SPOOF DETECTION USING OPTOKINETIC RESPONSE

TECHNICAL FIELD

[0001] This disclosure relates to image capture devices.

BACKGROUND

[0002] Biometrics allows a person to be identified and authenticated based on a set of recognizable and verifiable data, which are unique and specific to them. Biometric authentication includes the process of comparing data for a person's characteristics to that person's biometric "template" to determine resemblance. Biometric authentication systems can be grouped based on the physical characteristic employed to authenticate users. Examples of such systems include authentication based on fingerprints, hand geometry, palm veins, retina scans, iris scans, facial recognition, signatures, and voice analysis.

SUMMARY

[0003] In one aspect, this document features a method for preventing access to a secure system based on determining a captured video to be an alternative representation of a live person. The method includes presenting a stimulus on a user interface of a device. Video of a subject who is within a field of view of a video capture device is captured after presentation of the stimulus. The captured video is analyzed to extract ocular data comprising a response of the subject to the stimulus. A determination is made, by comparing the ocular data to one or more reference patterns that the subject in the captured video is an alternative representation of a live person. Responsive to determining that the subject in the captured video is an alternative representation of a live person, access to the secured system is prevented. In one aspect, the method includes: estimating a first distance between a subject and a user interface of a device; determining a first stimulus velocity at which to present a stimulus to the subject on the user interface of the device, wherein the first stimulus velocity is based on the first distance between the subject and the user interface; presenting the stimulus to the subject at the first stimulus velocity on the user interface of the device; estimating a second distance between the subject and the user interface of the device; selecting a second stimulus velocity

based on the second distance; presenting the stimulus at the second stimulus velocity on the user interface; capturing video of the subject while the subject is within a field of view of a video capture device after presentation of the stimulus at the second stimulus velocity; analyzing the video to extract ocular data comprising a response of the subject to the stimulus when presented at the second stimulus velocity; determining, by comparing the ocular data to one or more reference patterns that the subject in the captured video is an alternative representation of a live person, wherein the one or more reference patterns are selected based on the second stimulus velocity; and responsive to determining that the subject in the captured video is an alternative representation of a live person, preventing access to a secured system.

[0004] In another aspect, this document features a system that includes a video acquisition device and a video analysis engine that includes one or more processing devices. The processing device is configured to perform the methods described above. The video acquisition device is configured to capture a video of a subject who is within a field of view of a video capture device after presentation of a stimulus. The video analysis engine is configured to: analyze the captured video to extract ocular data comprising a response of the subject to the stimulus; determine, by comparing the ocular data to one or more reference patterns that the subject in the captured video is an alternative representation of a live person; and responsive to determining that the subject in the captured video is an alternative representation of a live person, prevent access to the secured system .

[0005] In another aspect, this document features one or more machine-readable storage devices that includes machine-readable instructions configured to cause one or more processing devices to execute various operations corresponding to the methods described above. The operations include: presenting a stimulus on a user interface of a device; capturing video of a subject who is within a field of view of a video capture device after presentation of the stimulus; analyzing the captured video to extract ocular data comprising a response of the subject to the stimulus; determining, by comparing the ocular data to one or more reference patterns that the subject in the captured video is an alternative representation

of a live person; and responsive to determining that the subject in the captured video is an alternative representation of a live person, preventing access to the secured system.

[0006] Implementations of the above aspects can include one or more of the following features. A second video of a second subject can be captured after presentation of the stimulus. The second video can be analyzed to extract a second set of ocular data comprising a response of the second subject to the stimulus. A determination can be made, by comparing the second set of ocular data to the one or more reference patterns, that the second subject is a live person. Responsive to determining that the second subject is a live person, an authentication process can be initiated for determining if the live person is authorized to access the secured system. A type of stimulus to present can be selected from among multiple types of stimulus. A velocity at which to present the stimulus can be determined. Presenting the stimulus can include presenting the stimulus at the determined velocity. The stimulus can be a high contrast stimulus. Analyzing the captured video can include tracking eye movements after presentation of the stimulus. The reference patterns can include a first pattern corresponding to optokinetic nystagmus. Comparing the ocular data can include comparing the tracked eye movements to the first pattern corresponding to optokinetic nystagmus. Analyzing the captured video can include tracking changes in pupillary dynamics after

CLAIMS

1. A method for preventing access to a secure system based on determining a captured video to be an alternative representation of a live person, the method comprising:

estimating a first distance between a subject and a user interface of a device;

determining a first stimulus velocity at which to present a stimulus to the subject on the user interface of the device, wherein the first stimulus velocity is based on the first distance between the subject and the user interface;

presenting the stimulus to the subject at the first stimulus velocity on the user interface of the device;

estimating a second distance between the subject and the user interface of the device;

selecting a second stimulus velocity based on the second distance;

presenting the stimulus at the second stimulus velocity on the user interface;

capturing video of the subject while the subject is within a field of view of a video capture device after presentation of the stimulus at the second stimulus velocity;

analyzing the video to extract ocular data comprising a response of the subject to the stimulus when presented at the second stimulus velocity;

determining, by comparing the ocular data to one or more reference patterns that the subject in the captured video is an alternative representation of a live person, wherein the one or more reference patterns are selected based on the second stimulus velocity; and

responsive to determining that the subject in the captured video is an alternative representation of a live person, preventing access to a secured system.

