METHODS, SYSTEMS, AND MEDIA FOR DETECTING SPOOFING IN MOBILE AUTHENTICATION

CROSS-REFERENCE

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 62/560,038, filed September 18, 2017, which is incorporated herein by reference in its entirety.

BACKGROUND

[0002] "Spoofing" a security system is generally defined as an act of masquerading as an authenticated user, by submitting false data. In this case, methods of liveness detection may be employed to determine whether a biometric modality, such as a face, a palm (palm print), a finger (fingerprint), or an ear, carries the unique structural qualities of the original three-dimensional biometric modality, or is-a two-dimensional replicate.

SUMMARY

[0003] Many current technologies for optical recognition of identity can be easily spoofed or hacked. In the case of facial recognition on mobile devices, for example, it is common for the facial recognition algorithms to be tricked into accepting a fake representation of a user's face, as presented via an image of the user's face on the front-facing video screen of another mobile device, or as presented via a print-out of the user's face on paper, among other methods of identity spoofing. Moreover, biometric implementations such as the facial recognition algorithm described in this example, providing identity management on mobile devices, are a regular feature of mobile devices across the world, and there is a current unmet need for an automated authentication technology for optical recognition of identity, while maintaining immunity to spoofing attempts.

[0004] In a first aspect, the present disclosure provides a mobile device comprising: a front-facing camera, a front-facing screen, at least one processor, a memory, an operating system configured to perform executable instructions, and a computer program including instructions executable by the at least one processor to run an application for detecting spoofing of a 3D object, using a 2D representation of the 3D object, in a mobile object authentication process, the application comprising: a) a software module capturing, via the front-facing camera, i) a first image data of the 3D object while displaying, via the front-facing screen, a first authentication pattern, the first authentication pattern comprising a plurality of first authentication pattern regions, wherein at least one of the first authentication pattern regions varies from another first authentication pattern region in at least one of: brightness, position, size, shape, and color over time causing a first variance of lighting effects, wherein the first image data comprises a first set of highlights and shadows on the 3D object over

time; and ii) a second image data of the 3D object while displaying, via the front-facing screen, the second authentication pattern after displaying the first authentication pattern, wherein the second authentication pattern is different from the first authentication pattern, the second authentication pattern comprising a plurality of second authentication pattern regions, wherein at least one of the second authentication pattern regions varies from another second authentication pattern regions in at least one of brightness, position, size, shape, and color causing a second variance of lighting effects, wherein the second image data comprises a second set of highlights and shadows on the 3D object over time; b) a software module calculating a difference between the first set of highlights and shadows and the second set of highlights and shadows to determine a current spatial characteristic of the 3D object; and c) a software module determining if spoofing of the 3D object, using the 2D representation, is attempted in the mobile authentication process by

comparing the current spatial characteristic of the 3D object with a stored reference spatial characteristic of the 3D object.

[0005] In some embodiments, the 3D object comprises a face, a palm (palm print), a finger (fingerprint), or an ear. In some embodiments, the 2D representation comprises a photograph of the 3D object. In some embodiments, the image data comprises a plurality of photographs of the 3D object. In some embodiments, the image data comprises a video of the 3D object. In some embodiments, the authentication pattern comprises a plurality of images. In some embodiments, the authentication pattern comprises a video. In some embodiments, the plurality of regions are arranged in two or more vertical or horizontal bands in the authentication pattern. In some embodiments, the plurality of regions are arranged in a horizontal band across the top or bottom of the screen, or in a vertical band across the left or right side of the screen in the authentication pattern. In some embodiments, the authentication pattern comprises variation of at least one region in at least one of: brightness, position, size, shape, and color to form a regular pulse or a random pulse in the authentication pattern. In some embodiments, at least one of the regions varies in position over time to form a translation or rotation of the region in the authentication pattern. In some embodiments, at least one of the regions varies in size over time to form a contraction or expansion of the region in the authentication pattern. In some embodiments, the application further comprises a software module receiving a request to authenticate the 3D object. In some embodiments, the application further comprises a software module instructing a user to orient the front-facing camera of the mobile device in a fixed position relative to the object during the capturing of the image data. In some embodiments, the variation of at least one region in at least one of: brightness, position, size, shape, and color encode information in the authentication pattern.

