Biometric Liveness Detection: Challenges and Research Opportunities

Article *in* IEEE Security and Privacy Magazine · September 2015

DOI: 10.1109/MSP.2015.116

Zahid Akhtar
State University of New York Polytechnic Institute

Christian Micheloni
University of Udine

G.L. Foresti
University of Udine

Biometric Liveness Detection: Challenges and Research Opportunities

Zahid Akhtar, Christian Micheloni, and Gian Luca Foresti | University of Udine

In a biometric spoofing attack, an impostor masquerades as a legitimate user by replicating that user's biometrics. Although methods exist to determine whether a live person or biometric artifact is in front of a biometric sensor, spoofing attacks remain a problem.

The term *biometrics* comes from the ancient Greek words *bios* (life) and *metrikos* (measure) and refers to recognizing people on the basis of anatomical or behavioral characteristics. Unlike conventional person identification methods, biometrics is based on "who you are" rather than "what you have" (such as an ID card) or "what you know" (such as a password). Biometrics is often required for government-controlled activities such as border crossings (see Figure 1), as well as by private institutions such as banks. Moreover, many mobile devices now use biometrics instead of passwords. For example, the iPhone 5s uses fingerprints, and Android phones use face recognition.

Essentially, a biometric system is a pattern-recognition system that

- senses a specific physiological or behavioral biometric signal,
- processes the signal to extract a set of salient features,
- compares these features against the feature set (template) stored in a database, and
- makes a decision about the identity of the person inputting the biometric signal.

Figure 2 shows the phases of biometric enrollment and verification.

Despite their many advantages, biometric systems, like any other security application, are vulnerable to a range of attacks. People usually attack biometric systems to disguise their identity, attain another person's privileges, or share a biometric and its subsequent benefits. (As an example of the third case, someone could first create an identity using a computer-generated, synthetic biometric during enrollment. Then, that person would share that identity with multiple people by sharing the synthetic biometric.)

Here, we review types of attacks on biometric systems; discuss the challenges of liveness detection methods for countering those attacks; and explore research opportunities for developers, researchers, and policymakers.

Types of Attacks

Attacks on biometric systems fall broadly into two categories: *presentation attacks* (direct attacks) and *indirect attacks*.[1]

Presentation attacks are defined as "presentation of an artifact or human characteristic to the biometric capture subsystem with the goal of interfering with the operation of the biometric system."[2] They occur externally at the sensor level (point 1 in Figure 3). So, they don't involve digital protection techniques such as hashing, encryption, and digital signatures.

On the other hand, intruders (for example, cybercriminals or hackers) perform indirect attacks inside the system by

- bypassing the feature extractor (point 3 in Figure 3) or matcher (point 5 in Figure 3),

1540-7993/15/$31.00 © 2015 IEEE

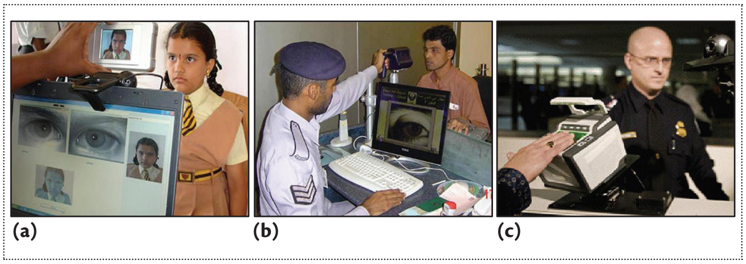

Figure 1. Three biometric systems. (a) A face and iris recognition system used by the Unique Identification Authority of India to identify all Indian residents. (b) An iris recognition system used in the United Arab Emirates' border-crossing and expellee-tracking systems. (Source: John Daugman; used with permission.) (c) A fingerprint recognition system used by the US Visitor and Immigration Status Indicator Technology Program. (Source: Crossmatch; used with permission.)

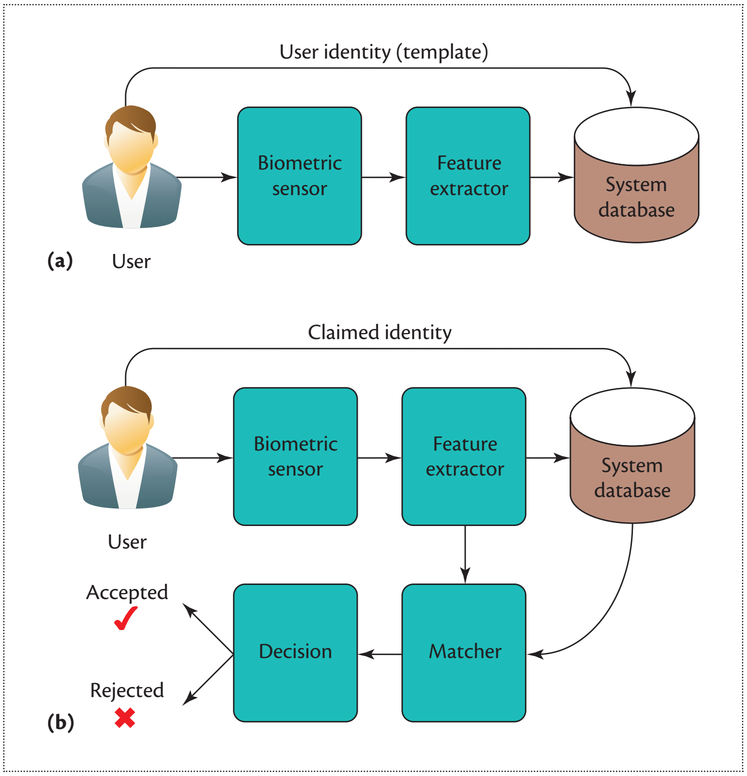

Figure 2. Biometric enrollment and verification. (a) The enrollment phase produces an association between a biometric characteristic and its identity. (b) In the verification phase, an enrolled user claims an identity, which the system verifies on the basis of the user's biometric feature set.

