

CLAIMS

1. A system for providing selective access to resources available in connection with a computing device based on a deep learning method, said system comprising:
 - (a) the computing device comprising a digital processor, a memory module, an operating system, and non-transitory storage media comprising instructions executable by the digital processor; and
 - (b) at least one camera associated with the computing device and configured to take at least one image of a human palm print of a first user, wherein the human palm print does not have a physical contact with the computing device;
 - (c) a detector module configured to:
 - (1) use sliding-window-based local classifiers to analyze the at least one image to label palm and non-palm pixels by classification scores, and
 - (2) locate and segment a region of interest of the human palm print;
 - (d) a conversion processor configured to:
 - (1) use small sampling windows within the region of interest to identify image patches encompassing characteristic biometric features of the human palm print, and
 - (2) extract a signature from pixel-level data of the image patches, wherein the signature ~~comprises a histogram of edge orientations~~, is unique to the first user and is used to distinguish the first user from a second user, and wherein the extracting the signature comprises (i) creating a histogram of edge orientations in a plurality of image patches and (ii) using a clustering algorithm to compare the histogram with prototypes derived from a training step; and
 - (e) an authentication and identification engine configured to determine an access to one or more of the resources based upon the signature and at least one database containing a plurality of user models.
2. The system of claim 1, further comprising a learning processor configured to improve the plurality of user models with new data, wherein the learning processor selectively includes the at least one image of the human palm print, the pixel-level data of the image patches, and the signature to augment said database and said authentication and identification engine.

3. The system of claim 1, wherein the computing device comprises a mobile device.
4. The system of claim 1, wherein the computing device comprises a desktop device.
5. The system of claim 1, wherein the computing device comprises a stationary embedded device.
6. The system of claim 1, wherein the computing device includes a flash component that selectively activates at the time of image capture to provide minimum sufficient light for region of interest detection, feature extraction and signature processing of the image of the human palm print.
7. The system of claim 1, wherein the conversion processor uses descriptors extracted from patches over the region of interest.
8. The system of claim 7, wherein the descriptors are encoded into high dimensional sparse vectors.
9. The system of claim 8, wherein the sparse vectors are pooled into at least one group.
10. The system of claim 1, wherein the signature is computed from a Bag of Features or multiple Bags of Features representations.
11. The system of claim 1, wherein the detector module uses Haar Wavelets and AdaBoost algorithms.
12. The system of claim 1, wherein the detector module uses support vector machines.
13. The system of claim 1, wherein the detector module uses a convolutional neural network.
14. The system of claim 1, wherein the user models comprise a statistical model computed from a collection of a human's palm images.
15. The system of claim 1, wherein the user models comprise a Gaussian density model.
16. The system of claim 1, wherein the user models comprise a mixture of Gaussians density models.
17. The system of claim 1, wherein at least one of the resources is remote from the computing device.
18. The system of claim 1, wherein at least one of the resources is resident on the computing device.
19. The system of claim 1, wherein said at least one of the resources is an application.
20. The system of claim 1, wherein said at least one of the resources is a database.
21. The system of claim 1, wherein individual signatures of both palm print images of the first user are utilized together for authentication or identification of the first user.
22. The system of claim 1, wherein palm print authentication or identification is combined with one or more other biometric modalities.