[0006] In a second aspect, the present disclosure provides a system for detecting spoofing of a 3D object, using a 2D representation of the 3D object, in a mobile object authentication process, the system comprising: a mobile device comprising a front-facing camera, a front-facing screen, at least one processor, a memory; and a server comprising at least one processor and a memory: the mobile device configured to: a) capture, via the front-facing camera, i) a first image data of the 3D object while displaying, via the front-facing screen, a first authentication pattern comprising a plurality of first authentication pattern regions, wherein at least one of the first authentication regions varies from another first authentication pattern region in at least one of: brightness, position, size, shape, and color over time causing a first variance of lighting effects, wherein the first image data comprises a first set of highlights and shadows on the 3D object over time; ii) a second image data of the 3D object while displaying, via the front-facing screen, the second authentication pattern after displaying

the first authentication pattern, wherein the second authentication pattern is different from the first authentication pattern, the second authentication pattern comprising a plurality of second authentication pattern regions, wherein at least one of the second authentication pattern regions varies from another second authentication pattern regions in at least one of brightness, position, size, shape, and color causing a second variance of lighting effects, wherein the second image data comprises a second set of highlights and shadows on the 3D object over time; and b) transmit the first image data and the second image data to the server; the server configured to: a) receive the first image data and the second image from the mobile device; b) calculate a difference between the first set of highlights and shadows and the second set of highlights and shadows to determine a current spatial characteristic of the 3D object; c) determine if spoofing of the 3D object, using a 2D

representation of the 3D object, is attempted in the mobile authentication process by comparing the current spatial characteristic of the 3D object with a stored reference spatial characteristic of the 3D object; and d) transmit a spoofing result to the mobile device.

[0007] In some embodiments, the 3D object comprises a face, a palm (palm print), a finger (fingerprint), or an ear. In some embodiments, the 2D representation comprises a photograph of the 3D object. In some embodiments, the image data comprises a plurality of photographs of the 3D object. In some embodiments, the image data comprises a video of the 3D object. In some embodiments, the authentication pattern comprises a plurality of images. In some embodiments, the authentication pattern comprises a video. In some embodiments, the plurality of regions are arranged in two or more vertical or horizontal bands in the authentication pattern. In some embodiments, the plurality of regions are arranged in a horizontal band across the top or bottom of the screen, or in a vertical band across the left or right side of the screen in the authentication pattern. In some embodiments, the authentication pattern comprises variation of at least one region in at least one of: brightness, position, size, shape, and color to form a regular pulse or a random pulse in the authentication pattern. In some embodiments, at least one of the regions varies in position over time to form a translation or rotation of the region in the authentication pattern. In some embodiments, at least one of the regions varies in size over time to form a contraction or expansion of the region in the authentication pattern. In some embodiments, the application further comprises a software module receiving a request to authenticate the 3D object. In some embodiments, the application further comprises a software module instructing a user to orient the front-facing camera of the mobile device in a fixed position relative to the object during the capturing of the image data. In some embodiments, the variation of at least one region in at least one of: brightness, position, size, shape, and color encode information in the authentication pattern.