- manipulating templates in the database (point 6 in Figure 3), or
- exploiting possible weak points in the communication channels (points 2, 4, 7, and 8 in Figure 3).

Clearly, indirect attacks require advanced programming skills.

Spoofing Attacks

With the large-scale deployment of biometric systems, the threat of presentation attacks has grown. In particular, in a *spoofing attack*, an impostor masquerades as a legitimate user by replicating that user's biometrics, thereby gaining illegitimate access and advantages. Spoofing attacks have great practical relevance because they don't require advanced technical skills; therefore, the potential number of attackers is large. The US National Institute of Standards and Technology now lists the vulnerability of biometrics to spoofing in its National Vulnerability Database.

Many types of biometrics are vulnerable to direct attacks. For example, as Figure 4 shows, the face, iris, and fingerprint images captured from a spoofing attack look similar to the images captured from the real user.

Spoofing attacks are a major issue for companies selling biometric-based identity management solutions. For instance, in 2013, doctors at the Ferraz de Vasconcelos hospital in Brazil were caught using fake silicone fingers to defraud the hospital's biometric punch-in clock to get overtime (see Figure 5a). Figures 5b and 5c describe other recent spoofing attacks.

Despite the recent advances in biometrics on mobile devices, their vulnerability to spoofing attacks has been largely overlooked. For example, in 2013, the German hacker group Chaos Computer Club demonstrated that an artificial fingerprint could fool the iPhone 5s's fingerprint scanner.

Countermeasures

To make biometric applications practical, the threat of presentation attacks must be urgently addressed. The countermeasure to such attacks is equipping systems with a *presentation attack detection* (PAD) method.[2] One PAD method is *liveness detection*, which assumes that an attacker pretending to be a legitimate user is intruding on the system by felonious biometric means. (In this article, we use the terms PAD and liveness detection interchangeably, unless we explicitly state otherwise.)

PAD operates in four modes (see Figure 6):

- using available sensors to detect patterns characteristic of attacks in the signal,
- using dedicated sensors to detect evidence of genuineness (which isn't always feasible),
- using challenge–response techniques that ask users to interact with the system, and
- using recognition techniques that are intrinsically robust against presentation attacks.

Multimodal biometric systems are commonly believed to be more intrinsically robust against spoofing

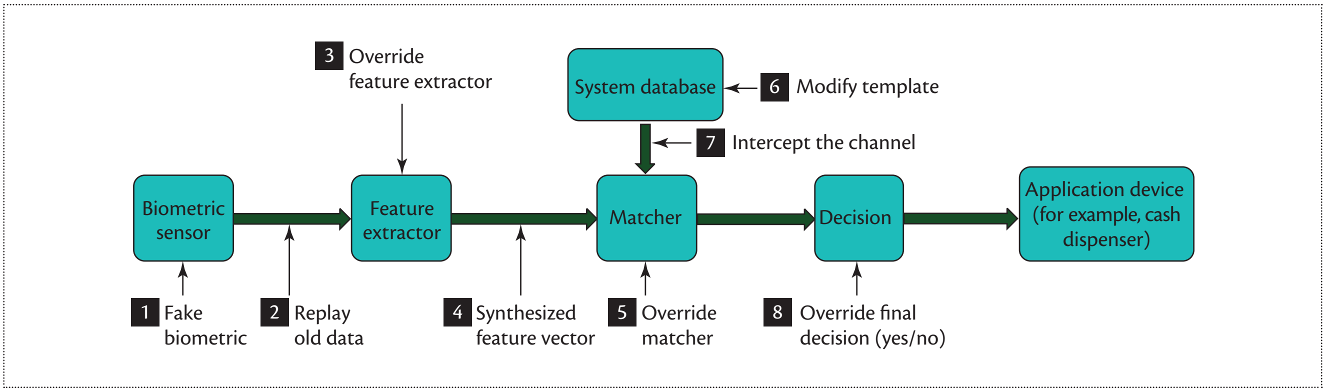

Figure 3. Eight points of attack on a generic biometric system. People usually attack biometric systems to disguise their identity, attain another person's privileges, or share a biometric and its subsequent benefits.

attacks. However, recent research showed that attackers can evade such systems by spoofing even a single biometric trait.[3]

Liveness detection can either be hardware based, which requires additional hardware, or software based, which uses signal-processing algorithms and is therefore cheaper and noninvasive. Following is an overview of the most commonly used biometric traits—face, fingerprint, and iris—and their software-based liveness detection methods.

Face Spoofing

Despite progress in its detection, face spoofing still poses a serious threat to face recognition systems. These systems might be spoofed by a photograph, a video, a 3D face model (mask), a sketch, a reverse-engineered face image based on the legitimate user's face, or makeup or plastic surgery that makes an impostor look like the legitimate user (see Figure 7).

Face liveness detection methods can be coarsely classified as *motion analysis* or *texture analysis*. Motion analysis detects the spontaneous movement clues generated when an attacker presents 2D counterfeits, such as photographs or videos, to the system. For instance, one research group, building on the fact that humans blink every 2 to 4 seconds, proposed eye blink–based liveness detection for photo-based spoofing.[1]

Other researchers have used Lambertian[4] and variational Retinex reflectance models[5] to differentiate between spoofed and live faces. Still other spoofing-detection methods use optical flow or scene context matching.

Texture analysis examines skin properties, such as texture and reflectance, under the assumption that the surface properties of real faces and prints (pigments) differ. In one study, microtexture analysis was exploited to detect spoofs using printed photos.[1]

Other methods have used differences in the 2D Fourier spectra of live and fake images, but such methods will likely fail for higher-quality samples. Further countermeasures are based on multispectral imaging, which analyzes object surfaces' reflectance.

