the OSNFD attack, it also takes low accessibility at the same time. Normally, conducting liveness detection requires extra equipment and close user interactions. Eye blinking, facial expression, and head rotation are common liveness detection methods applied. According to the analysis in [47], the usability of most liveness detection mechanisms is not good. We need to explore effective and usable liveness detection mechanisms. Galbally et al. [62] provided a comprehensive overview on face anti-spoofing. Herein, we do not go into details and only list them in Table 7.

In addition, morphing software makes face morphing at-

Table 6
Comparison of Different Types of Spoofing Defense Approaches

Types		RO	UA	RA	Pros	Cons
Hardware-based		++	++	++	Very high accuracy	Slow, extra equipment, intrusive
Software-based	Static	+	+	+	Fast	Low accuracy
	Dynamic	+	+	+	Highaccuracy	Slow
	Multimodal	+	+	++	Highsecurity	More cost

RO: robustness; UA: usability; RA: reliability.
-:The more symbols, the higher the level of the method under this standard.

Table 7
Summary of Face Anti-Spoofing Approaches

Types		Methods	Reference	Attacks	Accuracy
Hardware-based		Motion detection	[105]	Photo video	H
		Multispectral lighting	[213]	Photo video mask	M
		3D scans	[111]	mask	L
		Thermal images	[49]][26] [83]	mask	L
Software-based	Static	Lambertian model	[104]	photo	L
		Multiple Difference of Gaussian (DOG) filters	[212]	Photo video	L
		Local Binar Patterns	[110]	Photo	L
		Upper body and spoof support detection	[106]	Photo video	M
	Dynamic	Eye blinking	[105][146][181][182]	Photo	H
		Face and background motion	[9]	photo	L
		Gaze tracking	[19, 5]	Photomask	M
		Optical flow estimation	[8]	photo	H
Multi-biometric		Face images and speech	[33, 36][100, 14][199]	Photomaskvideo	M

tack easier [108]. Robertson et al. did a test to evaluate the human performance of recognizing morphed images based on Morph Acceptance Rate (MAR) and False Rejection Rate (FRR) [162]. MAR is a probability of falsely accepted morphing trials and FRR represents the number of false rejections. The experiment result shows the MAR is as much as 21%, which means the morphing attack needs to be highly considered. However, the performance of Automated Face Recognition (AFR) systems against morphing attacks is not good.

There are many methods proposed to perform morphing detection. In order to detect Face Morphing Forgery (FMF) attacks, in [96], Neubert et al. proposed a novel three-fold definition (visual, biometric and forensic qualities) for the quality of morphed images to improve morphing detection. In addition, Neubert et al. introduced a novel FMF realization method in order to improve visual and biometric quality. One "DE morphing" approach presented in [55] aims to achieve morphing detection for a live image. However, the error rate of existing morphing detection is still very high and their detection performance is also poor. Research on the defense of morphing attacks requests further study in the future.

Speech Anti-spoofing Voice recognition is drawing increasing attention and becomes one of mainstreams of today's authentication technologies. However, it is easy to record or imitate speech in direct or indirect ways, so voice authentication is also vulnerable to spoofing attacks. Automatic Speaker Verification (ASV) systems are widely used in modern society due to its unique convenience, rapidity and high security. Distinguishing natural speech signals and artificial speech signals is the key to resist spoofing attacks.

Table 8
Comparison of Different Speech Spoofing Attacks

Types	Input	Effort	Effectiveness
Zero-effort attack	Fake speech	Zero	Low
Speech synthesis	Text	High	High
Voice conversion	Fake speech	Medium	Medium
Voice Replay	Recording	Low	Medium

Speech synthesis, voice conversion and speech replay attacks are three types of spoofing in ASV systems. Janicki et al. [88] analyzed different types of spoofing attacks and tested their effects in different environments. They reviewed several defense methods of replay attacks and evaluated their performance in different ASV systems including a standard Gaussian Mixture Model with Universal Background Model (GMM-UBM) system, a GMM super vector linear kernel system [27], and an I-Vector system with Probabilistic Linear Discriminant Analysis (PLDA).

We make a comparison of different spoofing attacks in terms of attack input, attacker's effort and effectiveness in Table 8 [197]. Zero-effort imposter attack, in which attackers try to impost an authentication system with their own speech. Obviously, the effectiveness of this attack is the lowest. Voice conversion and speech synthesis need extra equipment and professional technologies. Hence, they belong to medium and high effort spoofing attacks. On the contrary, replay attacks only require recording and replaying, so it is regarded as a low effort attack compared with other attacks. From the table, we notice that the efficiency is proportional to input.

In [88], Janicki et al. described two replay countermeasures, one is Far-Field Channel Detection (FFCD) and the other is Local Binary Patterns (LBP). The experimental result shows LBP performs better than FFCD for replay spoofing detection. The EER of LBP is 2.87% and the EER of FFCD is 16.53%. Spoofing False Acceptance Rate (SFAR) is similar to the false rejection rate. Although SFARs with FFCD and LBP reduce a lot but the lowest SFAR is still around 30%. It suggests that replay attack is still an unsolved problem.

Pop noise, is a kind of distortion of speech when human voice is close to microphones. Researches showed that pop noise will be reproduced when a loud speaker play the same speech. Therefore, we can distinguish between real and artificial speech signals by detecting pop noise [197].

Zhang et al. [209] presented a liveness detection system named Voice-Live. They noticed that each phoneme could be uniquely located in the human vocal channel system. Microphones can capture the time difference of arrival (TDoA) of each phoneme. TDoA dynamic does not exist under replay attacks so Voice-Live can detect a live user using unique TDoA. The experimental result shows that the detection accuracy of the proposed system is over 99% and the EER is 1%. The proposed system is compatible to different phone models, as it does not require additional equipment but only smartphones with two-channel stereo recording. The level of accuracy is high and this defense has high usability.

There are many other works in defending against voice replay attacks. Some previous works [35, 147] use audio streams against spoofing attacks. They use static or dynamic relations between a user's face motion and voice. Rahman et al. [156] proposed Movee that combines video and accelerometer data to verify liveness. Movee estimates whether motion features in video stream are consistent with features extracted from an accelerometer sensor stream. During verification, a user moves a camera toward a target and the Movee client captures corresponding video stream and accelerometer data. In essence, Movee's accuracy ranges between 68-93%, which implies its accuracy level is medium. Movee has a number of shortcomings. First, it needs six seconds in verification, which obviously affects usability. Meanwhile, the verification needs user cooperation that decreases learnability and user preference. Second, Movee has difficulty to extract information from the video with blur or occlusions and illumination changes. The adaptability of this system is not good. At last, the cost of this system is not low because its requests a client and an extra server.

In [208], a novel system called Voice Gesture was proposed for detecting replay attacks. A user's pronunciation gesture may cause Doppler Effect. The Doppler shift produced by human speech is larger than that produced by a loudspeaker. The loudspeaker relies on a one-dimensional moving diaphragm to generate sound waves, so it produces a relatively stable output. The detection accuracy of Voice Gesture is over 99% and the EER is 1%. This system does not need complex operations and extra equipment, which implies high usability while ensuring security. In addition, the time of one authentication process is about 0.5 seconds, which shows high-level efficiency. One disadvantage is that users need to hold a phone in their hands when they are using Voice Gesture. Hence, this system's adaptability is not so good.

In addition, voice recognition is often combined with other technologies to realize liveness detection and enhance system security. For example, Kaman et al. [96] designed a practical authentication system for remote online banking. When a user is trying to login, a remote server will give a phone call to the user and ask he or she to record voice. Then the server conducts identification by comparing the received voice with a target.

In [34, 32], authors of these two works utilized lip movements for liveness detection. In particular, Chetty et al. [34] did a combination of text and lip features to improve the security of user authentication. Experimental results showed that EER of less than 1% is achieved. It is a powerful method to verify liveness and has good robustness and usability.

Cheng et al. [32] proposed a novel scheme to avoid replay attacks. Many existing systems use fixed password for authentication, thus using prerecorded video can trick the system. To solve this problem, random prompt password can protect system from replay attacks. In [32], Cheng et al. built a deep convolution neural network (DCNN) that consists of three parts, a lip characteristic network, an identity network and a content network. The DCNN can describe both static and dynamic lip characteristics comprehensively. Moreover, it can extract features to distinguish different speakers and contents. Compared with several methods based on fixed password, this scheme has high authentication accuracy and better performance.

In [201], Zhao and Yan proposed a voice authentication service system that contains User Agent (UA), Relying Party (RP) and Identity Provider (IDP). UA tries to get access to relevant services of RP by passing voiceprint authentication offered by IDP through random personal voice challenge. This system can efficiently resist the replay attack and it has medium accuracy and high usability.

AV-spoof is a public database of audio-visual deception [50]. In [50], Ergunay et al. provided a set of experimental results to show the impact of these spoofing attacks on two state-of-the-art ASV systems. They suggested that future work should focus on developing a general strategy that can effectively deal with various attacks in speech recogni-

Table 9
Replay Spoofing Attack Defenses for Speaker Authentication Systems.

Methods	RE	RO				UA			RA
		AC	EF	SE	PV	UP	OH	LE	
Far-field channel detection (FFD)	[88] [192]	M	H	-	-	-	M	-	L
Local binary patterns (LBP)	[88] [143]	L	H	-	-	-	M	-	L
Voice Live	[209]	H	H	M	-	H	L	-	H
Voice Gesture	[208]	H	H	M	M	M	M	-	M
Video Motion Analysis	[156]	M	M	M	M	L	L	L	L
Lip movements	[34]	H	-	H	-	-	-	H	M
	[32]	H	-	H	-	H	-	M	M

RE: references AC: accuracy; EF: Efficiency; SE: security; PV: privacy
UP: user preference; OH: overhead; LE: learnability;
-: this approach does not support this criterion.

tion. For easy reference, Table 9 summarizes the above reviewed approaches.

Fingerprint Anti-spoofing Fingerprints have been widely used in various applications for many years. Fingerprint spoofing methods include direct methods and indirect methods [176]. The direct methods often use various materials like silicone, candle wax, and thermoplastic to make fake fingerprints. The indirect methods use other ways to obtain genuine fingerprints pattern indirectly. For instance, attackers can obtain latent fingerprints left in public.

Liveness detection methods in fingerprint recognition can be divided into hardware-based and software-based. Hardware-based methods require extra hardware equipment and software-based methods need to embed a software component to realize liveness detection. Due to the use of extra hardware, the former methods introduce extra cost. On the contrary, the latter methods based on software may impact usability although with low cost.

The software-based liveness detection methods can be further divided into two types. One is static methods and the other is dynamic methods [176]. The static methods analyze differences between genuine and fake fingerprints through a 2D scan. Sweat pores are small structures and they are difficult to reproduce. Some research [39] achieves liveness detection based on the sweat pores analysis. Ridge and valley texture are detailed properties that can be used to distinguishing real and fake fingerprints [187, 185].