[0008] In a third aspect, the present disclosure provides a method of detecting spoofing of a 3D object, using a 2D representation of the 3D object, in a mobile object authentication process, the method comprising: a) capturing, via a front-facing camera of a mobile device, i) a first image data of the 3D object while displaying, via a front-facing screen of the mobile device, a first authentication pattern, the first authentication pattern comprising a plurality of first authentication pattern regions, wherein at least one of the first authentication pattern regions varies from another first authentication pattern region in at least one of: brightness, position, size, shape, and color over time causing a first variance of lighting effectsm wherein the first image data comprises a first set of highlights and shadows on the 3D object over time; and ii) a second image data of the 3D object while displaying, via the front-facing screen, the second authentication pattern after displaying the first authentication pattern,

wherein the second authentication pattern is different from the first authentication pattern, the second authentication pattern comprising a plurality of second authentication pattern regions, wherein at least one of the second authentication pattern regions varies from another second authentication pattern regions in at least one of brightness, position, size, shape, and color causing a second variance of lighting effects, wherein the second image data comprises a second set of highlights and shadows on the 3D object over time; b) calculating a difference between the first set of highlights and shadows and the second set of highlights and shadows to determine a current spatial characteristic of the 3D object; and c) determining if spoofing of the 3D object, using the 2D representation, is attempted in the mobile authentication process by comparing the current spatial characteristic of the 3D object with a stored reference spatial characteristic of the 3D object.

[0009] In some embodiments, the 3D object comprises a face, a palm (palm print), a finger (fingerprint), or an ear. In some embodiments, the 2D representation comprises a photograph of the 3D object. In some embodiments, the image data comprises a plurality of photographs of the 3D object. In some embodiments, the image data comprises a video of the 3D object. In some embodiments, the authentication pattern comprises a plurality of images. In some embodiments, the authentication pattern comprises a video. In some embodiments, the plurality of regions are arranged in two or more vertical or horizontal bands in the authentication pattern. In some embodiments, the plurality of regions are arranged in a horizontal band across the top or bottom of the screen, or in a vertical band across the left or right side of the screen in the authentication pattern. In some embodiments, the authentication pattern comprises variation of at least one region in at least one of: brightness, position, size, shape, and color, to form a regular pulse or a random pulse in the authentication pattern. In some embodiments, at least one of the regions varies in position over time to form a translation or rotation of the region in the authentication pattern. In some embodiments, at least one of the regions varies in size over time to form a contraction or expansion of the region in the authentication pattern. In some embodiments, further comprising receiving a request to authenticate the 3D object. In some embodiments, further comprising instructing a user to orient the front-facing camera of the mobile device in a fixed position relative to the object during the capturing of the image data. In some embodiments, the variation of at least one region in at least one of: brightness, position, size, shape, and color, encode information in the authentication pattern.

[0010] An embodiment provided herein is a mobile device comprising: a front-facing camera, a front-facing screen, at least one processor, a memory, an operating system configured to perform executable instructions, and a computer program including instructions executable by the at least one processor to run an application for recognizing a class or a within-class identity of a 3D object, solely or in combination with other mobile processes of object detection and identity recognition, the application comprising: a software module capturing, via the front-facing camera, image data of the 3D object while displaying, via the front-facing screen, an identification pattern comprising a plurality of regions, wherein at least one of the regions varies in at least one of: brightness, position, size, shape, and color over time causing a variance of lighting effects which create highlights and shadows on the 3D object over time; a software module using the image data and the identification pattern to determine a current spatial characteristic of the 3D object; and a software module determining the class, or the within-class identity of the 3D object, solely or in combination with other mobile processes of object detection and identity recognition by comparing the current spatial characteristic of the 3D object with a stored reference spatial characteristic of the 3D object.