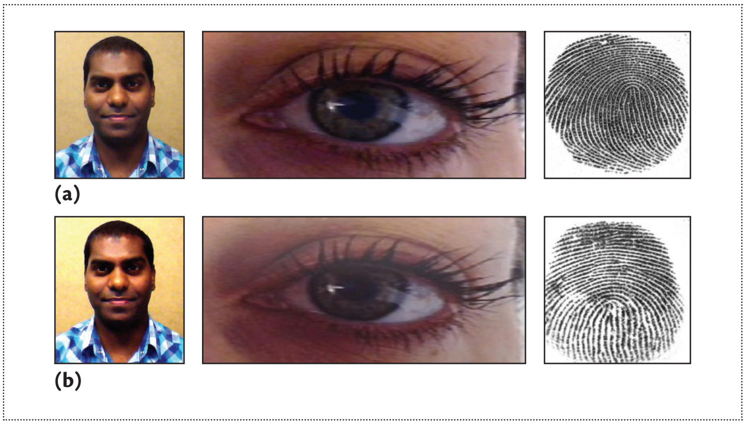

Figure 4. Sample images captured from (a) a real face, iris, and fingerprint and (b) a spoofing attack. The similarity between the real and spoofed images demonstrates why detecting spoofing attacks is so difficult.

Fingerprint Spoofing

Fingerprint spoofing is an old practice. Fingerprint recognition systems can be fooled by a 2D (flat) fake fingerprint, a synthesized 3D fake fingerprint, a reverse-engineered image based on the legitimate user's fingerprint, or even a cadaver fingerprint or finger cut from the legitimate user (see Figure 8). (In a rather violent example, in 2005, a gang in Kuala Lumpur chopped off a car owner's finger to disarm the car's high-tech security system.)

Fake fingerprints can be fabricated consensually or nonconsensually using readily available materials such as gelatin. In the consensual method (also called *cooperative* or *direct casts*), the user lets someone create spoofed fingerprints directly from his or her real fingers. In the nonconsensual method (also called *noncooperative* or *indirect*

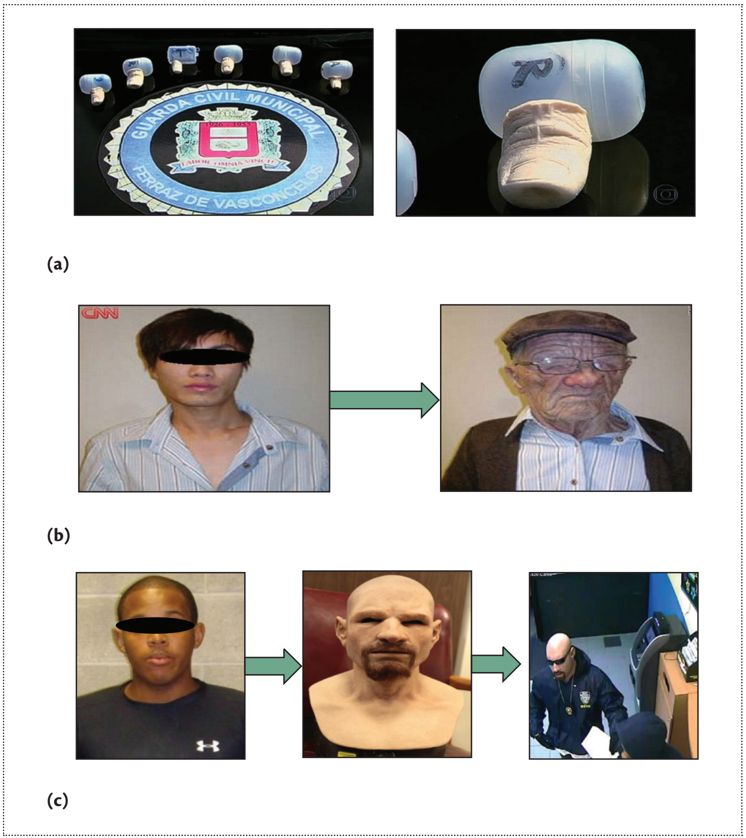

Figure 5. Examples of spoofing attacks. (a) In Brazil, doctors used fake silicone fingers to defraud a hospital's biometric punch-in clock. (b) In Hong Kong, a young passenger boarded a plane while wearing an old-man mask and arrived in Canada to claim asylum. (Source: CBS News; used with permission.) (c) In New York, an African American man wore a silicone mask to disguise himself as a white police officer to rob a check-cashing store. (Source: Composite Effects/CFX; used with permission.)

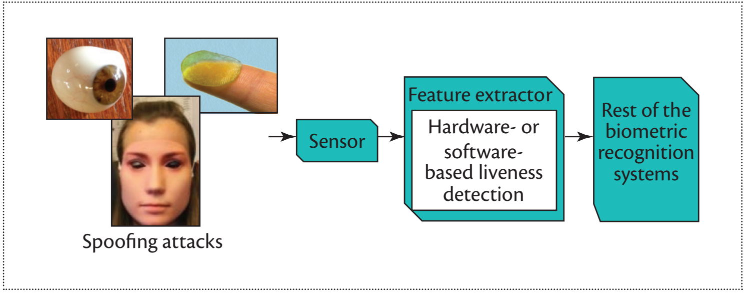
Spoofing attacks
Sensor
Feature extractor
Hardware- or software-based liveness detection
Rest of the biometric recognition systems

Figure 6. Spoofing attacks might be detected by hardware- or software-based liveness detection methods. Software-based methods are inexpensive and noninvasive because they use signal-processing algorithms.

casts), someone takes the spoofed prints from the user's latent fingermarks, hence not requiring their cooperation.