The dynamic methods make use of static features of fingerprints and try to analyze time series of fingerprint images. Common methods include skin distortion [92, 10] and perspiration analysis [185, 150, 184]. Jin et al. [93] noticed that sweat fluid looks different on living fingers and fake fingers. This perspiration phenomenon has been studied in some literatures [24, 186, 48, 150, 91, 46, 140, 128].

Comparing with software countermeasures, hardware-based methods are more straightforward. The goal of these methods is to enhance defense capability by adding additional hardware components. Yau et al. [202] proposed a challenge and response system with an electrode array that can generate electric pulses. The basis of this design is that fake fingers may not be able to sense the electrical signal accurately. Odor analysis was applied in [11] based on an electronic nose that can distinguish different materials like silicone, latex and gelatin. Table 10 summarizes the above reviewed approaches.

Table 10
Summary of Fingerprint Anti-Spoofing Approaches.

Types		Methods	Reference	AC
Hardware-based		Challenge-response	[202]	H
		Odor analysis	[12]	H
Software-based	Static	Sweat pores	[39]	M
		Ridge and valley	[187, 185]	M
	Dynamic	Skin distortion	[92][10]	M
		Perspiration	[185][150][184]	M

Iris Anti-spoofing Photo attacks, contact-lens attacks and artificial eye attacks are three types of iris spoofing attacks [60, 61]. In most cases, an attacker shows an iris picture of a genuine user to perform photo attacks. In contact-lens attacks, an attacker wears contact lens with a pattern of genuine iris in order to evade detection. The third type of attacks utilize artificial eyes made of glass or plastic.

Anti-spoofing approaches are also referred as liveness detection, vitality detection or standardized term presentation attack detection [60]. Javier et al. provided a comprehensive review on iris spoofing detection. Similar to other biological modalities, there are two types of iris spoofing detection methods. One is hardware-based

techniques that use hardware to identify eye features. The other is software-based, which is further classified into static and dynamic methods.

Hardware-based methods for iris anti-spoofing usually take advantage of specific camera or other hardware devices. In early studies, spectrographic properties of the eye such as tissue, fat and blood are used to detecting the spoofing attack. And another type is based on behavioral eye features, such as blinks, pupil fynamics, eyeball movements, etc. [156]. Almost all methods need high quality cameras to capture iris features, which obviously introduces extra costs.

Software-based approaches are based on biological features extracted from biometric samples rather than users directly. Automated feature-level methods [145, 41] were proposed to analyze artificial frequencies in iris images. Currently, deep neural networks have shown good performance against iris spoofing attacks [200, 112]. Beyond that, in [172], an iris recognition method based on random projections and sparse representations was proposed by Pillai et al. This method gains high accuracy about 99%. At the same time, the method can also protect user privacy but the level is only medium.

Most approaches mentioned above are starting to be ap-

Table 11
Summary of Iris Anti-Spoofing Approaches

Types		Reference	Methods	AC
Hardware-based		[87]	Pupil contraction	M
		[139]	NIR camera	M
		[42]	Pupil dynamics	H
Software-based	Static	[207]	LBP	M
		[63]	Image quality measures	M
		[200][112]	Using Deep learning	H
	Dynamic	[155]	Multi binary statistical image features	H

plied into mobile applications. We summarize our review about iris anti-spoofing approaches in Table 11.

Other Approaches There are many other ways to resist spoofing attacks, such as secret sharing. The digitization of personal identity requires high security of authentication systems. Secret sharing, which cut a complete data into some small parts called as shares [206]. These parts are then stored at different places. A secret sharing scheme can solve issues such as spoofing and excessive demand for data storage. However, security and privacy of authentication need improvement. In [161], Patil et al. proposed a biometric-based authentication system using multiple secret shares, which reduces computational complexity and space complexity. Comparing to traditional biometric systems, this system reduces the computational complexity and space complexity of a system. The experiment result shows that space complexity of the system is half of that of the traditional systems. The accuracy of the secret sharing system in [161] is 94%, higher than 90% in traditional systems.

Pirlo et al. proposed a new system using a multi-domain strategy for signature verification [151]. Its main idea is similar to secret sharing. They split a signature into different segments and authenticated each segment separately during verification. A distance-based consistency model on features was applied to demonstrate that pen position, velocity, and inclination have high consistency among segments. In [151], the SUSIG [57] database of handwritten signatures was used to test system performance. Using the multi-domain strategy, each segment of the signature is evaluated separately. The final result is determined by combing different segment decisions. Verification results of the multi-domain system are FRR=2.15% and FAR=2.10%. When using all the domains of representation, results are FRR=3.60% and FAR=4.15%. That is, the proposed multi-domain strategy has better accuracy compared with traditional approaches.

4.5. Deep Learning Approaches For Spoofing Attacks

This subsection reviews existing literatures on the use of deep learning algorithms and deep neural networks to defend spoofing attacks in terms of face recognition, speech recognition, and signature recognition, etc.

4.5.1. Deep Learning for Face Recognition

Deep learning algorithm can effectively improve the accuracy of face recognition-based authentication. During face recognition, detection accuracy is often affected by lighting and position changes. In [193], Wang et al. used Deep Reinforcement Learning (DRL) with Convolutional Neural Networks (CNNs) to process face features. The proposed scheme effectively improves the accuracy of face recognition up to 99.5

4.5.2. Deep Learning for Speech Recognition

Artificial neural networks have made a big impact on speech recognition. Deng and Li [47] gave an overview of recent achievements of deep learning in speech recognition. There is a sort of standardized technology of using Gaussian mixture models for acoustic analysis and Hidden Model Markov (HMM) models, and so on. By using deep learning models for speech recognition, recognized word error rate can be enormously decreased about 30

Using machine learning and deep learning in voice identification is one popular topic recently. However, there remain some outstanding problems. First, it is still prior to do audio pre-processing to build a specific speech model for each person. Second, since people sound at different volumes in different situations, all levels of data need to be obtained during training phase. In addition, environmental noise also causes a negative impact when training a model.

Noise processing is one of the most difficult parts in speech recognition systems. Traditional models, such as HMM, have achieved good speech processing performance, but they are not robust in noisy environments [45]. In [167], a speech recognition system that combines two different deep neural networks, CNN and RNN, significantly improves system accuracy.

Hybrid speech recognition systems show better performance comparing with Deep Neural Network (DNN) [45], experiments show that Deep Max-out Networks (DMNs) using a max-out technique performs better in comparison to other systems (DNN with pre-training, DNN with dropout, and DMN-based ASR systems) . In addition, the system employing DMN has good robustness in different noisy conditions.

4.5.3. Deep Learning for Signature Recognition

Leap Motion can detect people's motion using infrared rays. Katagiri et al. believe that aerial signatures are more robust than paper signatures [124]. In [31], Hatanaka et al. collected signatures using the Leap Motion and conducted experiments for signature authentication. Both researches [97, 77] proved that aerial input was robust for signature recognition. In [62], Yamamoto et al. proposed a method of writing numbers in the air by using the Leap Motion. The average accuracy of the proposed system was 90.3%, FRR was 3.8% and FAR was 5.9%. The biggest disadvantage of this method is the need of Leap Motion that increases cost. To improve the accuracy, they proposed to use several numerals as input data instead of single numeral.

4.5.4. More Authentication Systems Using Deep Learning

In [163], Rodrigues et al. used Long Short-Term Memory (LSTM), a deep learning approach, to deny unauthorized access in security intensive places like hotels and shopping malls. LSTMs are a special kind of RNN that can remember information for a long period of time. The proposed model achieves high authentication accuracy of 95% by processing Channel State Information (CSI) from Wi-Fi signal. Experimental results show this model is better than other CSI based authentication models.

Footprint scanning is practical for personal verification because everyone has specific footprints. It is novel to use footprint images to build a footprint-based identification system [98]. Keatsamarn et al. [98] executed footprint recognition using deep learning. They used an optical sensor system to get foot images and a convolutional neural network for deep learning classification. A validation test among 13 people showed that the system achieves 92.69% recognition rate that means a high-level accuracy.

Safavi et al. [165] gave us a novel idea that associate the fingerprint, voiceprint, facial recognition of a person to build a fusion model. This approach can reduce the likelihood of replay attacks, because it is difficult for an attacker to obtain different biological characteristics of a legitimate user at the same time. Users need to provide three different forms of biological features (face images, fingerprints, and voice) for authentication. The fusion method enhances the security of authentication system. The hybrid model is trained by machine learning algorithms. The model merges the scores of three different characteristics into one score to determine whether a current user is legal or not. Experiments show that the fusion model significantly improves the system performance against replay attacks. But this work only provides EER without touching other evaluation criteria listed in Section III.

As mentioned in [47], transfer learning and multi-task learning in DNN-based authentication systems are novel and practical. In speech recognition systems, different kinds of languages can be treated as multiple tasks. A multi-lingual or cross-lingual speech model can not only distinguish different languages but also enhance security and accuracy of speech recognition [68].

In order to clearly show the effect of using deep learning algorithms in biometric authentication systems, we compare deep learning methods with the classic methods introduced earlier in Table 12. From Table 11, we can see that both methods have advantages or shortcomings. Using deep learning methods normally has high accuracy and security, but they request more cost than the classic methods. The combination of both methods may be an ideal strategy to improve the performance of biometric systems.

Table 12
Comparison of Classic Approaches and Deep Learning Approaches for Spoofing Attacks in Biometric-Based Systems.

Approaches	AC	SE	UA	CO
Classic	ow	low	low	less
Deep learning	high	high	high	more

4.6. Defenses against Poisoning Attacks

Shen et al. proposed Auror against poisoning attacks to ensure good performance of indirect deep learning systems [170]. Collaborative deep learning is a technology that collects data from different sources and combines them together. In direct collaborative learning, users make modification on data than submitting raw data directly. Direct collaborative learning trains user data directly. Submitting processed data can avoid user personal privacy leakage. Moreover, partial calculation or feature extraction can greatly reduce the amount of data, thus reducing the computational burden of the server. The server generates a global model using data submitted by the users. Unlike direct collaboration, the users submit processed features instead of raw features in indirect collaborative learning. It is noticed that the indirect way is superior to the direct way because privacy can be protected and it distributes the computation cost at the same time.

Auror is a defense that can detect malicious users and it is applied in image recognition systems to evaluate their performance. Auror can achieve a 100% detection successful rate for 10% to 30% of malicious users. The levels of Auror's accuracy and security are both high, with the consideration on privacy preservation.

4.7. Defenses against Adversarial Attacks

Inspired by [4] and [205], we discuss defenses against adversarial attacks by classifying them into three main types, as reported in Table 13 and described below. We also list the robustness of these schemes in the table. For defensive systems, we mainly focus on their robustness in face of attacks, that is, whether the system can still ensure high accuracy when attacked, and whether its defense affects similarly when facing different degrees of attack.