[0011] In some embodiments, the 3D object comprises a face, a palm (palm print), a finger (fingerprint), or an ear. In some embodiments, the image data comprises a plurality of photographs of the 3D object. In some embodiments, the image data comprises a video of the 3D object. In some embodiments, the identification pattern comprises a plurality of images. In some embodiments, the identification pattern comprises a video. In some embodiments, the plurality of regions are arranged in two or more vertical or horizontal bands in the identification pattern. In some embodiments, the plurality of regions are arranged in a horizontal band across the top or bottom of the screen, or in a vertical band across the left or right side of the screen in the identification pattern. In some embodiments, the identification pattern comprises variation of at least one region in at least one of: brightness, position, size, shape, and color to form a regular pulse or a random pulse in the identification pattern. In some embodiments, at least one of the regions varies in position over time to form a translation or rotation of the region in the identification pattern. In some embodiments, at least one of the regions varies in size over time to form a contraction or expansion of the region in the identification pattern. In some embodiments, the application further comprises a software module receiving a request to recognize the class, or the within-class identity of the 3D object. In some embodiments, the application further comprises a software module instructing a user to orient the front-facing camera of the mobile device in a fixed position relative to the object during the capturing of the image data. In some embodiments, the variation of at least one region in at least one of: brightness, position, size, shape, and color encode information in the identification pattern.

[0012] Another embodiment provided herein is a system for recognizing a class or a within-class identity of a 3D object, solely or in combination with other mobile processes of object detection and identity recognition, the system comprising: a mobile device comprising a front-facing camera, a front-facing screen, at least one processor, a memory; and a server comprising at least one processor and a memory: the mobile device configured to: capture, via the front-facing camera, image data of the 3D object while displaying, via the front-facing screen, an identification pattern comprising a plurality of regions, wherein at least one of the regions varies in at least one of: brightness, position, size, shape, and color over time causing a variance of lighting effects which create highlights and shadows on the 3D object over time; and transmit the image data and the identification pattern to the server; the server configured to: receive the image data and the identification pattern from the mobile device; use the image data and the identification pattern to determine a current spatial characteristic of the 3D object; determine the class, or the within-class identity of the 3D object, solely or in combination with other mobile processes of object detection and identity recognition , by comparing the current spatial

characteristic of the 3D object with a stored reference spatial characteristic of the 3D object; and transmit the class, or the within-class identity of the 3D object to the mobile device.

[0013] In some embodiments, the 3D object comprises a face, a palm (palm print), a finger (fingerprint), or an ear. In some embodiments, the image data comprises a plurality of photographs of the 3D object. In some embodiments, the image data comprises a video of the 3D object. In some embodiments, the identification pattern comprises a plurality of images. In some embodiments, the identification pattern comprises a video. In some embodiments, the plurality of regions are arranged in two or more vertical or horizontal bands in the identification pattern. In some embodiments, the plurality of regions are arranged in a horizontal band across the top or bottom of the screen, or in a vertical band across the left or right side of the screen in the identification pattern. In some embodiments, the identification pattern comprises variation of at least one region in at least one of: brightness, position, size, shape, and color to form a regular pulse or a random pulse in the identification pattern. In some embodiments, at least one of the regions varies in position over time to form a translation or rotation of the region in the identification pattern. In some embodiments, at least one of the regions varies in size over time to form a contraction or expansion of the region in the identification pattern. In some embodiments, the application further comprises a software module receiving a request to determine a class or within-class identity of the 3D object. In some embodiments, the application further comprises a software module instructing a user to orient the front-facing camera of the mobile device in a fixed position relative to the object during the capturing of the image data. In some embodiments, the variation of at least one region in at least one of: brightness, position, size, shape, and color encode information in the identification pattern.

[0014] Yet another embodiment provided herein is a method of recognizing a class or within-class identity of a 3D object, solely or in combination with other mobile processes of object detection and identity recognition, the method comprising: capturing, via a front-facing camera of a mobile device, image data of the 3D object while displaying, via a front-facing screen of the mobile device, an identification pattern comprising a plurality of regions, wherein at least one of the regions varies in at least one of: brightness, position, size, shape, and color over time causing a variance of lighting effects which create highlights and shadows on the 3D object over time; using the image data and the identification pattern to determine a current spatial characteristic of the 3D object; and determining the class, or the within-class identity of a 3D object of the 3D object, solely or in combination with other mobile processes of object detection and identity recognition, by comparing the current spatial characteristic of the 3D object with a stored reference spatial characteristic of the 3D object.