Fingerprint liveness detection methods can be based on perspiration, skin deformation, image quality, pores, or a combination thereof. Perspiration-based methods analyze the fingerprint's perspiration pattern. Sujan Parthasaradhi and his colleagues proposed a time-consuming method to detect spoofed fingerprints by measuring the finger's perspiration process.[6]

Skin deformation–based methods exploit skin elasticity. For instance, thin-plate splines have been used to capture finger distortion.[7] Such methods require special training.

Image quality–based methods use image quality or texture properties. For example, Javier Galbally and his colleagues proposed a method based on 10 quality measures, including ridge strength, continuity, and clarity.[8] Luca Ghiani and his colleagues exploited local phase quantization texture features for liveness detection.[9]

Pore-based methods detect pores as a sign of fingerprint vitality. These methods typically use high-pass and correlation filtering.

Iris Spoofing

Iris recognition is generally conceded to be the most accurate person identification method.[10] However, iris recognition systems could be deceived by an iris photograph or video, a printed contact lens, a glass or plastic artificial eyeball, a reverse-engineered iris image based on the legitimate user's iris, or a real eye removed from the legitimate user's body (see Figure 9).

Iris liveness detection methods can be broadly categorized as *frequency spectrum analysis*, *reflectance analysis*, *dynamics analysis*, or *texture analysis*. Frequency spectrum analysis assumes that frequency artifacts exist in the images of spoofing attacks. John Daugman proposed using spectrographic analysis to detect a printed iris.[11] However, this method fails if the printed spoof's resolution is twice that of the biometric system's camera.

Reflectance analysis illuminates the eye with multiple light wavelengths and compares the relative response in the sclera and iris.

Dynamics analysis acquires several images while manipulating the illumination level to assess pupil dilation changes. For instance, Galbally and his colleagues used motion features with image quality properties caused by either the iris's or the sensor's motion.[12]

Texture analysis classifies texture features to determine forgery. For example, one investigative team analyzed the statistical texture of four distinct features to detect spoofed contact lenses.[1]

Finally, another group of researchers developed a method (using a human eye model) for fake iris detection based on Purkinje images, but this method tends to fail for contact lenses.[10]

Research Opportunities

A recent systematic analysis revealed that no existing spoofing countermeasure has achieved a very low error rate.[1] The ever-increasing demand for reduced PAD failure rates has opened up interesting research opportunities across multiple domains.

A Performance Evaluation Framework

Classification accuracy deals with such fundamental problems as how to evaluate, configure, or compare PADs. So, we need a comprehensive evaluation framework to rate PAD performance. Researchers might be able to achieve this by

- designing protocols and tools for attack detection (vulnerability analysis) of PADs (biometric recognition systems);
- developing standardized common criteria; and
- developing an online, open platform to transparently and independently evaluate systems against validated benchmarks.

The call to design new protocols and tools should encourage researchers to not only propose new method-, matrix-, and security-relevant error rates for attacks but also introduce a unified framework and common vocabulary for discussing PAD performance. Protocols should establish a baseline for developing and testing effective countermeasures against known and unknown attacks. Moreover, equal attention must be paid to performance metrics that distinguish the false acceptance of an impostor as genuine in biometric recognition from the false acceptance of a spoofing attack as genuine in PAD. Finally, protocols must incorporate sociocultural factors such as users' privacy, perceptions, dress, and lifestyle.

Common criteria for evaluating spoofability, attack sophistication, decision making, and policies will help us report baseline operations without giving a false sense of progress. Germany's Federal Office for Information Security (www.bsi.bund.de), an independent certification body, is developing such criteria.

The present "reproducible research" trend should also be encouraged through large public databases, open source software, and experimental setups. Such resources will greatly benefit studies on scalability and challenges in real-world applications.