Active Defense Active defense modifies the structures of networks or input during testing. It can be further divided into modified training/input (e.g., brute force adversarial training) and modified networks (e.g., adding layers or changing loss function).

Several contributions show adversarial training can help improving robustness [133, 51]. Adversarial examples are required when training a network as training data. Since this kind of methods increase training data size, it also refers to a brute-force method.

Network distillation improves robustness by reducing the size of deep neural networks [149]. Papernot et al. [149] tested "network distillation" on two datasets: MNIST and CIFAR10. The MNIST contains 70,000 black and white images of handwritten digits. CIFAR10 contains 60,000 color images. The result shows that the distillation method proposed in [149] reduces the success rate of Jacobian-based

Table 13
Summary of Defense Strategies for Adversarial Attacks

Types	Sub-types		References	RO
Active Defenses	Modified training/input	Adversarial training	[70, 85] [84, 122]	+
	Modified networks	Network distillation	[149]	+
	Modified networks	Network verification	[72, 99]	+
Passive Defenses	Add networks	Adversarial detecting	[43, 80, 148] [194, 183, 47]	+
		Input transformation	[74, 3]	+
Ensemble defenses			[81]	+

Saliency Map Attack (JSMA) attack. JSMA is a kind of adversarial attacks for fooling neural networks. Network verification is another active defense method. It can prevent unseen attacks by checking the properties of deep neural networks [188] [189].

Passive Defense Passive defense usually detects adversarial attacks when building deep neural networks. This type of methods does not change the structure of the neural network. Adversarial detecting and input transformation are two types of passive defense approaches. After input transformation, adversarial data become real data. Deep Contractive Auto-encoder (DCA) is a kind of auto-encoder network trained from adversarial examples to clean data and from clean samples to adversarial examples [74]. In [116], Ledig et al. proposed a framework by appending extra layers to the deep neural network. These extra layers are Perturbation Rectifying Networks (PRNs), which are trained to rectify adversarial examples.

Generative Adversarial Networks (GAN) consists of a generative model and a discriminative model. The purpose of generative model is to generate a confrontational sample similar to the real data, while the discriminant model attempts to distinguish real data from fake samples. These two networks compete with each other and play a two-player minimax game [71]. Lee et al. proposed to train a generator network that generates perturbation for a target network, and it helps the classifier to classify the real and adversarial images during training [117]. Detecting adversarial examples during the testing stage is a popular way to defend attacks. In [130], the authors trained an auxiliary network to detect adversarial examples. Feinman et al. deployed Bayesian neural networks to distinguish clean data and adversarial data [52]. Besides, Carlini et al. showed that most detecting methods [16, 52, 69, 73, 82, 131] are not strong enough under C&W attacks.

Ensemble Defense This type of methods combines multiple defense strategies together to prevent adversarial attacks. Meng and Chen integrated more than two detectors and re-constructors based on auto-encoders to detect adversarial examples [81] However, work in [78] showed that combination of several weak approaches does not make networks stronger than a single defense approach.

Table 14
Comparison of Different Authentication Systems.

Types	Advantages	Disadvantages
Text-based systems	Quick response; Easy to implement; Familiar for user to use	Dictionary attack, Brute force attack, Shoulder surfing, Social engineering
Graphical-based systems	Good memorability Less vulnerable to phishing and other social engineering attacks	Requirement of password space More vulnerable to shoulder surfing than text passwords Log-in success rates, log-in times and password creation times
Token-based systems	Resist replay attacks	Need to carry physical devices, Need more time
Biometric-based systems	No need to memorize complex passwords High security and usability	Usually need bigger storage to store biological template; Require expensive hardware to extract such features; Spoofing attack; Privacy disclosure; Need more time

Up to now, according our investigation, all defenses mentioned above are only effective for weak attacks. Some of them only work on a certain type of attacks. When an attacker changes its attacking method (e.g., C&W), most of the defensing methods will fail. Obviously, these methods are still very weak. Hence, the methods that can offer strong defense effectively in practice are highly expected, especially in the field of speech recognition, in which deep learning algorithms are widely used.

5. Comparison and Analysis

In this section, we evaluate the existing methods of detecting and resisting user authentication attacks by employing evaluation criteria proposed in Section III.

5.1. Comparison of Authentication Systems

We divide authentication systems into four categories. They are traditional text-based systems, graphical-based systems, token-based systems and biometric-based systems. Readers can clearly find the advantages and disadvantages of these four types of systems from Table 14.

The advantages of traditional password-based systems are obvious. They are easy to understand and accept by most users. Meanwhile, plain text or combination of letters and numbers require small storage space, so response time of registration and authentication is short. Nonetheless, password-based systems are vulnerable to brute force attacks so they are less secure than other types of systems. As an improvement measure, authentication systems based on image passwords have improved security. But this type of systems requires more password storage space and takes a longer time to register and authenticate. Graphical password

systems may impact user experiences. Token-based systems improve authentication security, but they require users to carry extra devices. In other words, the usability of token-based systems is unsatisfactory.

Some technologies effectively improve traditional password authentication systems, such as the CAPTCHA techniques. We have classified the existing techniques and compare their performance based on the criteria proposed in Section III. We show our evaluation results in Table 5.

Recently, the emerging biometric-based authentication systems adopt unique biological characteristics as a password, which greatly enhance the security compared with the traditional password-based systems. At the same time, using biometrics can solve the usability problem of remembering complex passwords. Unfortunately, attackers still can hack this kind of systems by spoofing or replaying users' biometric information.

Despite the diversity of biological characteristics, current researches have shown that some characteristics (e.g., gait, voice) are more robust than others (e.g., face, iris) under spoofing attacks [76]. The most influential reason is that

Fingerprints are more likely to forge due to the difference between behavioral and physiological features. Generally, gait, voice and signature have high variability compared with physiological features like fingerprints. However, physiological features outperform behavioral features regarding recognition and authentication accuracy if spoofing does not exist in most cases. In [76, 38], an evaluation method was presented for the assessment of spoofing and countermeasures.

Table 15 compares different biometric authentication systems by dividing them into three categories: physical feature systems, behavioral feature systems, and multi-model feature systems. The physical feature systems, such as face recognition and fingerprint recognition, have the advantage of not requiring users to remember any passwords or do additional operations. With the advance of modern biological science and technologies, the accuracy of identifying features of fingerprints and faces has also increased significantly. However, the main drawback of this kind of static feature authentication systems is that most systems require special devices to collect user input signals. This requirement introduces extra cost in practical applications. Keystrokes and signatures have been applied into the behavioral feature systems in early years. Then, voice recognition appeared. Refer to Table 9, these authentication systems are easily to be accepted by users because behavior characteristics are convenient to be provided in most cases. However, such systems are relatively insecure due to spoofing and replaying attacks. In addition, the multi-model feature systems combine a variety of biological features to take the advantages of different approaches. They offer high security, but hard to be deployed in real world.

Through comparison, we notice that authentication systems based on biometric features generally have high accuracy and good usability. Although face recognition systems are efficient and users prefer facial recognition systems, some extra cost of detecting face images exists in practice.

5.2. Comparison of Defense Mechanisms

In Section IV, we review the defense work related to the attacks classified in Section II. In what follows, we make a comparison and summary.

We list three methods to defend against brute force attacks. Table 5 shows comparison of their performance. CAPTCHA is currently widely used in our life, especially text-based and graph-based CAPTCHAs, and their efficiency is relatively high. At present, the biggest disadvantage of CAPTCHA technologies is that they usually require user cooperation, e.g., graphical CAPTCHA. For other categories of CAPTCHA technologies, text CAPTCHA cannot defend Optical Character Recognition (OCR). Audio CAPTCHA require attackers to have enough knowledge. Both video and puzzle CAPTCHA have the problem of correspondingly long-time consumption.

High accuracy and simple operation are important advantages of SMS technology, but its security is not strong. Using challenge questions has the same advantages as SMS, e.g., good accuracy and usability, but low security.

For defending against shoulder-surfing attacks, the BW method and Tic-Toc PIN are two ways to improve the performance. In addition, a graphical way called CaRP is robust to shoulder-surfing attacks. This method has high robustness and usability, which also means high reliability.

Spoofing attacks in biometric-based systems is a hot discussion angle at present. Liveness detection can efficiently prevent the replay attack that is one kind of spoofing attacks. In Section IV, we reviewed the mechanisms to defend the replay attacks in face recognition, speech recognition, fingerprint recognition and iris recognition, which contain three categories: hardware-based approaches, software-based approaches and multi-model approaches. Due to the use of extra hardware, the hardware-based approaches increase the cost although they have good robustness normally. Methods based on software limit the cost but decrease usability at the same time. Software methods are invasive and usually need more user coordination, so they may impact user friendliness. The multi-model approaches enhance system robustness, but may increase system cost and impact usability.

We reviewed recent advances in applying deep learning algorithms into authentication systems. In speech recognition, the word error can decrease about 30%. Using deep reinforcement learning in face recognition can reach an accuracy up to 99.5%. There is no doubt that deep learning does improve the performance of biometric authentication systems. But attacking deep neural network systems is not difficult. There are already many examples of adversarial attacks that pose a threat to authentication systems. Unfortunately, existing defense methods are not robust enough, which requests further exploration in the future.

Through our review, we can see that the defense methods are generally divided into the following two categories: hardware based methods and software based methods.

Table 15
Advantages and Disadvantages of Different Biological Features Authentication System

Scheme	Features	References	AC	UA	AD	DA
Physical features	Face	[157, 169, 62, 26] [19, 23, 107]	H	M	Higher fake detection rate Higher accuracy	Extra devices expensive Required higher user cooperation
	Iris	[15, 61, 145, 41] [200, 112, 139] [42, 63, 155]	H	M	Easy to use Great accuracy	Poor generalization ability Performance degrade with light intensity variation
	Fingerprint	[127, 22, 171, 12] [176, 39, 187, 185] [150, 184, 93, 24] [186, 91, 46, 140] [128, 11, 63]	H	M	Easy to use Generally applicable	Need extra equipment High cost
	Palm	[89, 191]	M	M		
Behavioral features	Key stroke	[215]	M	M	High Acceptability	Key position and velocity can be attacked by key loggers
	Dynamic Signatures	[152]	M	M	Resist shoulder-surfing	Need extra equipment
	Voice	[30, 36, 201] [50, 210]	M	H	High Acceptability Against photo attack	Low security
Multi-modal features	Fingerprint, Palm print and Iris	[148]	M	M	Enhance the security	Difficult to deploy in real-world scenarios
	Audio-visual cross-modal fusion	[153]	H	M	Good performances, acceptability, and respect of privacy. Don't need complex interactions with the user	
	Keystroke dynamics and 2D-face recognition	[67]	H	M		
	Face and voice	[58]	M	H		

Hardware based defense usually aims at "patching" system architecture, which requires additional equipment and authentication process, e.g., SMS verification code, ID card, etc. This kind of extra equipment is held by users. That is to say, the device is a legal certificate corresponding to the user. Only those who hold it are legal users. Unless the user accidentally loses it, it is difficult to steal or copy. This method has high security, so it is often used in e-commerce and other systems involving transactions. But the corresponding authentication process is complex. If users use the system frequently, such as unlocking a mobile phone, the usability of such a method will be greatly affected.