CLAIMS

WHAT IS CLAIMED IS:

1. A mobile device comprising: a front-facing camera, a front-facing screen, at least one processor, a memory, an operating system configured to perform executable instructions, and a computer program including instructions executable by the at least one processor to run an application for detecting spoofing of a 3D object, using a 2D representation of the 3D object, in a mobile object authentication process, the application comprising:

    a) a software module capturing, via the front-facing camera,

        i) a first image data of the 3D object while displaying, via the front-facing screen, a first authentication pattern, the first authentication pattern comprising a plurality of first authentication pattern regions, wherein at least one of the first authentication pattern regions varies from another first authentication pattern region in at least one of: brightness, position, size, shape, and color over time causing a first variance of lighting effects, wherein the first image data comprises a first set of highlights and shadows on the 3D object over time, and

        ii) a second image data of the 3D object while displaying, via the front-facing screen, the second authentication pattern after displaying the first authentication pattern, wherein the second authentication pattern is different from the first authentication pattern, the second authentication pattern comprising a plurality of second authentication pattern regions, wherein at least one of the second authentication pattern regions varies from another second authentication pattern regions in at least one of brightness, position, size, shape, and color causing a second variance of lighting effects, wherein the second image data comprises a second set of highlights and shadows on the 3D object over time;

    b) a software module calculating a difference between the first set of highlights and shadows and the second set of highlights and shadows to determine a current spatial characteristic of the 3D object; and

    c) a software module determining if spoofing of the 3D object, using the 2D representation, is attempted in the mobile authentication process by comparing

the current spatial characteristic of the 3D object with a stored reference spatial characteristic of the 3D object.

2. The device of claim 1, wherein the 3D object comprises a face, a palm (palm print), a finger (fingerprint), or an ear.

3. The device of claim 1, wherein the 2D representation comprises a photograph of the 3D object.

4. The device of claim 1, wherein at least one of the first image data and the second image data comprises a plurality of photographs of the 3D object, a video of the 3D object, or both.

5. The device of claim 1, wherein at least one of the first authentication pattern and the second authentication pattern comprises a plurality of images, a video, or both.

6. The device of claim 1, wherein the at least one of the plurality of the first authentication pattern regions and the plurality of the second authentication pattern regions are arranged in two or more vertical or horizontal bands.

7. The device of claim 1, wherein the variation within at least one of the first authentication pattern regions and the second authentication pattern regions forms a regular pulse or a random pulse in the first or second authentication pattern.

8. The device of claim 1, wherein the variation within at least one of the first authentication pattern regions and the second authentication pattern regions forms a translation or rotation of the first authentication pattern region or the second authentication pattern region in the first authentication pattern or the second authentication pattern, forms a contraction or expansion of the first authentication pattern region or the second authentication pattern region in the first authentication pattern or the second authentication pattern, or both.

9. The device of claim 1, wherein the application further comprises a software module receiving a request to authenticate the 3D object, and a software module instructing a user to orient the front-facing camera of the mobile device in a fixed position relative to the object during the capturing of the first image data, the second image data, or both.

10. The device of claim 1, wherein the variation within at least one of the first authentication pattern regions and the second authentication pattern regions encodes information in the first or second authentication pattern.

11. A system for detecting spoofing of a 3D object, using a 2D representation of the 3D object, in a mobile object authentication process, the system comprising: a mobile device comprising a front-facing camera, a front-facing screen, at least one processor, a memory; and a server comprising at least one processor and a memory:

the mobile device configured to:

a) capture, via the front-facing camera,

i) a first image data of the 3D object while displaying, via the front-facing screen, first authentication pattern comprising a plurality of first authentication pattern regions, wherein at least one of the first authentication pattern regions varies from another first authentication pattern region in at least one of: brightness, position, size, shape, and color over time causing a first variance of lighting effects, wherein the first image data comprises a first set of highlights and shadows on the 3D object over time;