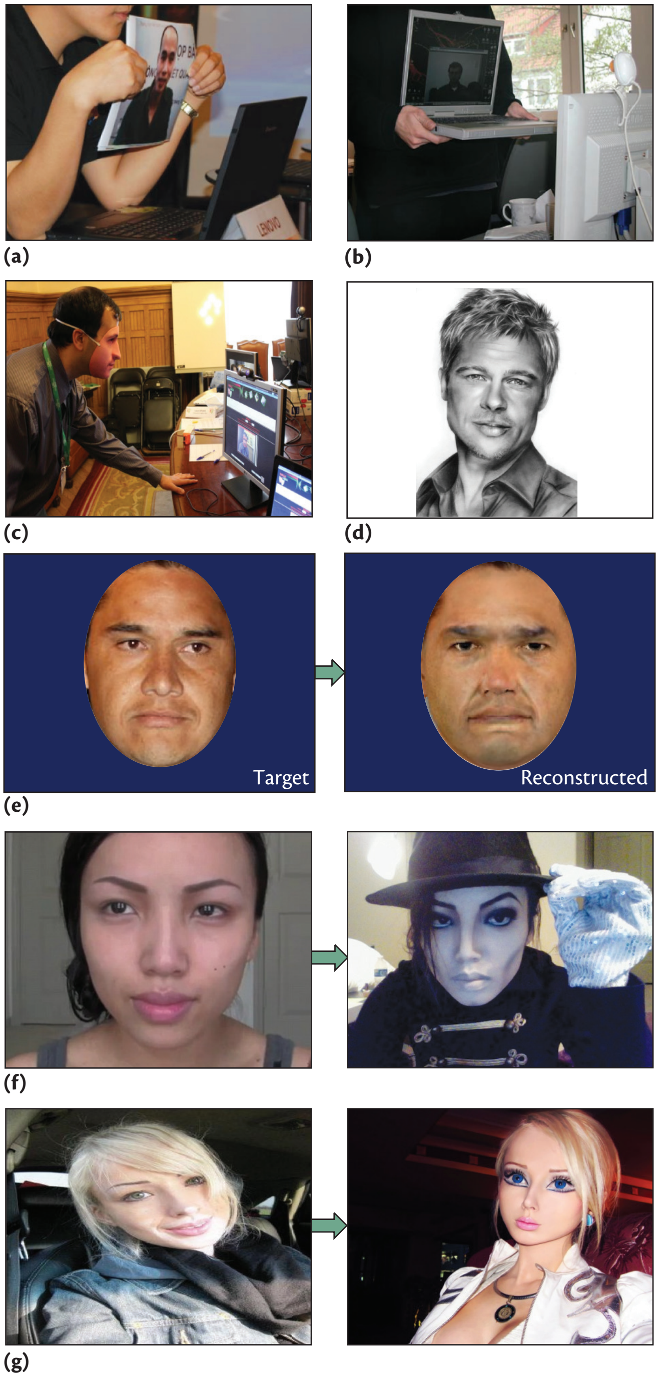

Figure 7. Face spoofing can be achieved using (a) a photograph, (b) a video, (c) a 3D mask (Source: Sébastien Marcel; used with permission), (d) a sketch, (e) a reverse-engineered face image, (f) makeup, and (g) excessive plastic surgery (here, to look like a doll).

Standardization of Liveness Detection

Biometric standards are the general rules for collecting, evaluating, storing, and sharing biometrics.[1] No international standard exists for liveness detection, although the International Organization for Standardization (ISO) is working on one.[2] It's vital to establish precise standards to capitalize on the use of biometric technologies. Moreover, as government agencies and top-level decision makers weigh the risks of attacks against the convenience of security mechanisms, they must understand the need for appropriate biometric standards to test vulnerability and certification.

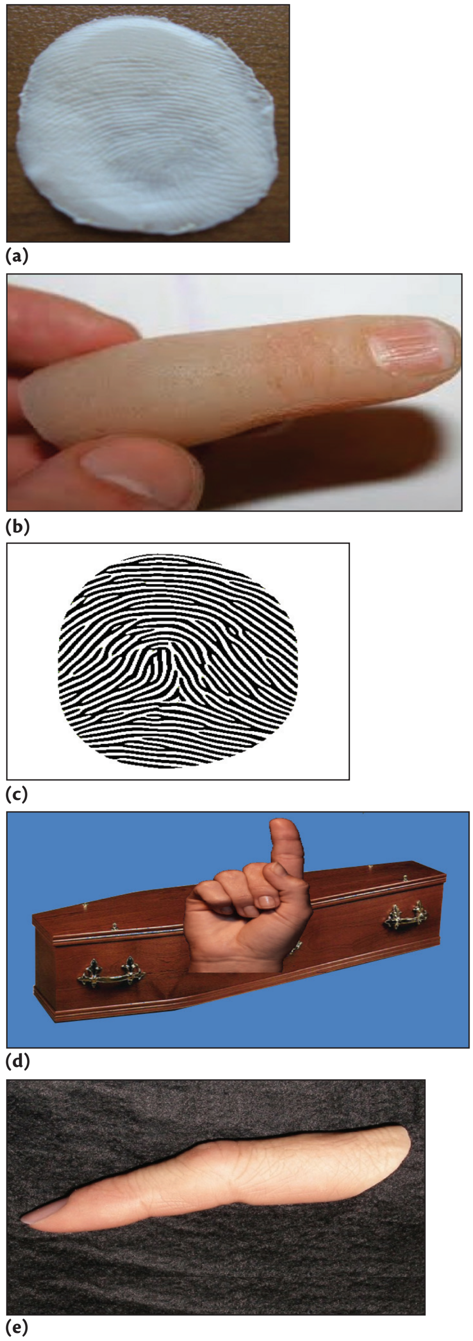

Figure 8. Fingerprint spoofing can be achieved using (a) a 2D (flat) fake silicone fingerprint, (b) a synthesized 3D fake fingerprint, (c) a reverse-engineered fingerprint image, (d) a cadaver fingerprint, or (e) part of a finger.

Mobile Liveness Detection

A recent industry survey estimated that by 2018, almost 3.4 billion users will access biometrics on their devices.[13] Existing liveness detection methods are unsuited for mobile applications because of the complex features they analyze or high computational cost. So, to make such applications more practical, researchers must address the issue of presentation attacks on mobile devices.

Spoof Material–Invariant Liveness Detection

Ajita Rattani and Arun Ross reported that a liveness detection algorithm's performance degrades remarkably when it encounters unfamiliar spoof fabrication materials.[14] Liveness detection systems are often based on unrealistic, a priori known spoof fabrication materials. This limits their application in the real world, where the nature of attacks is unpredictable.

So, researchers need to develop generalized liveness detection methods that detect varying or previously unseen spoofing attacks. Although training PADs with all possible materials and techniques is infeasible, one alternative might be to devise mathematical models of spoofs characterized by different materials, techniques, and so on.[3]

Trait-Independent Liveness Detection

Most liveness detection methods are trait dependent, meaning that the feature descriptors proposed for face spoofing might not function effectively for iris or fingerprint spoofing and vice versa. So, another research direction might be to develop a generic PAD—useable in multiple biometric systems.[1] This PAD would detect all traits' diverse presentation attacks, regardless of the biometric trait used in training. Such a system would bypass time-consuming large-scale spoof fabrication and mitigate the class imbalance problem, in which one class of data contains far more samples than another.

Sensor-Based Solutions

Researchers could develop sensor technologies that proactively adopt PAD technology to maximize the chance of successfully rejecting a biometric artifact; for instance, a sensor that directly scans a biometric pattern from just below the skin's surface. This technique might not only provide better-quality biometric characteristics in unconstrained environments but also discriminate artifacts from genuine samples. Any such solution will likely revolutionize the field and lead to numerous new biometric applications.