2. The method of claim 1, further comprising:

capturing a second video of a second subject after a second presentation of the stimulus, to the second subject, at the second stimulus velocity;

analyzing the second video to extract a second set of ocular data comprising a response of the second subject to the stimulus;

determining, by comparing the second set of ocular data to the one or more reference patterns, that the second subject is a live person; and

responsive to determining that the second subject is a live person, initiating an authentication process for determining if the live person is authorized to access the secured system.

3. The method of claim 1, further comprising selecting a type of stimulus to present from among multiple types of stimulus.

4. The method of claim 1, wherein the stimulus is a high contrast stimulus.

5. The method of claim 1, wherein analyzing the captured video comprises tracking eye movements after presentation of the stimulus.

6. The method of claim 5, wherein the reference patterns include a first pattern corresponding to optokinetic nystagmus.

7. The method of claim 6, wherein comparing the ocular data comprises comparing the tracked eye movements to the first pattern corresponding to optokinetic nystagmus.

8. The method of claim 1, wherein analyzing the captured video comprises tracking changes in pupillary dynamics after presentation of the stimulus.

9. The method of claim 8, wherein the reference patterns include a second pattern corresponding to an expected change in pupillary dynamics.

10. The method of claim 9, wherein comparing the ocular data comprises comparing the tracked changed in pupillary dynamics to the second pattern corresponding to the expected change in pupillary dynamics.

11. A system comprising:

a video acquisition device configured to capture a video of a subject who is within a field of view of a video capture device;

a processing device configured to:

estimate a first distance between the subject and a user interface of a device,

determine a first stimulus velocity at which to present a stimulus to the subject on the user interface of the device wherein the first stimulus velocity is based on the first distance between the subject and the user interface,

present the stimulus to the subject at the first stimulus velocity,

estimate a second distance between the subject and the user interface of the device,

select a second stimulus velocity based on the second distance, and

present the stimulus at the second stimulus velocity on the user interface; and

a video analysis engine comprising one or more processing devices, the video analysis engine configured to:

analyze video of the subject captured by the video acquisition device while the subject is within a field of view of the video capture device after presentation of the stimulus at the second stimulus velocity, to extract ocular data comprising a response of the subject to the stimulus when presented at the second stimulus velocity;

determine, by comparing the ocular data to one or more reference patterns that the subject in the captured video is an alternative representation of a live person, wherein the one or more reference patterns are selected based on the second stimulus velocity; and

responsive to determining that the subject in the captured video is an alternative representation of a live person, prevent access to a secured system.

12. The system of claim 11:

wherein the video acquisition device is configured to capture a second video of a second subject after a second presentation of the stimulus, to the second subject, at the updated stimulus velocity; and

wherein the video analysis engine is configured to:

analyze the second video to extract a second set of ocular data comprising a response of the second subject to the stimulus;

determine, by comparing the second set of ocular data to the one or more reference patterns, that the second subject is a live person; and

responsive to determining that the second subject is a live person, initiate an authentication process for determining if the live person is authorized to access the secured system.

13. The system of claim 11, wherein the stimulus is a high contrast stimulus.

14. The system of claim 11, wherein analyzing the captured video comprises tracking eye movements after presentation of the stimulus.

15. One or more machine-readable non-transitory storage devices comprising machine-readable instructions configured to cause one or more processing devices to execute operations comprising:

estimating a first distance between a subject and a user interface of a device;

determining a first stimulus velocity at which to present a stimulus to the subject on the user interface of the device, wherein the first stimulus velocity is based on the first distance between the subject and the user interface;

presenting the stimulus to the subject at the first stimulus velocity on the user interface of the device;

estimating a second distance between the subject and the user interface of the device;

selecting a second stimulus velocity based on the second distance;

presenting the stimulus at the second stimulus velocity on the user interface;

capturing video of the subject while the subject is within a field of view of a video capture device after presentation of the stimulus at the second stimulus velocity;

analyzing the video to extract ocular data comprising a response of the subject to the stimulus when presented at the second stimulus velocity;

determining, by comparing the ocular data to one or more reference patterns that the subject in the captured video is an alternative representation of a live person, wherein the one or more reference patterns are selected based on the second stimulus velocity; and

responsive to determining that the subject in the captured video is an alternative representation of a live person, preventing access to a secured system.

16. The machine-readable storage devices of claim 15, the operations further comprising:

capturing a second video of a second subject after a second presentation of the stimulus, to the second subject, at the second stimulus velocity;

analyzing the second video to extract a second set of ocular data comprising a response of the second subject to the stimulus;

determining, by comparing the second set of ocular data to the one or more reference patterns, that the second subject is a live person; and

responsive to determining that the second subject is a live person, initiating an authentication process for determining if the live person is authorized to access the secured system.

17. The machine-readable storage devices of claim 15, the operations further comprising selecting a type of stimulus to present from among multiple types of stimulus.