Software based defense is usually designed based on the algorithm used in the system, but sometimes it also introduces additional process. For example, when a cryptosystem is faced with the threat of brute force cracking, we can add a graphic verification code. The time cost of machine learning to identify the graphics is intolerable for attackers. For the systems that have already used machine learning and deep learning (such as user authentication based on images, audio and other data), it is possible to add adversarial training to improve classification accuracy, and offer random transformation to cover the target user model. Generally speaking, the weakness of this kind of method is that its scope of defense is limited, and the defense method itself is actually equivalent to an algorithm. When the attacker finds a further attack method on this algorithm, the system will be exposed to risk. Therefore, the effectiveness of this method in practical applications needs further research and verification.

In view of the application of machine learning has become a trend, it is inevitable to research attacks and defense measures of machine learning. In fact, many attacks on deep learning have been studied. It is worth noting that there is a difference in the performance of this kind of attack between black-box test and white-box test, which is shown in Table 3. Therefore, in the real environment, whether an effective attack can be implemented is a problem worthy of discussion. In addition, defense measures against existing attacks are also very limited. They can only prevent one kind of attack, but they can't meet the needs of practical application. Defending against most attacks is a very difficult thing, and so far there is no work to do so. Therefore, in the research of this aspect, we should pay attention to confirm which specific attack scenarios the defense method can deal with. But we think that a more secure system architecture may be able to better solve this kind of problem basically. In addition, blockchain offers a new way to avoid many weaknesses in common centralized systems, and seems to be a better choice in the future. But at the same time, this kind of systems will faces some new security threats. In view of the fact that there is no longer a single server in the distributed system, how to confirm the credibility of team members and how to carry out mutual verification are issues that need to be specially concerned.

6. Open Issues and Future Directions

6.1. Open Issues

Based on the analysis in Section V, we found that the performance of the current authentication systems is much better than that of the early days, but attacks are emerging and there still exist some open issues about defense in authentication systems.

First, because of the high demand of both security and usability and their conflict in the authentication systems, how

to balance between usability and security is always an open issue. How to reduce complex operations and improve user experience while effectively resisting various attacks is the key to design a well-accepted authentication system. At the same time, we prefer a system that gains high performance with a low cost. Reliability refers to the balance of system robustness and usability. Low reliability is prevalent in today's authentication systems.

Second, current liveness detection methods suffer from high cost and usability problems. Liveness detection is an effective and practical way to prevent spoofing attacks for biometric-based authentication systems. However, current liveness detection methods usually need additional devices or close user cooperation. These extra requirements decrease system usability and increase system cost. Some biometric-based authentication systems require additional devices to collect biological signals, thus minimizing cost is preferred.

Third, user privacy protection is often ignored in existing work. User private information, such as user identity, user profile, user biometric information should be protected from leaking to any untrusted and unauthorized parties. But many existing systems ignore this issue without any consideration.

At last, defense mechanisms to resist attacks on machine learning in authentication systems are not strong enough. Machine learning and deep learning technologies actually improve the performance, especially in face and speech recognition. However, due to the immaturity of machine learning technologies, defenses against some novel attacks, such as adversarial attacks, are still under study. The latest research has shown that it is relatively easy to attack deep learning networks. For example, for adversarial attacks and poisoning attacks, their corresponding defense methods are not strong enough. In addition, applications of deep learning in other fields besides computer vision are still under continuous research.

6.2. Future Directions

Based on the open issues given above, we suggest some future research directions for designing a secure and usable authentication system.

First, robustness is always the key point in authentication. Facing all kinds of new types of attacks, the performance of the authentication system against different attacks need to be improved. Many current authentication systems have been able to achieve a relatively high accuracy, but there are still cases of false rejection and false acceptance in biometric authentication systems. User privacy is also an important factor that should be paid specially attention, but most systems ignore it. Adding attack defense mechanisms may impact authentication speed and introduce extra cost. Current systems cannot satisfy all above in a perfect way. High security, high accuracy, high efficiency and user privacy preservation are expected to be fulfilled simultaneously.

Second, we should pay attention to improving user experience, including the convenience of system operation, the appearance of system, and the response speed of system. There is no doubt that enhancing system usability will be one focus of future research work. Overall, an authentication system with high reliability is mainly expected.

Third, preservation on user private information should be ensured. Past work did not pay much attention to this study, while user privacy preservation is crucially important, especially in biometric authentication systems. We think privacy-preserving or leakage resilient user authentication systems will be a future research focus in this field.

Fourth, a system with high adaptability to resist various attacks should be investigated. A good authentication system needs to be able to resist different types of attacks rather than just one of them. This means that the system needs to have good adaptability. Some new attacks like adversarial attacks are trying to break deep neural networks. These attacks indeed pose a great threat to authentication systems based on deep learning. Through our literature review, we found that corresponding defense mechanisms are not mature, and current research only has a breakthrough in the field of computer vision. Future research needs to make efforts to inspire highly effective methods against adversarial attacks in user authentication.

Last but not the least, the wide usage and applications of user authentication systems request continuous research to constantly optimize and improve system performance with regard to robustness, usability and reliability in a holistic way.

7. Conclusion

This paper reviewed attacks and corresponding defense mechanisms in the authentication systems. We introduced common attacks on user authentication by classifying them into different categories. We put forward a series of evaluation criteria and employ them to compare and analyze existing defense mechanisms against different types of attacks in different categories of authentication systems. Through a thorough review, we proposed some open questions and pointed out suggestions on future research.

CRediT authorship contribution statement

Xuerui Wang: Conceptualization of this study, Investigation, Writing - Original draft preparation. **Zheng Yan:** Supervision, Project administration, and Funding acquisition. **Rui Zhang:** Investigation, Writing - Review & editing. **Peng Zhang:** Supervision.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 62072351; in part by the Academy of Finland under Grant 308087 and Grant 335262; in part by the Shaanxi Innovation Team Project under Grant 2018TD-007; and in part by the 111 Project under Grant B16037.

References

[1] Adams, C., Jourdan, G.V., Levac, J.P., Prevost, F., 2010. Lightweight protection against brute force login attacks on web applications, in: 2010 Eighth International Conference on Privacy, Security and Trust, IEEE. pp. 181–188.

[2] Adler, A., 2005. Vulnerabilities in biometric encryption systems, in: International Conference on Audio-and Video-Based Biometric Person Authentication, Springer. pp. 1100–1109.

[3] Akhtar, N., Liu, J., Mian, A., 2018. Defense against universal adversarial perturbations. doi:10.1109/CVPR.2018.00357.

[4] Akhtar, N., Mian, A., 2018. Threat of adversarial attacks on deep learning in computer vision: A survey. IEEE Access 6, 14410–14430.

[5] Ali, A., Deravi, F., Hoque, S., 2012. Liveness detection using gaze collinearity, in: 2012 Third International Conference on Emerging Security Technologies, IEEE. pp. 62–65.

[6] Alomar, N., Alsaleh, M., Alarifi, A., 2017. Social authentication applications, attacks, defense strategies and future research directions: a systematic review. IEEE Communications Surveys & Tutorials 19, 1080–1111.

[7] Alpar, O., 2017. Frequency spectrograms for biometric keystroke authentication using neural network based classifier. Knowledge-Based Systems 116, 163–171.

[8] Anjos, A., Chakka, M.M., Marcel, S., 2013. Motion-based countermeasures to photo attacks in face recognition. IET biometrics 3, 147–158.

[9] Anjos, A., Marcel, S., 2011. Counter-measures to photo attacks in face recognition: a public database and a baseline, in: 2011 international joint conference on Biometrics (IJCB), IEEE. pp. 1–7.

[10] Antonelli, A., Cappelli, R., Maio, D., Maltoni, D., 2006. Fake finger detection by skin distortion analysis. IEEE Transactions on Information Forensics and Security 1, 360–373. doi:10.1109/TIFS.2006.879289.

[11] Baldisserra, D., Franco, A., Maio, D., Maltoni, D., 2005. Fake fingerprint detection by odor analysis, in: Zhang, D., Jain, A.K. (Eds.), Advances in Biometrics, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 265–272.

[12] Baldisserra, D., Franco, A., Maio, D., Maltoni, D., 2006. Fake fingerprint detection by odor analysis, in: International Conference on Biometrics, Springer. pp. 265–272.

[13] Baluja, S., Fischer, I., 2017. Adversarial transformation networks: Learning to generate adversarial examples. arXiv preprint arXiv:1703.09387 .

[14] Basori, A.H., Bade, A., Sunar, M.S., Daman, D., Saari, N., 2010. E-facetic: the integration of multimodal emotion expression for avatar through facial expression, acoustic and haptic, in: Proceedings of the 9th ACM SIGGRAPH Conference on Virtual-Reality Continuum and its Applications in Industry, pp. 147–150.

[15] Bazrafkan, S., Corcoran, P., 2018. Enhancing iris authentication on handheld devices using deep learning derived segmentation techniques, in: 2018 IEEE international conference on consumer electronics (ICCE), IEEE. pp. 1–2.

[16] Bhagoji, A., Cullina, D., Mittal, P., 2017. Dimensionality reduction as a defense against evasion attacks on machine learning classifiers .

[17] Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H., Bhogle, P., 2015. Comparison of graphical password authentication techniques. International Journal of Computer Applications 116.

[18] Biggio, B., Akthar, Z., Fumera, G., Marcialis, G.L., Roli, F., 2011. Robustness of multi-modal biometric verification systems under realistic spoofing attacks, in: 2011 International Joint Conference on Biometrics (IJCB), pp. 1–6. doi:10.1109/IJCB.2011.6117474.

[19] Bigun, J., Fronthaler, H., Kollreider, K., 2004. Assuring liveness in biometric identity authentication by real-time face tracking, in: Proceedings of the 2004 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, 2004. CIHSPS 2004., IEEE. pp. 104–111.

[20] Blasco, J., Chen, T.M., Tapiador, J., Peris-Lopez, P., 2016. A survey of wearable biometric recognition systems. ACM Computing Surveys (CSUR) 49, 1–35.

[21] Boles, A., Rad, P., 2017. Voice biometrics: Deep learning-based voiceprint authentication system, in: 2017 12th System of Systems Engineering Conference (SoSE), IEEE. pp. 1–6.