Integrating Match Scores with Liveness Values

Liveness detection typically generates a liveness measure value. How to combine this value with biometric match scores to counteract presentation attacks hasn't been systematically investigated. So, researchers might devise methods or models that combine biometric match scores with liveness values or depict their relationship.

Template Security

Recent studies on *inverse biometrics* (regenerating the original biometric sample from its template) have challenged the common belief that templates don't contain enough information to allow reconstruction of the original sample.[1]

However, the reconstructed trait can serve as a spoofing attack. Inverse biometrics can also be exploited to create synthetic databases or enlarge existing, real spoofing databases.

The threat of inverse biometrics can be addressed by three research directions. The first is to store liveness-related information in the biometric template. This will reduce interclass variations and make acquiring additional information for spoof fabrication difficult.

The second direction is to use cancelable biometrics, which applies a noninvertible mathematical transformation to the biometric template and stores only the transformed template. Although the transformed template is exposed, the real biometric trait can't be easily procured.

The final direction is to use biometric cryptosystems that generate cryptographic keys based on biometric samples. This would prevent inverse-biometric spoofing attacks and attacks on templates while protecting the user's privacy.

Security by Design

All the steps in traditional biometric-system design—from data acquisition to classification, including feature extraction, selection, and performance evaluation—should be revisited to take into account spoofing attacks. This approach is commonly called *security by design*.[3] For instance, feature selection should look for not only the highest generalization capability but also the feature's vulnerability to spoofing attacks.

Another solution is to constantly update systems, typically by retraining or adding new features. This procedure would need to be fast, computationally efficient, and, if possible, automated. To proactively embed security by design into algorithms, researchers could use concept drift, unsupervised learning, and active learning.

Cross-Sensor and Cross-Dataset Liveness Detection

The *cross-sensor* setting (in which the training and testing sets are from different sensors) and *cross-dataset* setting (in which the training and testing sets are from different datasets) haven't received much attention. However, they're important to the real-world application of liveness detection. So, cross-sensor and cross-dataset liveness detection (sensor and dataset interoperability) are major unresolved problems.

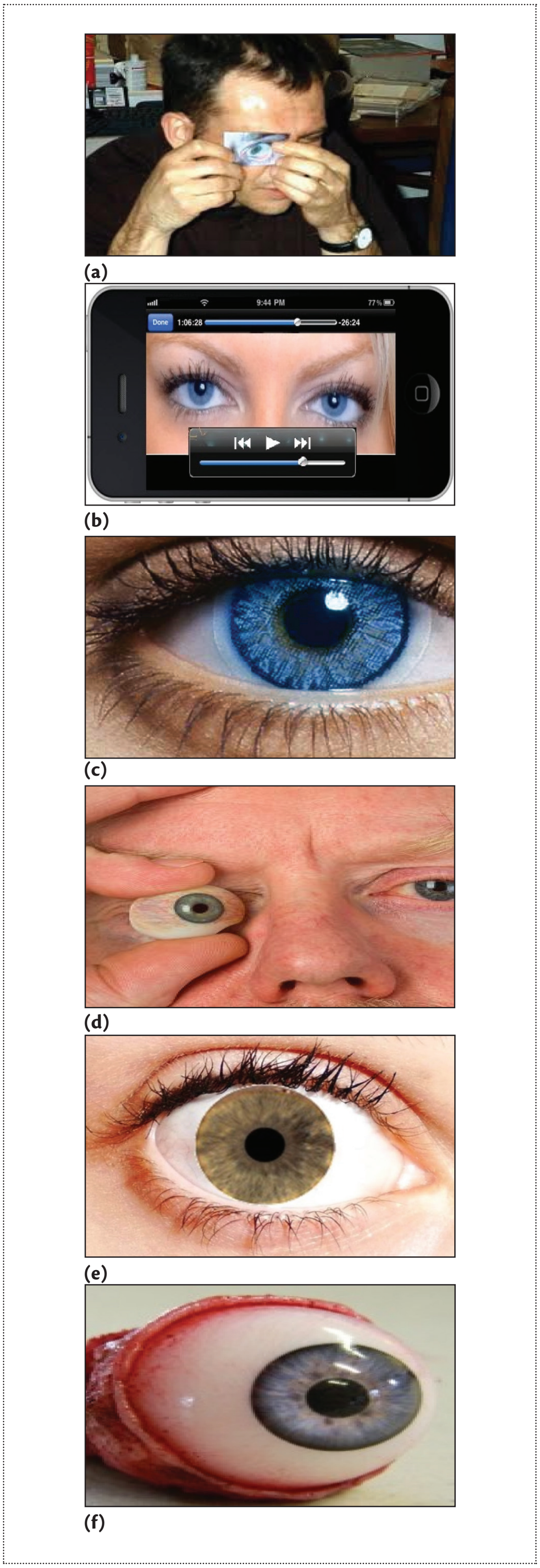

Figure 9. Iris spoofing can be achieved using (a) a photograph, (b) a video, (c) a printed contact lens, (d) an artificial eyeball, (e) a reverse-engineered iris image, or (f) a real eye removed from the legitimate user's body.

