certain time window of observation at a high enough frame rate to be able to resolve the aforesaid motion vectors to their required velocity and frequency profiles, if any. They can also falsely reject live subjects that are holding very still during the scan, or falsely accept static reproductions with added motion, e.g., by bending and shaking the spoofing photos in certain ways.

[0005] A second category of existing anti-spoofing measures assumes that the photographic or video reproduction of the biometric sample is not of sufficient quality and thus image texture analysis methods can give identify the spoof. However, the assumption of discernibly low quality spoof reproduction is not a reliable one, especially with the advent of advanced high quality and exceedingly commonplace high definition recording and display technologies that can even be found in modern smartphones and tablets. Not surprisingly, by relying on specific and technology-dependent spoof reproduction artifacts, such techniques have been shown to be dataset dependent and have demonstrated subpar generalization capabilities. Another category of anti-spoofing measures, related to the second, which is based on reference or no-reference image quality metrics, suffers from the same shortcomings.

Summary

[0006] In various implementations described herein, the detection of physical properties indicating the presence of a live person is used to distinguish live, authentic faces from images/videos, verifications made under duress, and other spoofed and fraudulent authentication methods, and/or to identify spoofs, such as by detecting the presence of devices used to playback recorded images/videos/other physical reconstructions of the legitimate user for spoofing a biometric system. This is achieved, in part, by (a) detecting signatures of spoofs and (b) verifying the liveness and physical presence of an individual using three-dimensional face detection and two-factor pulse identification.

[0006a] In one aspect, a method of spoof detection includes capturing, by a user device having an image sensor, a plurality of images of a target; determining whether the target comprises at least one of a face-like structure and face-like tissue based on at least one of (i) reflections of audio signals emitted by the user device off the target and (ii) photometric stereo effects across the plurality of images, wherein the photometric stereo effects are induced by high frequency patterns of a screen of the user device coded with illumination intensity, phase and frequency, and color; identifying, based on the images, whether the target has a first pulse; measuring a second pulse of the target through physical contact with

the target; and determining whether the target is a spoof based at least in part on (i) the determination of whether the target comprises at least one of a face-like structure and face-like tissue, (ii) the identification of whether the target has a pulse and (iii) the measurement of the second pulse.

[0006b] In another aspect, a system for spoof detection includes at least one memory for storing computer-executable instructions; and at least one processor for executing the instructions stored on the at least one memory. Execution of the instructions programs the at least one processor to perform operations comprising capturing, by a user device having an image sensor, a plurality of images of a target; determining whether the target comprises at least one of a face-like structure and face-like tissue based on at least one of (i) reflections of audio signals emitted by the user device off the target and (ii) photometric stereo effects across the plurality of images, wherein the photometric stereo effects are induced by high frequency patterns of a screen of the user device coded with illumination intensity, phase and frequency, and color; identifying, based on the images, whether the target has a first pulse; measuring a second pulse of the target through physical contact with the target; determining whether the target is a spoof based at least in part on (i) the determination of whether the target comprises at least one of a face-like structure and face-like tissue, (ii) the identification of whether the target has a pulse and (iii) the measurement of the second pulse.

[0006c] In another aspect, a method of spoof detection includes capturing, by a user device having an image sensor, a plurality of images of a target; emitting, using an audio output component of the user device, audio signals, wherein one or more characteristics of the audio signals are randomized; receiving, using an audio input component of the user device, reflections of the audio signals off the target; determining whether the target comprises at least one of a face-like structure and face-like tissue based on at least one of (i) the reflections of the audio signals emitted by the user device off the target, and (ii) photometric stereo effects across the plurality of images; identifying, based on the images, whether the target has a first pulse; measuring a second pulse of the target through physical contact with the target; and determining whether the target is a spoof based at least in part on (i) the determination of whether the target comprises at least one of a face-like structure and face-like tissue, (ii) the identification of whether the target has a pulse and (iii) the measurement of the second pulse.

[0006d] In another aspect, a system for spoof detection includes at least one memory for storing computer-executable instructions, and at least one processor for executing the instructions stored on the at least one memory. Execution of the instructions programs the at least one processor to perform operations comprising capturing, by a user device having an image sensor, a plurality of images of a target; emitting, using an audio output component of the user device, audio signals, wherein one or more characteristics of the audio signals are randomized; receiving, using an audio input component of the user device, reflections of the audio signals off the target; determining whether the target comprises at least one of a face-like structure and face-like tissue based on at least one of (i) the reflections of the audio signals emitted by the user device off the target, and (ii) photometric stereo effects across the plurality of images; identifying, based on the images, whether the target has a first pulse; measuring a second pulse of the target through physical contact with the target; and determining whether the target is a spoof based at least in part on (i) the determination of whether the target comprises at least one of a face-like structure and face-like tissue, (ii) the identification of whether the target has a pulse and (iii) the measurement of the second pulse.

[0007] In an aspect of the disclosure, a computer-implemented method includes the steps of: emitting, using an audio output component of a user device, one or more audio signals; receiving, using an audio input component of the user device, one or more reflections of the audio signals off a target; determining, based on the one or more reflections, whether the target comprises at least one of a face-like structure and face-like tissue; and determining whether the target is a spoof based at least in part of the determination of whether the target