23. The system of claim 21, wherein the one or more other biometric modalities comprise one or more of the following: passcodes, security questions, fingerprint recognition, facial recognition, iris recognition, written signature recognition, and other biometric and non-biometric modalities.
24. The system of claim 1, wherein an application selectively permits one or more users to conduct one or more transactions.
25. The system of claim 1, wherein a sequence of flash and non-flash images of the human palm print of the first user are utilized as part of an anti-spoofing mechanism to determine whether the presented hand is a 3-D object or a 2-D representation of a hand.
26. The system of claim 1, wherein image data captured during movement of the human palm print of the first user are utilized as part of an anti-spoofing mechanism to determine whether the presented hand is a 3-D object or a 2-D representation of a hand.
27. The system of claim 1, wherein a sequence of flash and non-flash images of the human palm print of the first user as well as one or more time intervals between successive images are utilized as part of an anti-spoofing mechanism to determine whether an adversary is attempting to utilize a previously-recorded sequence of images for authentication or identification.
28. The system of claim 1, wherein all of the first user's previously used images are stored for comparison against new images as part of an anti-spoofing mechanism to determine whether an adversary is attempting to utilize previously-recorded images for authentication or identification.
29. The system of claim 1, wherein transaction information or other data is embedded within a timing of a sequence of images or flash patterns as part of an anti-spoofing mechanism to determine whether the image sequence provided for authentication or identification matches the information from the transaction itself.

other biological hazards between people. In the case of individual devices being shared amongst multiple people, contact-based methods of authentication and identification in which a user types an identifying string with his or her fingertips, or authenticates or identifies himself or herself through contact-based biometric methods, such as fingerprint or palm print recognition, among others, create risk of transferring said biological hazards via the shared contact medium.

SUMMARY OF THE INVENTION

[010] It is thus an object of the invention to provide a non-contact based biometric system and methodology that supports accurate, secure, and rapid authentication and identification of users and devices to provide selective access to resources accessible through camera-equipped devices.

[011] In one embodiment of the present invention, users of such camera-equipped devices (hereinafter referred to at times as "smartphones" for convenience, although the devices are to be understood as including all devices with a camera capability, including both mobile devices and stationary devices, such as desktop computers) who are required to identify or authenticate themselves as a condition of obtaining access to one or more resources take one or a series of photos of their palm or both palms using the smartphone camera. The system of the present invention then employs computer vision technology to analyze the palm print image and either verify that the palm print signature matches the user's model in a database (user authentication) or find the matching user model among many models in a database (user identification).

[012] Further features and aspects of the present invention will become apparent from the following detailed description of exemplary embodiments in connection with reference to the attached figures.

[012A] The present disclosure provides a system for providing selective access to resources available in connection with a computing device based on a deep learning method comprising software executed on suitable computer hardware, said system comprising:

—— (a) ~~at least one camera associated with said device, said camera being capable of taking at least one photograph of a human palm print;~~

—— (b) ~~a detector module using local classifiers to locate and segment the region of interest of the palm without physical contact;~~

—— (c) ~~a conversion processor which converts raw pixel data associated with said region of interest of a human palm print into a unique signature associated with said palm print; and~~

~~— (d) an authentication and identification engine, said authentication and identification engine determining whether access to one or more of said resources should be granted based upon said unique signature and at least one database containing a plurality of user models.~~

- (a) the computing device comprising a digital processor, a memory module, an operating system, and non-transitory storage media comprising instructions executable by the digital processor; and
- (b) at least one camera associated with the computing device and configured to take at least one image of a human palm print of a first user, wherein the human palm print does not have a physical contact with the computing device;
- (c) a detector module configured to:
 - (1) use sliding-window-based local classifiers to analyze the at least one image to label palm and non-palm pixels by classification scores, and
 - (2) locate and segment a region of interest of the human palm print;
- (d) a conversion processor configured to:
 - (1) use small sampling windows within the region of interest to identify image patches encompassing characteristic biometric features of the human palm print, and
 - (2) extract a signature from pixel-level data of the image patches, wherein the signature is unique to the first user and is used to distinguish the first user from a second user, and wherein the extracting the signature comprises (i) creating a histogram of edge orientations in a plurality of image patches and (ii) using a clustering algorithm to compare the histogram with prototypes derived from a training step; and
- (e) an authentication and identification engine configured to determine an access to one or more of the resources based upon the signature and at least one database containing a plurality of user models.

BRIEF DESCRIPTION OF THE DRAWINGS

[013] Figure 1 is a diagram depicting the major components of the system of the present invention in a preferred embodiment thereof;