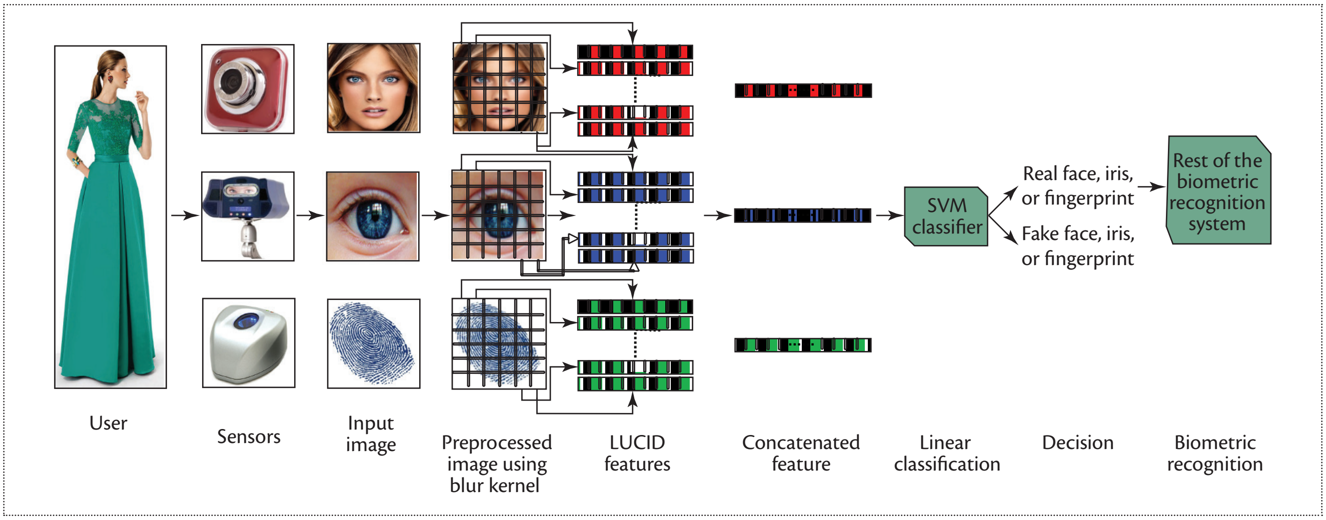
User
Sensors
Input image
Preprocessed image using blur kernel
LUCID features
Concatenated feature
SVM classifier
Linear classification
Real face, iris, or fingerprint
Fake face, iris, or fingerprint
Decision
Rest of the biometric recognition system
Biometric recognition

Figure 10. Our multibiometric spoofing-detection prototype. The prototype preprocesses the captured image of the respective biometric trait by averaging the blur kernel. It divides the resulting image into blocks according to the LUCID (Locally Uniform Comparison Image Descriptor) patch size. It computes features from each patch and concatenates them to devise a feature vector. Finally, a linear SVM (support vector machine) classifier determines whether the input image belongs to a live user.

Challenge–Response-Based Liveness Detection

In challenge–response liveness detection, users must, for example, repeat a phrase or blink their eyes to ensure that random instructions are performed properly. Nevertheless, this approach is user hostile and has low acceptability and high computational costs. So, researchers must develop novel, user-friendly, and effortless response methods. For instance, the system can issue challenges in response to some other trigger, such as the absence of change or movement during data acquisition.

Soft Biometrics

Soft biometrics typically refers to human attributes (for example, gender) that don't explicitly identify the person but narrow the range of possibilities. Soft biometrics could be employed separately or with other biometrics against spoofing.

Biological Presentation Attacks

Examples of biological presentation attacks include surgically transplanted hands or fingerprints, eyeballs removed from a legitimate user, and plastic surgery or makeup to make the imposter look like the legitimate user. Liveness detection of these attacks differs considerably from that of synthetic spoofing attacks. With synthetic attacks, the system learns the difference between live (natural) and spoofed (synthetic) biometric sample features, whereas with biological attacks, the system is faced with attacks (biometrics traits) that appear natural. So, existing techniques have limited capability to tackle them. The lack of public databases containing biological presentation attacks has further stymied research on this topic.

Interdisciplinary Research

To further state-of-the-art liveness detection technology, the research community needs to promote interdisciplinary basic science research to attain reliable, natural, and generalized methodologies for presentation attack countermeasures.

A Case Study on Trait-Independent Liveness Detection

The following case study is a first step toward trait-independent liveness detection.

The Prototype

We developed a multibiometric spoofing-detection prototype that derives a face, iris, and fingerprint representation to capture distinctive characteristics of real and spoofed traits. The system learns the fine differences between images of real and spoofed biometrics through a Locally Uniform Comparison Image Descriptor (LUCID).[15] LUCID is a novel approach to real-time feature description based on order permutations and is computable in linear time with respect to the number of pixels.

Let p be an $n \times n$ image patch with c color channels. We compute the LUCID descriptor for the patch in one line of Matlab as [~, desc] = sort(p(:)). Here, "sort" sorts the elements of p in ascending order, and we use "~" to ignore the first return value of sort. The desc is the order permutation representations for p. LUCID

Table 1. Results of experiments with multibiometric spoofing-detection prototype.

Dataset*	Feature	No. of users	No. of spoofed samples per user	No. of live samples per user	Performance†	
					Our method	Other methods
ATVS-FIr DB[12]	Iris	100	8	8	1.03 ± 0.34	4.66 ± 1.15[12]
Print Attack[1]	Face	50	20	20	2.88 ± 0.88	4.54 ± 1.35[5]
NUAA Photograph Impostor Database[4]	Face	15	500 (average)	340 (average)	1.54 ± 0.16	0.54 ± 0.10[5]
ATVS-FFp DB[8]	Fingerprint	68	12	12	7.17 ± 1.97	14.22 ± 4.10[9]
Feature extraction time (s)					0.0025	0.0814

**ATVS is the Biometric Recognition Group at Universidad Autónoma de Madrid; NUAA stands for Nanjing University of Aeronautics and Astronautics.*
†Mean ± standard deviation of the half total error rate (%).

has three parameters: the blur kernel width, the image patch size, and the use of color or grayscale images.

The prototype (see Figure 10) analyzes local features of face, fingerprint, and iris images using LUCID and encodes local patterns into an enhanced feature vector. The system feeds the results to a linear support vector machine classifier that determines whether the input biometric trait comes from a live person.

The Experiments

Experiments on publicly available datasets showed promising results. We used printed photographs to fabricate iris and face spoofs and used silicone to generate fake fingerprints.