ii) a second image data of the 3D object while displaying, via the front-facing screen, the second authentication pattern after displaying the first

authentication pattern, wherein the second authentication pattern is different from the first authentication pattern, the second authentication pattern comprising a plurality of second authentication pattern regions, wherein at least one of the second authentication pattern regions varies from another second authentication pattern regions in at least one of brightness, position, size, shape, and color causing a second variance of lighting effects, wherein the second image data comprises a second set of highlights and shadows on the 3D object over time; and

b) transmit the first image data and the second image data to the server;

the server configured to:

a) receive the first image data and the second image data from the mobile device;

b) calculate a difference between the first set of highlights and shadows and the second set of highlights and shadows to determine a current spatial characteristic of the 3D object;

c) determine if spoofing of the 3D object, using a 2D representation of the 3D object, is attempted in the mobile authentication process by comparing the current spatial characteristic of the 3D object with a stored reference spatial characteristic of the 3D object; and

d) transmit a spoofing result to the mobile device.

12. The system of claim 11, wherein the 3D object comprises a face, a palm (palm print), a finger (fingerprint), or an ear.

13. The system of claim 11, wherein the 2D representation comprises a photograph of the 3D object.

14. The system of claim 11, wherein at least one of the first image data and the second image data comprises a plurality of photographs of the 3D object, a video of the 3D object, or both.

15. The system of claim 11, wherein at least one of the first authentication pattern and the second authentication pattern comprises a plurality of images, a video, or both.

16. The system of claim 11, wherein at least one of the plurality of first authentication pattern regions and second authentication pattern regions are arranged in two or more vertical or horizontal bands.

17. The system of claim 11, wherein the variation within at least one of the first authentication pattern regions and the second authentication pattern regions forms a regular pulse or a random pulse in the first or second authentication pattern.

18. The system of claim 11, wherein the variation within at least one of the first authentication pattern regions and the second authentication pattern regions forms a translation or rotation of the first authentication pattern region or the second authentication pattern region in the first authentication pattern or the second authentication pattern, forms a contraction or expansion of the first authentication pattern region or the second authentication pattern region in the first authentication pattern or the second authentication pattern, or both.

19. The system of claim 11, wherein the application further comprises a software module receiving a request to authenticate the 3D object, and a software module instructing a user to orient the front-facing camera of the mobile device in a fixed position relative to the object during the capturing of the first image data, the second image data, or both.

20. The system of claim 11, wherein the variation within at least one of the first authentication pattern regions and the second authentication pattern regions encodes information in the first or second authentication pattern.

21. A method of detecting spoofing of a 3D object, using a 2D representation of the 3D object, in a mobile object authentication process, the method comprising:

a) capturing, via a front-facing camera of a mobile device,

i) a first image data of the 3D object while displaying, via a front-facing screen of the mobile device, a first authentication pattern, the first authentication pattern comprising a plurality of first authentication pattern regions, wherein at least one of the first authentication pattern regions varies from another first authentication pattern region in at least one of: brightness, position, size, shape, and color over time causing a first variance of lighting effects, wherein the first image data comprises a first set of highlights and shadows on the 3D object over time, and

ii) a second image data of the 3D object while displaying, via the front-facing screen, the second authentication pattern after displaying the first authentication pattern, wherein the second authentication pattern is different from the first authentication pattern, the second authentication pattern comprising a plurality of second authentication pattern regions, wherein at least one of the second authentication pattern regions varies from another second authentication pattern regions in at least one of brightness, position, size, shape, and color causing a second variance of lighting effects, wherein the second image data comprises a second set of highlights and shadows on the 3D object over time;

b) calculating a difference between the first set of highlights and shadows and the second set of highlights and shadows to determine a current spatial characteristic of the 3D object; and

c) determining if spoofing of the 3D object, using the 2D representation, is attempted in the mobile authentication process by comparing the current spatial characteristic of the 3D object with a stored reference spatial characteristic of the 3D object.