[22] Borra, S.R., Reddy, G.J., Reddy, E.S., 2016. A broad survey on fingerprint recognition systems, in: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE. pp. 1428–1434.

[23] Bowyer, K.W., Chang, K., Flynn, P., 2006. A survey of approaches and challenges in 3d and multi-modal 3d+2d face recognition. Computer Vision and Image Understanding 101, 1–15. URL: https://www.sciencedirect.com/science/article/pii/S1077314205000822, doi:https://doi.org/10.1016/j.cviu.2005.05.005.

[24] Bozhao Tan, Schuckers, S., 2006. Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing, in: 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), pp. 26–26. doi:10.1109/CVPRW.2006.120.

[25] Brooks, J., 2005. Netcraft stats bode well for fedora. URL: https://www.eweek.com/servers/netcraft-stats-bode-well-for-fedora.

[26] Buddharaju, P., Pavlidis, I.T., Tsiamyrtzis, P., Bazakos, M., 2007. Physiology-based face recognition in the thermal infrared spectrum. IEEE transactions on pattern analysis and machine intelligence 29, 613–626.

[27] Campbell, W.M., Sturim, D.E., Reynolds, D.A., 2006. Support vector machines using gmm supervectors for speaker verification. IEEE signal processing letters 13, 308–311.

[28] Carlini, N., Katz, G., Barrett, C., Dill, D.L., 2018. Ground-truth adversarial examples .

[29] Chandavale, A.A., Sapkal, A.M., Jalnekar, R.M., 2010. A framework to analyze the security of text based captcha. International Journal of Computer Applications 1, 127–132.

[30] Chen, D., Mak, B., Leung, C.C., Sivadas, S., 2014. Joint acoustic modeling of triphones and trigraphemes by multi-task learning deep neural networks for low-resource speech recognition, in: 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE. pp. 5592–5596.

[31] Chen, J., Guo, C., 2006. Online detection and prevention of phishing attacks, in: 2006 First International Conference on Communications and Networking in China, IEEE. pp. 1–7.

[32] Cheng, F., Wang, S.L., Liew, A.W.C., 2018. Visual speaker authentication with random prompt texts by a dual-task cnn framework. Pattern Recognition 83, 340–352.

[33] Chetty, G., 2009. Biometric liveness detection based on cross modal fusion, in: 2009 12th International Conference on Information Fusion, IEEE. pp. 2255–2262.

[34] Chetty, G., Wagner, M., 2004. Automated lip feature extraction for liveness verification in audio-video authentication. Proc. Image and Vision Computing , 17–22.

[35] Chetty, G., Wagner, M., 2006. Multi-level liveness verification for face-voice biometric authentication, in: 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, IEEE. pp. 1–6.

[36] Chibelushi, C.C., Deravi, F., Mason, J.S., 2002. A review of speech-based bimodal recognition. IEEE transactions on multimedia 4, 23–37.

[37] Chiew, K.L., Yong, K.S.C., Tan, C.L., 2018. A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications 106, 1–20.

[38] Chingovska, I., d. Anjos, A.R., Marcel, S., 2014. Biometrics evaluation under spoofing attacks. IEEE Transactions on Information Forensics and Security 9, 2264–2276. doi:10.1109/TIFS.2014.2349158.

[39] Choi, H., Kang, R., Choi, K., Jin, A.T.B., Kim, J.H., 2009. Fake-fingerprint detection using multiple static features. Optical Engineering 48, 047202.

[40] Choudhury, H., Roychoudhury, B., Saikia, D.K., 2012. Enhancing user identity privacy in lte, in: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Commu-

nications, IEEE. pp. 949–957.
[41] Czajka, A., 2013. Database of iris printouts and its application: Development of liveness detection method for iris recognition, in: 2013 18th International Conference on Methods Models in Automation Robotics (MMAR), pp. 28–33. doi:10.1109/MMAR.2013.6669876.
[42] Czajka, A., 2015. Pupil dynamics for iris liveness detection. IEEE Transactions on Information Forensics and Security 10, 726–735. doi:10.1109/TIFS.2015.2398815.
[43] Das, A., Pal, U., Ferrer, M.A., Blumenstein, M., 2016. A framework for liveness detection for direct attacks in the visible spectrum for multimodal ocular biometrics. Pattern Recognition Letters 82, 232–241.
[44] Das, S., Suganthan, P.N., 2010. Differential evolution: A survey of the state-of-the-art. IEEE transactions on evolutionary computation 15, 4–31.
[45] De-La-Calle-Silos, F., Gallardo-Antolín, A., Peláez-Moreno, C., 2014. Deep maxout networks applied to noise-robust speech recognition, in: Advances in Speech and Language Technologies for Iberian Languages, Springer International Publishing, Cham. pp. 109–118.
[46] DeCann, B., Tan, B., Schuckers, S., 2009. A novel region based liveness detection approach for fingerprint scanners, in: Tistarelli, M., Nixon, M.S. (Eds.), Advances in Biometrics, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 627–636.
[47] Deng, L., 2016. Deep learning: from speech recognition to language and multimodal processing. APSIPA Transactions on Signal and Information Processing 5.
[48] Derakhshani, R., Schuckers, S.A., Hornak, L.A., O'Gorman, L., 2003. Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognition 36, 383–396. URL: https://www.sciencedirect.com/science/article/pii/S0031320302000389, doi:https://doi.org/10.1016/S0031-3203(02)00038-9. biometrics.
[49] Dhamecha, T.I., Nigam, A., Singh, R., Vatsa, M., 2013. Disguise detection and face recognition in visible and thermal spectrums, in: 2013 International Conference on Biometrics (ICB), IEEE. pp. 1–8.
[50] Ergünay, S.K., Khoury, E., Lazaridis, A., Marcel, S., 2015. On the vulnerability of speaker verification to realistic voice spoofing, in: 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), IEEE. pp. 1–6.
[51] Evtimov, I., Eykholt, K., Fernandes, E., Kohno, T., Li, B., Prakash, A., Rahmati, A., Song, D., 2017. Robust physical-world attacks on machine learning models. CoRR abs/1707.08945. URL: http://arxiv.org/abs/1707.08945, arXiv:1707.08945.
[52] Feinman, R., Curtin, R.R., Shintre, S., Gardner, A.B., 2017. Detecting adversarial samples from artifacts. arXiv:1703.00410.
[53] Feng, Q., He, D., Zeadally, S., Liang, K., 2020. Bpas: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. IEEE Transactions on Industrial Informatics 16, 4146–4155. doi:10.1109/TII.2019.2948053.
[54] Ferrara, M., Franco, A., Maltoni, D., 2017a. Face demorphing. IEEE Transactions on Information Forensics and Security 13, 1008–1017.
[55] Ferrara, M., Franco, A., Maltoni, D., 2017b. Face demorphing. IEEE Transactions on Information Forensics and Security 13, 1008–1017.
[56] Ferrer, M.A., Diaz, M., Carmona-Duarte, C., Plamondon, R., 2018. A biometric attack case based on signature synthesis, in: 2018 International Carnahan Conference on Security Technology (ICCST), pp. 1–6. doi:10.1109/CCST.2018.8585714.
[57] Ferrer, M.A., Morales, A., Díaz, A., 2014. An approach to swir hyperspectral hand biometrics. Inf. Sci. 268, 3–19.
[58] Finandhita, A., Afrianto, I., 2018. Development of e-diploma system model with digital signature authentication, in: IOP Conference Series: Materials Science and Engineering, IOP Publishing. p. 012109.
[59] Fischer, V., Kumar, M.C., Metzen, J.H., Brox, T., 2017. Adversarial examples for semantic image segmentation. arXiv preprint arXiv:1703.01101 .
[60] Galbally, J., Gomez-Barrero, M., 2016a. A review of iris antispoofing, in: 2016 4th International Conference on Biometrics and Forensics (IWBF), pp. 1–6. doi:10.1109/IWBF.2016.7449676.
[61] Galbally, J., Gomez-Barrero, M., 2016b. A review of iris antispoofing, in: 2016 4th International Conference on Biometrics and Forensics (IWBF), pp. 1–6. doi:10.1109/IWBF.2016.7449676.
[62] Galbally, J., Marcel, S., Fierrez, J., 2014. Biometric antispoofing methods: A survey in face recognition. IEEE Access 2, 1530–1552.
[63] Galbally, J., Marcel, S., Fierrez, J., 2014. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE Transactions on Image Processing 23, 710–724. doi:10.1109/TIP.2013.2292332.
[64] Gao, H., Liu, H., Yao, D., Liu, X., Aickelin, U., 2010a. An audio captcha to distinguish humans from computers, in: 2010 Third International Symposium on Electronic Commerce and Security, IEEE. pp. 265–269.
[65] Gao, H., Yao, D., Liu, H., Liu, X., Wang, L., 2010b. A novel image based captcha using jigsaw puzzle, in: 2010 13th IEEE International Conference on Computational Science and Engineering, IEEE. pp. 351–356.
[66] Gevers, S., Verslype, V., De Decker, B., 2007. Enhancing privacy in identity management systems, in: Proceedings of the 2007 ACM workshop on Privacy in electronic society, pp. 60–63.
[67] Giot, R., Hemery, B., Rosenberger, C., 2010. Low cost and usable multimodal biometric system based on keystroke dynamics and 2d face recognition, in: 2010 20th International Conference on Pattern Recognition, pp. 1128–1131. doi:10.1109/ICPR.2010.282.
[68] Giri, R., Seltzer, M.L., Droppo, J., Yu, D., 2015. Improving speech recognition in reverberation using a room-aware deep neural network and multi-task learning, in: 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 5014–5018. doi:10.1109/ICASSP.2015.7178925.
[69] Gong, Z., Wang, W., Ku, W., 2017. Adversarial and clean data are not twins. CoRR abs/1704.04960. URL: http://arxiv.org/abs/1704.04960, arXiv:1704.04960.
[70] Goodfellow, I., Shlens, J., Szegedy, C., 2015. Explaining and harnessing adversarial examples, in: International Conference on Learning Representations. URL: http://arxiv.org/abs/1412.6572.
[71] Goodfellow, I.J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y., 2014. Generative adversarial networks. arXiv:1406.2661.
[72] Gopinath, D., Katz, G., Pasareanu, C.S., Barrett, C.W., 2017. Deepsafe: A data-driven approach for checking adversarial robustness in neural networks. CoRR abs/1710.00486. URL: http://arxiv.org/abs/1710.00486, arXiv:1710.00486.
[73] Grosse, K., Manoharan, P., Papernot, N., Backes, M., McDaniel, P.D., 2017. On the (statistical) detection of adversarial examples. CoRR abs/1702.06280. URL: http://arxiv.org/abs/1702.06280, arXiv:1702.06280.
[74] Gu, S., Rigazio, L., 2015. Towards deep neural network architectures robust to adversarial examples. arXiv:1412.5068.
[75] Guo, S., Hu, X., Guo, S., Qiu, X., Qi, F., 2020. Blockchain meets edge computing: A distributed and trusted authentication system. IEEE Transactions on Industrial Informatics 16, 1972–1983. doi:10.1109/TII.2019.2938001.
[76] Hadid, A., Evans, N., Marcel, S., Fierrez, J., 2015. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Processing Magazine 32, 20–30.
[77] Hatanaka, I., Kashima, M., Sato, K., Watanabe, M., 2016. Study on flexible aerial signature individual authentication system using the finger discrimination information. The Journal of the Institute of Image Information and Television Engineers 70, J125–J132. doi:10.3169/itej.70.J125.
[78] He, W., Wei, J., Chen, X., Carlini, N., Song, D., 2017. Adversarial example defenses: Ensembles of weak defenses are not strong, in: Proceedings of the 11th USENIX Conference on Offensive Technologies, USENIX Association, USA. p. 15.
[79] Hein, M., Andriushchenko, M., 2017. Formal guarantees on the robustness of a classifier against adversarial manipulation, in: Ad-

vances in Neural Information Processing Systems, pp. 2266–2276.