The protocol. Table 1 shows the four datasets we used. We split each dataset randomly into a training set and testing set, each with 40 percent real users and 70 spoofed users; we repeated this procedure five times. We used a 5 × 5 averaging blur and 24 × 24 image patches for LUCID.

We evaluated the performance of previous systems[1,8,12] using the half total error rate (HTER), which combines the false-rejection rate (FRR; real access is rejected) and false-acceptance rate (FAR; the spoofing attack is accepted):

$$HTER(\tau,\mathcal{D})=\frac{FAR(\tau,\mathcal{D})+FRR(\tau,\mathcal{D})}{2}\%,$$

where $\mathcal{D}$ denotes the dataset. We chose the threshold τ as the equal error rate for the training set and reported the HTER using the test dataset.

The results. Table 1 shows that our method not only is a potentially simple, fast way to detect spoofing attacks, but it also demonstrates high classification accuracy for different biometric traits. Moreover, it doesn't deploy trait-specific properties (such as minutiae points, face detection, or iris position), thereby minimizing the computational load.

Unlike the other methods, the individual image feature descriptor used in this study (LUCID) delivered liveness detection for all three features (face, iris, and fingerprint). Our method performed better than the others on all the datasets except the NUAA Photograph Impostor Database. Our method was also much faster than the others.

For fingerprints, feature descriptors (LUCID) employed in this study and local phase quantization by Ghiani and his colleagues[9] obtained considerable error rates. That result was possibly due to fewer quality differences between the fake and real fingerprint images, which can cause overlap between fake and live classes.

We hope this research stimulates the development of generalized liveness detection solutions. Likewise, we expect expanded research efforts toward emerging biometrics such as vein, gait, and electrophysiological signals (electrocardiography) because such features are potentially difficult or even impossible to spoof. ■

References

1. S. Marcel, M.S. Nixon, and S.Z. Li, eds., *Handbook of Biometric Anti-spoofing*, Springer, 2014.
2. *Information Technology—Biometric Presentation Attack Detection—Part 1: Framework*, ISO/IEC DIS 30107-1, Int'l Org. for Standardization, 2014.
3. Z. Akhtar, "Security of Multimodal Biometric Systems against Spoofing Attacks," PhD thesis, Dept. Electrical Electronic Eng., Univ. Cagliari, 2012.
4. X. Tan et al., "Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model," *Proc. 11th European Conf. Computer Vision* (ECCV 10), 2010, pp. 504–517.

5. N. Kose and J.-L. Dugelay, “Reflectance Analysis Based Countermeasure Technique to Detect Face Mask Attacks,” *Proc. IEEE Int'l Conf. Digital Signal Processing* (DSP 13), 2013, pp. 1–6.
6. S. Parthasaradhi et al., “Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices,” *IEEE Trans. Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 35, no. 3, 2005, pp. 335–343.
7. C. Sousedik and C. Busch, “Presentation Attack Detection Methods for Fingerprint Recognition Systems: A Survey,” *IET Biometrics*, vol. 3, no. 1, 2014, pp. 1–15.
8. J. Galbally et al., “A High Performance Fingerprint Liveness Detection Method Based on Quality Related Features,” *Future Generation Computer Systems*, vol. 28, no. 1, 2012, pp. 311–321.
9. L. Ghiani, G.L. Marcialis, and F. Roli, “Fingerprint Liveness Detection by Local Phase Quantization,” *Proc. 21st Int'l Conf. Pattern Recognition* (ICPR 12), 2012, pp. 537–540.
10. S.Z. Li and A.K. Jain, eds., *Encyclopedia of Biometrics*, Springer, 2009.
11. J. Daugman, “Demodulation by Complex-Valued Wavelets for Stochastic Pattern Recognition,” *Int'l J. Wavelets, Multi-resolution Information Processing*, vol. 1, no. 1, 2003, pp. 1–17.
12. J. Galbally et al., “Iris Liveness Detection Based on Quality Related Features,” *Proc. 5th IAPR Int'l Conf. Biometrics* (ICB 12), 2012, pp. 271–276.
13. A. Goode, *Mobile Biometric Security Market Forecasts 2013–2018*, Goode Intelligence, 28 Oct. 2013.
14. A. Rattani and A. Ross, “Automatic Adaptation of Fingerprint Liveness Detector to New Spoof Materials,” *Proc. 2014 IEEE Int'l Joint Conf. Biometrics* (IJCB 14), 2014, pp. 1–8.
15. A. Ziegler et al., “Locally Uniform Comparison Image Descriptor,” *Proc. 26th Ann. Conf. Neural Information Processing Systems* (NIPS 2012), 2012, pp. 1–9.

Zahid Akhtar is a research associate in the University of Udine's Department of Mathematics and Computer Science. His research interests include computer vision, pattern recognition, and image processing with applications in biometrics, affective computing, and security systems. Akhtar received a PhD in electronic and computer engineering from the University of Cagliari. He's a member of the Italian Association for Pattern Recognition—Group of Italian Researchers in Pattern Recognition. Contact him at zahid.akhtar@uniud.it.

Christian Micheloni is an associate professor in the University of Udine's Department of Mathematics and Computer Science. His research interests include active vision for wide-area scene understanding and neural networks as well as pattern recognition and machine learning. Micheloni received a PhD in computer science from the University of Udine. Contact him at christian.micheloni@uniud.it.

Gian Luca Foresti is a professor of computer science and the director of the Artificial Vision and Real-Time System Laboratory at the University of Udine. His research interests include surveillance systems, multisensor image processing, active vision, data fusion, and pattern recognition. Foresti received a PhD in computer science from the University of Genoa. He's a fellow of the International Association for Pattern Recognition and a senior member of IEEE. Contact him at gianluca.foresti@uniud.it.