[80] Hendrik Metzen, J., Chaithanya Kumar, M., Brox, T., Fischer, V., 2017. Universal adversarial perturbations against semantic image segmentation, in: Proceedings of the IEEE International Conference on Computer Vision, pp. 2755–2764.

[81] Hendrycks, D., Gimpel, K., 2016. Visible progress on adversarial images and a new saliency map. CoRR abs/1608.00530. URL: http://arxiv.org/abs/1608.00530, arXiv:1608.00530.

[82] Hendrycks, D., Gimpel, K., 2017. Early methods for detecting adversarial images. arXiv:1608.00530.

[83] Hermosilla, G., Ruiz-del Solar, J., Verschae, R., Correa, M., 2012. A comparative study of thermal face recognition methods in unconstrained environments. Pattern Recognition 45, 2445–2459.

[84] Huang, L., Joseph, A.D., Nelson, B., Rubinstein, B.I., Tygar, J.D., 2011. Adversarial machine learning, in: Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence, Association for Computing Machinery, New York, NY, USA. p. 43–58. URL: https://doi.org/10.1145/2046684.2046692, doi:10.1145/2046684.2046692.

[85] Huang, R., Xu, B., Schuurmans, D., Szepesvári, C., 2015. Learning with a strong adversary. CoRR abs/1511.03034. URL: http://arxiv.org/abs/1511.03034, arXiv:1511.03034.

[86] Huang, S., Papernot, N., Goodfellow, I., Duan, Y., Abbeel, P., 2017. Adversarial attacks on neural network policies. arXiv preprint arXiv:1702.02284 .

[87] Huang, X., Ti, C., Hou, Q., Tokuta, A., Yang, R., 2013. An experimental study of pupil constriction for liveness detection, in: 2013 IEEE Workshop on Applications of Computer Vision (WACV), pp. 252–258. doi:10.1109/WACV.2013.6475026.

[88] Janicki, A., Alegre, F., Evans, N., 2016. An assessment of automatic speaker verification vulnerabilities to replay spoofing attacks. Security and Communication Networks 9, 3030–3044.

[89] Jaswal, G., Kaul, A., Nath, R., 2018. Multiple feature fusion for unconstrained palm print authentication. Computers & Electrical Engineering 72, 53–78.

[90] Jeyaraman, S., Topkara, U., 2005. Have the cake and eat it too-infusing usability into text-password based authentication systems, in: 21st Annual Computer Security Applications Conference (ACSAC'05), IEEE. pp. 10–pp.

[91] Jia, J., Cai, L., 2007. Fake finger detection based on time-series fingerprint image analysis, in: Huang, D.S., Heutte, L., Loog, M. (Eds.), Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 1140–1150.

[92] Jia, J., Cai, L., Zhang, K., Chen, D., 2007. A new approach to fake finger detection based on skin elasticity analysis, in: International Conference on Biometrics, Springer. pp. 309–318.

[93] Jin, C., Li, S., Kim, H., Park, E., 2011. Fingerprint liveness detection based on multiple image quality features, in: Chung, Y., Yung, M. (Eds.), Information Security Applications, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 281–291.

[94] Jose, J., Tomy, T.T., Karunakaran, V., Varkey, A., Nisha, C., et al., 2016. Securing passwords from dictionary attack with character-tree, in: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE. pp. 2301–2307.

[95] Joshi, Y., Saklikar, S., Das, D., Saha, S., 2008. Phishguard: a browser plug-in for protection from phishing, in: 2008 2nd International Conference on Internet Multimedia Services Architecture and Applications, IEEE. pp. 1–6.

[96] Kaman, S., Swetha, K., Akram, S., Varaprasad, G., 2013. Remote user authentication using a voice authentication system. Information Security Journal: A Global Perspective 22, 117–125.

[97] Katagiri, M., Sugimura, T., 2002a. Personal authentication by free space signing with video capture , 23–25.

[98] Katagiri, M., Sugimura, T., 2002b. Personal authentication by free space signing with video capture , 23–25.

[99] Katz, G., Barrett, C., Dill, D.L., Julian, K., Kochenderfer, M.J., 2017. Towards proving the adversarial robustness of deep neural networks. Electronic Proceedings in Theoretical Computer Science 257, 19–26. URL: http://dx.doi.org/10.4204/EPTCS.257.3, doi:10.4204/eptcs.257.3.

[100] Kessous, L., Castellano, G., Caridakis, G., 2010. Multimodal emotion recognition in speech-based interaction using facial expression, body gesture and acoustic analysis. Journal on Multimodal User Interfaces 3, 33–48.

[101] Kirushnaamoni, R., 2013a. Defenses to curb online password guessing attacks, in: 2013 International Conference on Information Communication and Embedded Systems (ICICES), IEEE. pp. 317–322.

[102] Kirushnaamoni, R., 2013b. Defenses to curb online password guessing attacks, in: 2013 International Conference on Information Communication and Embedded Systems (ICICES), IEEE. pp. 317–322.

[103] Kluever, K.A., 2008. Evaluating the usability and security of a video captcha .

[104] Kolekar, V.K., Vaidya, M.B., 2015. Click and session based—captcha as graphical password authentication schemes for smart phone and web, in: 2015 International Conference on Information Processing (ICIP), IEEE. pp. 669–674.

[105] Kollreider, K., Fronthaler, H., Bigun, J., 2008. Verifying liveness by multiple experts in face biometrics, in: 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, Ieee. pp. 1–6.

[106] Komulainen, J., Hadid, A., Pietikäinen, M., 2013. Context based face anti-spoofing, in: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), IEEE. pp. 1–8.

[107] Komulainen, J., Hadid, A., Pietikäinen, M., 2013. Context based face anti-spoofing, in: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp. 1–8. doi:10.1109/BTAS.2013.6712690.

[108] Korshunova, I., Shi, W., Dambre, J., Theis, L., 2017. Fast face-swap using convolutional neural networks, in: Proceedings of the IEEE International Conference on Computer Vision, pp. 3677–3685.

[109] Kos, J., Song, D., 2017. Delving into adversarial attacks on deep policies. arXiv preprint arXiv:1705.06452 .

[110] Kose, N., Dugelay, J.L., 2012. Classification of captured and recaptured images to detect photograph spoofing, in: 2012 International Conference on Informatics, Electronics & Vision (ICIEV), IEEE. pp. 1027–1032.

[111] Kose, N., Dugelay, J.L., 2013. Reflectance analysis based countermeasure technique to detect face mask attacks, in: 2013 18th International Conference on Digital Signal Processing (DSP), IEEE. pp. 1–6.

[112] Kuehlkamp, A., Pinto, A., Rocha, A., Bowyer, K.W., Czajka, A., 2019. Ensemble of multi-view learning classifiers for cross-domain iris presentation attack detection. IEEE Transactions on Information Forensics and Security 14, 1419–1431. doi:10.1109/TIFS.2018.2878542.

[113] Kurakin, A., Goodfellow, I., Bengio, S., 2016. Adversarial examples in the physical world. arXiv preprint arXiv:1607.02533 .

[114] Kwon, T., Hong, J., 2014. Analysis and improvement of a pin-entry method resilient to shoulder-surfing and recording attacks. Ieee transactions on information forensics and security 10, 278–292.

[115] Kwon, T., Shin, S., Na, S., 2013. Covert attentional shoulder surfing: Human adversaries are more powerful than expected. IEEE Transactions on Systems, Man, and Cybernetics: Systems 44, 716–727.

[116] Ledig, C., Theis, L., Huszar, F., Caballero, J., Cunningham, A., Acosta, A., Aitken, A., Tejani, A., Totz, J., Wang, Z., Shi, W., 2017. Photo-realistic single image super-resolution using a generative adversarial network. arXiv:1609.04802.

[117] Lee, H., Han, S., Lee, J., 2017. Generative adversarial trainer: Defense to adversarial perturbations with GAN. CoRR abs/1705.03387. URL: http://arxiv.org/abs/1705.03387, arXiv:1705.03387.

[118] Li, J., Monroe, W., Jurafsky, D., 2016a. Understanding neural networks through representation erasure. arXiv preprint

arXiv:1612.08220 .

[119] Li, Y., Li, Y., Xu, K., Yan, Q., Deng, R.H., 2016b. Empirical study of face authentication systems under osnfd attacks. IEEE Transactions on Dependable and Secure Computing 15, 231–245.

[120] Li, Y., Li, Y., Xu, K., Yan, Q., Deng, R.H., 2016c. Empirical study of face authentication systems under osnfd attacks. IEEE Transactions on Dependable and Secure Computing 15, 231–245.

[121] Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., Choo, K.R., 2020. Homechain: A blockchain-based secure mutual authentication system for smart homes. IEEE Internet of Things Journal 7, 818–829. doi:10.1109/JIOT.2019.2944400.

[122] Liu, W., Cao, Y., Cao, C., Liu, Y., Hu, Y., Guo, L., 2018. An adversarial training framework for relation classification, in: Shi, Y., Fu, H., Tian, Y., Krzhizhanovskaya, V.V., Lees, M.H., Dongarra, J., Sloot, P.M.A. (Eds.), Computational Science – ICCS 2018, Springer International Publishing, Cham. pp. 194–205.

[123] Liu, Y., Chen, X., Liu, C., Song, D., 2016. Delving into transferable adversarial examples and black-box attacks. arXiv preprint arXiv:1611.02770 .

[124] Lu, G., Chadha, K., Debray, S., 2013. A simple client-side defense against environment-dependent web-based malware, in: 2013 8th International Conference on Malicious and Unwanted Software:" The Americas"(MALWARE), IEEE. pp. 124–131.

[125] Luong, M.T., Le, Q.V., Sutskever, I., Vinyals, O., Kaiser, L., 2015. Multi-task sequence to sequence learning. arXiv preprint arXiv:1511.06114 .

[126] Ma, G.I., Park, K.W., Yi, J.H., Jin, S.H., 2012. Smartphone remote lock and data wipe system based on message authentication codes, in: Applied Mechanics and Materials, Trans Tech Publ. pp. 267–271.

[127] Marasco, E., Ross, A., 2014. A survey on antispoofing schemes for fingerprint recognition systems. ACM Computing Surveys (CSUR) 47, 1–36.

[128] Marcialis, G.L., Roli, F., Tidu, A., 2010. Analysis of fingerprint pores for vitality detection, in: 2010 20th International Conference on Pattern Recognition, pp. 1289–1292. doi:10.1109/ICPR.2010.321.

[129] Meng, W., Wong, D.S., Furnell, S., Zhou, J., 2014. Surveying the development of biometric user authentication on mobile phones. IEEE Communications Surveys & Tutorials 17, 1268–1293.

[130] Metzen, J.H., Genewein, T., Fischer, V., Bischoff, B., 2017a. On detecting adversarial perturbations. arXiv:1702.04267.

[131] Metzen, J.H., Genewein, T., Fischer, V., Bischoff, B., 2017b. On detecting adversarial perturbations. arXiv:1702.04267.

[132] Meutzner, H., Kolossa, D., 2016. A non-speech audio captcha based on acoustic event detection and classification, in: 2016 24th European Signal Processing Conference (EUSIPCO), IEEE. pp. 2250–2254.

[133] Moore, J., Hammerla, N., Watkins, C., 2019. Explaining deep learning models with constrained adversarial examples. CoRR abs/1906.10671. URL: http://arxiv.org/abs/1906.10671, arXiv:1906.10671.

[134] Moosavi-Dezfooli, S.M., Fawzi, A., Fawzi, O., Frossard, P., 2017. Universal adversarial perturbations, in: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1765–1773.

[135] Moosavi-Dezfooli, S.M., Fawzi, A., Frossard, P., 2016. Deepfool: a simple and accurate method to fool deep neural networks, in: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 2574–2582.

[136] Morris, R., Thompson, K., 1979. Password security: A case history. Communications of the ACM 22, 594–597.

[137] Nagarsheth, P., Khoury, E., Patil, K., Garland, M., 2017. Replay attack detection using dnn for channel discrimination, pp. 97–101. doi:10.21437/Interspeech.2017-1377.

[138] Nguyen, A., Yosinski, J., Clune, J., 2015. Deep neural networks are easily fooled: High confidence predictions for unrecognizable images, in: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 427–436.

[139] Nguyen, D.T., Baek, N.R., Pham, T.D., Park, K.R., 2018. Presentation attack detection for iris recognition system using nir camera sensor. Sensors 18. URL: https://www.mdpi.com/1424-8220/18/5/1315, doi:10.3390/s18051315.

[140] Nikam, S.B., Agarwal, S., 2009. Wavelet-based multiresolution analysis of ridges for fingerprint liveness detection. Int. J. Inf. Comput. Secur. 3, 1–46.

[141] Nugroho, A.R., Li, Q., 2017. Inferring mobile apps from resource usage patterns, in: 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), IEEE. pp. 82–87.

[142] Nugroho, E.P., Putra, R.R.J., Ramadhan, I.M., 2016. Sms authentication code generated by advance encryption standard (aes) 256 bits modification algorithm and one time password (otp) to activate new applicant account, in: 2016 2nd International Conference on Science in Information Technology (ICSITech), IEEE. pp. 175–180.

[143] Ojala, T., Pietikainen, M., Maenpaa, T., 2002. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Transactions on Pattern Analysis and Machine Intelligence 24, 971–987. doi:10.1109/TPAMI.2002.1017623.

[144] Otsuka, A., 2013. Wolf attack: Algorithmic vulnerability in biometric authentication systems, in: 2013 International Conference on Biometrics and Kansei Engineering, IEEE. pp. 309–313.

[145] Pacut, A., Czajka, A., 2006. Aliveness detection for iris biometrics, in: Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology, pp. 122–129. doi:10.1109/CCST.2006.313440.

[146] Pan, G., Sun, L., Wu, Z., Lao, S., 2007a. Eyeblink-based anti-spoofing in face recognition from a generic webcamera, in: 2007 IEEE 11th international conference on computer vision, IEEE. pp. 1–8.

[147] Pan, G., Sun, L., Wu, Z., Lao, S., 2007b. Eyeblink-based anti-spoofing in face recognition from a generic webcamera, in: 2007 IEEE 11th international conference on computer vision, IEEE. pp. 1–8.

[148] Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z.B., Swami, A., 2016. The limitations of deep learning in adversarial settings, in: 2016 IEEE European symposium on security and privacy (EuroS&P), IEEE. pp. 372–387.

[149] Papernot, N., McDaniel, P.D., Wu, X., Jha, S., Swami, A., 2015. Distillation as a defense to adversarial perturbations against deep neural networks. CoRR abs/1511.04508. URL: http://arxiv.org/abs/1511.04508, arXiv:1511.04508.

[150] Parthasaradhi, S.T.V., Derakhshani, R., Hornak, L.A., Schuckers, S.A.C., 2005. Time-series detection of perspiration as a liveness test in fingerprint devices. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 35, 335–343. doi:10.1109/TSMCC.2005.848192.

[151] Pirlo, G., Cuccovillo, V., Diaz-Cabrera, M., Impedovo, D., Mignone, P., 2015a. Multidomain verification of dynamic signatures using local stability analysis. IEEE Transactions on Human-Machine Systems 45, 805–810. doi:10.1109/THMS.2015.2443050.

[152] Pirlo, G., Cuccovillo, V., Diaz-Cabrera, M., Impedovo, D., Mignone, P., 2015b. Multidomain verification of dynamic signatures using local stability analysis. IEEE Transactions on Human-Machine Systems 45, 805–810. doi:10.1109/THMS.2015.2443050.

[153] Potamianos, G., 2009. Audio-visual automatic speech recognition and related bimodal speech technologies: A review of the state-of-the-art and open problems, in: 2009 IEEE Workshop on Automatic Speech Recognition Understanding, pp. 22–22. doi:10.1109/ASRU.2009.5373530.

[154] Potamianos, G., Neti, C., Luettin, J., Matthews, I., . Audio-visual automatic speech recognition: An overview, p. 23.

[155] Raghavendra, R., Busch, C., 2015. Robust scheme for iris presentation attack detection using multiscale binarized statistical image features. IEEE Transactions on Information Forensics and Security 10, 703–715. doi:10.1109/TIFS.2015.2400393.

[156] Rahman, M., Topkara, U., Carbunar, B., 2015. Movee: Video live-

ness verification for mobile devices using built-in motion sensors. IEEE Transactions on Mobile Computing 15, 1197–1210.

[157] Ranjan, R., Bansal, A., Zheng, J., Xu, H., Gleason, J., Lu, B., Nanduri, A., Chen, J.C., Castillo, C.D., Chellappa, R., 2019. A fast and accurate system for face detection, identification, and verification. IEEE Transactions on Biometrics, Behavior, and Identity Science 1, 82–96.

[158] Rao, K., Sri, K., Sai, G., 2016. A novel video captcha technique to prevent bot attacks. Procedia Computer Science 85, 236–240.

[159] Ratha, N.K., Connell, J.H., Bolle, R.M., 2001a. An analysis of minutiae matching strength, in: International Conference on Audio-and Video-Based Biometric Person Authentication, Springer. pp. 223–228.

[160] Ratha, N.K., Connell, J.H., Bolle, R.M., 2001b. An analysis of minutiae matching strength, in: International Conference on Audio-and Video-Based Biometric Person Authentication, Springer. pp. 223–228.

[161] Ratha, N.K., Connell, J.H., Bolle, R.M., 2001. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40, 614–634. doi:10.1147/sj.403.0614.

[162] Robertson, D.J., Kramer, R.S., Burton, A.M., 2017. Fraudulent id using face morphs: Experiments on human and automatic recognition. PLoS One 12, e0173319.

[163] Rodrigues, R.N., Kamat, N., Govindaraju, V., 2010. Evaluation of biometric spoofing in a multimodal system, in: 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp. 1–5. doi:10.1109/BTAS.2010.5634531.

[164] Roth, V., Richter, K., Freidinger, R., 2004. A pin-entry method resilient against shoulder surfing, in: Proceedings of the 11th ACM conference on Computer and communications security, pp. 236–245.

[165] Safavi, S., Gan, H., Mporas, I., Sotudeh, R., 2016. Fraud detection in voice-based identity authentication applications and services, in: 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW), pp. 1074–1081. doi:10.1109/ICDMW.2016.0155.

[166] Sanfeliu, A., Alquezar, R., 1992. Understanding neural networks for grammatical inference and recognition, in: Advances in Structural and Syntactic Pattern Recognition. World Scientific, pp. 75–98.

[167] d. Santana, L.M.Q., Santos, R.M., Matos, L.N., Macedo, H.T., 2018. Deep neural networks for acoustic modeling in the presence of noise. IEEE Latin America Transactions 16, 918–925. doi:10.1109/TLA.2018.8358674.

[168] Seyed, T., Yang, X.D., Tang, A., Greenberg, S., Gu, J., Zhu, B., Cao, X., 2015. Ciphercard: A token-based approach against camera-based shoulder surfing attacks on common touchscreen devices, in: IFIP Conference on Human-Computer Interaction, Springer. pp. 436–454.

[169] Sharif, M., Bhagavatula, S., Bauer, L., Reiter, M.K., 2016. Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition, in: Proceedings of the 2016 acm sigsac conference on computer and communications security, pp. 1528–1540.

[170] Shen, S., Tople, S., Saxena, P., 2016. Auror: Defending against poisoning attacks in collaborative deep learning systems, in: Proceedings of the 32nd Annual Conference on Computer Security Applications, Association for Computing Machinery, New York, NY, USA. p. 508–519. URL: https://doi.org/10.1145/2991079.2991125, doi:10.1145/2991079.2991125.

[171] Shreyas, K.K., Rajeev, S., Panetta, K., Agaian, S.S., 2017. Fingerprint authentication using geometric features, in: 2017 IEEE International Symposium on Technologies for Homeland Security (HST), IEEE. pp. 1–7.

[172] Shunmugam, S., Selvakumar, R.K., 2014. Electronic transaction authentication — a survey on multimodal biometrics, in: 2014 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1–4. doi:10.1109/ICCIC.2014.7238509.

[173] Singh, A.K., Joshi, P., Nandi, G.C., 2014. Face recognition with liveness detection using eye and mouth movement, in: 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014), IEEE. pp. 592–597.

[174] Singh, Y.N., Singh, S.K., 2011. Vitality detection from biometrics: state-of-the-art, in: 2011 World Congress on Information and Communication Technologies, IEEE. pp. 106–111.

[175] Singh, Y.N., Singh, S.K., 2013. A taxonomy of biometric system vulnerabilities and defences. International journal of biometrics 5, 137–159.

[176] Sousedik, C., Busch, C., 2014. Presentation attack detection methods for fingerprint recognition systems: a survey. Iet Biometrics 3, 219–233.

[177] Steinhardt, J., Koh, P.W.W., Liang, P.S., 2017. Certified defenses for data poisoning attacks, in: Advances in neural information processing systems, pp. 3517–3529.

[178] Su, J., Vargas, D.V., Sakurai, K., 2019a. One pixel attack for fooling deep neural networks. IEEE Transactions on Evolutionary Computation 23, 828–841.

[179] Su, J., Vargas, D.V., Sakurai, K., 2019b. One pixel attack for fooling deep neural networks. IEEE Transactions on Evolutionary Computation 23, 828–841.

[180] Suo, X., Zhu, Y., Owen, G.S., 2005. Graphical passwords: A survey, in: 21st Annual Computer Security Applications Conference (ACSAC'05), IEEE. pp. 10–pp.

[181] Szwoch, M., Pieniążek, P., 2012a. Eye blink based detection of liveness in biometric authentication systems using conditional random fields, in: International Conference on Computer Vision and Graphics, Springer. pp. 669–676.

[182] Szwoch, M., Pieniążek, P., 2012b. Eye blink based detection of liveness in biometric authentication systems using conditional random fields, in: International Conference on Computer Vision and Graphics, Springer. pp. 669–676.

[183] Tabacof, P., Valle, E., 2016. Exploring the space of adversarial images, in: 2016 International Joint Conference on Neural Networks (IJCNN), IEEE. pp. 426–433.

[184] Tan, B., Schuckers, S., 2006a. Comparison of ridge- and intensity-based perspiration liveness detection methods in fingerprint scanners, in: Flynn, P.J., Pankanti, S. (Eds.), Biometric Technology for Human Identification III, International Society for Optics and Photonics. SPIE. pp. 94 – 103. URL: https://doi.org/10.1117/12.666415, doi:10.1117/12.666415.

[185] Tan, B., Schuckers, S., 2006b. Comparison of ridge-and intensity-based perspiration liveness detection methods in fingerprint scanners, in: Biometric Technology for Human Identification III, International Society for Optics and Photonics. p. 62020A.

[186] Tan, B., Schuckers, S., 2010. Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. Pattern Recognition 43, 2845–2857. URL: https://www.sciencedirect.com/science/article/pii/S0031320310000993, doi:https://doi.org/10.1016/j.patcog.2010.01.023.

[187] Tan, B., Schuckers, S.C., 2008. New approach for liveness detection in fingerprint scanners based on valley noise analysis. Journal of Electronic Imaging 17, 011009.

[188] Thompson, S.C., 2005. Scamblocker. The Journal of the American Taxation Association 27, 113.

[189] Une, M., Otsuka, A., Imai, H., 2007a. Wolf attack probability: A new security measure in biometric authentication systems, in: International Conference on Biometrics, Springer. pp. 396–406.

[190] Une, M., Otsuka, A., Imai, H., 2007b. Wolf attack probability: A new security measure in biometric authentication systems, in: International Conference on Biometrics, Springer. pp. 396–406.

[191] Vidhyapriya, R., et al., 2019. Personal authentication mechanism based on finger knuckle print. Journal of medical systems 43, 1–7.

[192] Villalba, J., Lleida, E., 2011. Detecting replay attacks from far-field recordings on speaker verification systems, in: Vielhauer, C., Dittmann, J., Drygajlo, A., Juul, N.C., Fairhurst, M.C. (Eds.), Biometrics and ID Management, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 274–285.

[193] Wang, P., Lin, W.H., Chao, K.M., Lo, C.C., 2017a. A face-recognition approach using deep reinforcement learning approach

for user authentication, in: 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), IEEE. pp. 183–188.

[194] Wang, X., Shrivastava, A., Gupta, A., 2017b. A-fast-rcnn: Hard positive generation via adversary for object detection, in: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 2606–2615.

[195] Weng, T.W., Zhang, H., Chen, P.Y., Yi, J., Su, D., Gao, Y., Hsieh, C.J., Daniel, L., 2018. Evaluating the robustness of neural networks: An extreme value theory approach. arXiv preprint arXiv:1801.10578 .

[196] Witkowski, M., Kacprzak, S., Żelasko, P., Kowalczyk, K., Gałka, J., 2017. Audio replay attack detection using high-frequency features, pp. 27–31. doi:10.21437/Interspeech.2017-776.

[197] Wu, Z., Yamagishi, J., Kinnunen, T., Hanilçi, C., Sahidullah, M., Sizov, A., Evans, N., Todisco, M., Delgado, H., 2017. Asvspoof: the automatic speaker verification spoofing and countermeasures challenge. IEEE Journal of Selected Topics in Signal Processing 11, 588–604.

[198] Xie, C., Wang, J., Zhang, Z., Zhou, Y., Xie, L., Yuille, A., 2017. Adversarial examples for semantic segmentation and object detection, in: Proceedings of the IEEE International Conference on Computer Vision, pp. 1369–1378.

[199] Xie, Z., Tie, Y., Guan, L., 2015. A new audiovisual emotion recognition system using entropy-estimation-based multimodal information fusion, in: 2015 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE. pp. 726–729.

[200] Yadav, D., Kohli, N., Agarwal, A., Vatsa, M., Singh, R., Noore, A., 2018. Fusion of handcrafted and deep learning features for large-scale multiple iris presentation attack detection, in: 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 685–6857. doi:10.1109/CVPRW.2018.00099.

[201] Yan, Z., Zhao, S., 2016. A usable authentication system based on personal voice challenge, in: 2016 International Conference on Advanced Cloud and Big Data (CBD), IEEE. pp. 194–199.

[202] Yau, W., Tran, H., Teoh, E., 2008. Fake finger detection using an electrotactile display system, in: 2008 10th International Conference on Control, Automation, Robotics and Vision, pp. 962–966. doi:10.1109/ICARCV.2008.4795648.

[203] Ye, H., Huang, Z., Fang, C., Li, C.J., Zhang, T., 2018. Hessian-aware zeroth-order optimization for black-box adversarial attack. arXiv preprint arXiv:1812.11377 .

[204] Yu, P., Song, K., Lu, J., 2018. Generating adversarial examples with conditional generative adversarial net, in: 2018 24th International Conference on Pattern Recognition (ICPR), IEEE. pp. 676–681.

[205] Yuan, X., He, P., Zhu, Q., Li, X., 2019. Adversarial examples: Attacks and defenses for deep learning. IEEE transactions on neural networks and learning systems 30, 2805–2824.

[206] Zhang, C., Lam, K.Y., Jajodia, S., 1999. Scalable threshold closure. Theoretical Computer Science 226, 185–206. URL: https://www.sciencedirect.com/science/article/pii/S0304397599000729, doi:https://doi.org/10.1016/S0304-3975(99)00072-9.

[207] Zhang, H., Sun, Z., Tan, T., 2010. Contact lens detection based on weighted lbp, in: 2010 20th International Conference on Pattern Recognition, pp. 4279–4282. doi:10.1109/ICPR.2010.1040.

[208] Zhang, L., Tan, S., Yang, J., 2017. Hearing your voice is not enough: An articulatory gesture based liveness detection for voice authentication, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 57–71.

[209] Zhang, L., Tan, S., Yang, J., Chen, Y., 2016a. Voicelive: A phoneme localization based liveness detection for voice authentication on smartphones, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1080–1091.

[210] Zhang, L., Tan, S., Yang, J., Chen, Y., 2016b. Voicelive: A phoneme localization based liveness detection for voice authentication on smartphones, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, New York, NY, USA. p. 1080–1091. URL: https://doi.org/10.1145/2976749.2978296, doi:10.1145/2976749.2978296.

[211] Zhang, R., Yan, Z., 2019. A survey on biometric authentication: Toward secure and privacy-preserving identification. IEEE Access 7, 5994–6009. doi:10.1109/ACCESS.2018.2889996.

[212] Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D., Li, S.Z., 2012. A face antispoofing database with diverse attacks, in: 2012 5th IAPR international conference on Biometrics (ICB), IEEE. pp. 26–31.

[213] Zhang, Z., Yi, D., Lei, Z., Li, S.Z., 2011. Face liveness detection by learning multispectral reflectance distributions, in: Face and Gesture 2011, IEEE. pp. 436–441.

[214] Zhao, Z., Dua, D., Singh, S., 2017. Generating natural adversarial examples. arXiv preprint arXiv:1710.11342 .

[215] Zheng, W., Jia, C., 2017. Combinedpwd: A new password authentication mechanism using separators between keystrokes, in: 2017 13th International Conference on Computational Intelligence and Security (CIS), IEEE. pp. 557–560.

[216] Ziyad, S., Sampathkumar, K., 2014. A Multifactor Biometric Authentication for the Cloud. pp. 395–403. doi:10.1007/978-81-322-1680-3_43.

Xuerui Wang received the B.E. degree in Computer Science and Technology from Xidian University, Xi'an, China, 2018. She is currently pursuing the master degree in Xidian University in Xi'an, China. Her main research interests are attacks and defense in authentication systems.

Zheng Yan (M'06-SM'14) is currently a professor at the Xidian University, China and a visiting professor and Finnish academy research fellow at the Aalto University, Finland. She received the Doctor of Science in Technology from the Helsinki University of Technology, Finland. Her research interests are in trust, security, privacy, and security-related data analytics. She is an associate editor of IEEE Internet of Things Journal, Information Fusion, Information Sciences, IEEE Access, and JNCA. She served as a general chair or program chair for over 30 international conferences including IEEE TrustCom 2015. She is a founding steering committee co-chair of IEEE Blockchain conference. She received several awards, including the Distringuished Inventor Award issued by Nokia (2020), the Aalto ELEC Impact Award (2021), the 2017 Best Journal Paper Award issued by IEEE Communication Society Technical Committee on Big Data and the Outstanding Associate Editor of 2017/2018 for IEEE Access.

Rui Zhang received the B.Sc. degree in Computer Science and Technology from CUMT, Xuzhou, China, in 2016. Now she is major in information security and studying for a PhD in Xidian University in Xi'an, China. Her research interests are in information security, authentication and privacy preserving in social network.

Peng Zhang received the Ph.D. degree in computer and communication engineering from the Beijing University of Posts and Telecommunications, China. He conducted his post-doctoral research at the Helsinki University of Technology from 1999 to 2001. He is currently a Computer Scientist with an interest in trust and mobile services. He has published more than 70 papers and invented 10 granted patents. He also served as an organization committee member for numerous international conferences and a reviewer for many prestigious journals.