

A process for detecting presentation attacks on face recognition capture devices has been proposed in the document of S. Bharadwaj, T.I. Dhamecha, M. Vatsa and R. Singh, *Computationally efficient face spoofing detection with motion magnification*, in 2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops, pages 105-110, IEEE, 2013.

This process relies on using magnitude of motion magnification and texture descriptors, and is therefore not adapted for other kinds of biometric characteristics such as, for instance, irises that are relied upon on replay video attacks.

Therefore there is a need for a process allowing detection of replay video attacks in iris recognition.

SUMMARY OF THE INVENTION

Embodiments of the invention seek to provide a process for determining a video as being a spoof or a genuine record of a biometric characteristic, no matter which type of biometric characteristic is the subject of the video.

Accordingly, an aspect of the invention provides a process for determining a video of a biometric characteristic as being a spoof or a genuine recording of a live biometric characteristic, wherein the video comprises a temporal sequence of frames, the process being implemented in a system comprising a processing unit, characterized in that it comprises the steps of:

- preprocessing the video, said preprocessing comprising aligning the biometric characteristic on each frame of the video,
- determining a liveness score of the video, said determination comprising, for each frame of a plurality of frames:
 - o computing a difference between a motion intensity of a current frame and a motion intensity of each frame of a set of preceding frames,
 - o inferring, from said differences, a differential motion intensity of the current frame,
 - o inferring from the differential motion intensities of the plurality of frames a motion intensity of the video,
 - o comparing said motion intensity to a predetermined threshold, and assigning a liveness score to the video, depending on the

- The biometric characteristic on the video is an iris, and the preprocessing of the video comprises selecting (230) frames of the video to remove blinks of the eye.
- The process further comprises comparing the motion intensity of the video to a second threshold, and the step of assigning a liveness score to the video depends on the comparison of the motion intensity with the two thresholds.
- The differential motion intensity of each frame is further normalized by applying a sigmoid function to it.
- The motion intensity of the video is the mean of the normalized differential intensities, and said motion intensity is compared to the first threshold and, if it exceeds said threshold, the video is considered as being a spoof of the replay video type, and the liveness score assigned to the frame is 0.
- The second threshold is lower than the first threshold, the motion intensity of the video is compared to the second threshold, and, if below said threshold, the video is considered as being a spoof of the print type and the liveness score assigned to the frame is 0.

Another aspect of the invention provides a computer program product, comprising software code adapted to perform the process as described when implemented by a processing unit.

Another aspect of the invention relates to a processing unit that it is configured to implement the process as described.

Another aspect of the invention relates to an authentication or identification system, comprising a processing unit adapted to implement the above-mentioned process and a video camera adapted to acquire a video of a biometric characteristic, and to transfer said video to the processing unit.

The process according to embodiments of the invention may make it possible to differentiate between a replay video attack and a genuine recording of a biometric characteristic, by assessing a motion intensity in the video.

Indeed, the replay video attack has more frequency components than in a true recording of a biometric characteristic. Therefore if a motion intensity in a video is more important than average, the video can be considered as a spoof video.

The process may be particularly robust when the assessed motion intensity
5 of the video is a phase variation of the video.

Furthermore, the decomposition of the video frames into blocks may make the process more robust.

BRIEF DESCRIPTION OF THE DRAWINGS

10 The features and advantages of the invention will be apparent from the following more detailed description of certain embodiments of the invention and as illustrated in the accompanying drawings, in which:

- Figure 1 schematically shows an authentication or identification system adapted to perform a process according to an embodiment of the invention.
- 15 - Figure 2a schematically shows the main steps of the process according to an embodiment of the invention.
- Figure 2b schematically shows the computation steps of a frame differential phase information.
- Figure 2c schematically shows the implementation of the step of computing
20 differential phase information of a frame.

DETAILED DESCRIPTION OF AT LEAST AN EMBODIMENT OF THE INVENTION

System for authentication or identification

25 With reference to figure 1, a system 1 for authentication or identification of an individual is shown. This system is preferably used for controlling access rights, for instance of individuals wishing to enter a secured zone.

The system 1 comprises a video camera 11 and a processing unit 12, connected, either by a wire or wirelessly, to the video camera in order to receive
30 video recordings from said camera. In an embodiment, the system is integrated in a portable device such as a smartphone, a tablet or the like. In another embodiment, the video camera can be remote from the processing unit, for instance in an installation where the camera is at the entrance of a secured zone and the processing unit is in a separate room.

CLAIMS

1. A process for determining a video of a biometric characteristic as being a spoof or a genuine recording of a live biometric characteristic, wherein the video comprises a temporal sequence of frames, the process being implemented in a system comprising a processing unit, characterized in that it comprises the steps of:
 - preprocessing the video, said preprocessing comprising aligning the biometric characteristic on each frame of the video,
 - 10 - determining a liveness score of the video, said determination comprising, for each frame of a plurality of frames:
 - o computing a difference between a motion intensity of a current frame and a motion intensity of each frame of a set of preceding frames,
 - o inferring, from said differences, a differential motion intensity of the current frame,
 - 15 o inferring from the differential motion intensities of the plurality of frames a motion intensity of the video,
 - o comparing said motion intensity to a predetermined threshold, and assigning a liveness score to the video, depending on the comparison of the motion intensity of the video with the threshold,
 - 20 and
 - according to the liveness scores of the video, determining whether the video is a genuine recording of a biometric characteristic or a spoof.
- 25 2. A process according to claim 1, wherein the motion intensity of a frame comprises phase variation of the frame, and motion intensity of the video comprises phase variation of the video.
3. A process according to claim 1 or 2, wherein motion intensity of the video is
 - 30 inferred from differential motion intensities of at least ten frames of the video.

4. A process according to claim 1 to 3, wherein the set of frames for computation of the motion intensity difference with the current frame comprises from three to eight frames, and preferably five frames preceding the current frame.
5. A process according to any of claims 1 to 4, wherein each frame is divided into non-overlapping blocks of constant size, and the computation of the difference in motion intensity between two frames is carried out by computing, for every block in the current frame, the difference between a motion intensity of the block and a motion intensity of a corresponding block of each of the set of previous frames,
and the differential motion intensity of the current frame is obtained by :
- electing, for each block of the current frame, the maximum motion intensity difference between said block and the corresponding block of each of the set of previous frames, and
 - summing the maximum motion intensities of all the blocks in the frame.
6. A process according to any of the preceding claims, wherein the preprocessing step further comprises a step of magnifying the motion in the video.
7. A process according to claim 6, wherein the motion magnification is a phase-variation magnification and comprises:
- decomposing the video using a Fast Fourier Transform,
 - applying a bandpass filter to the phase,
 - applying an amplification factor to at least some phase components, and
 - implementing an inverse Fourier Transform to reconstruct the video.
8. A process according to any of the preceding claims, wherein the biometric characteristic on the video is an iris, and the preprocessing of the video comprises selecting frames of the video to remove blinks of the eye.
9. A process according to any of preceding claims, further comprising comparing the motion intensity of the video to a second threshold, and the step of assigning a liveness score to the video depends on the comparison of the motion intensity with the two thresholds.

10. A process according to any of the preceding claims, wherein the differential motion intensity of each frame is further normalized by applying a sigmoid function to it.
- 5 11. A process according to claim 10, wherein the motion intensity of the video is the mean of the normalized differential intensities, and said motion intensity is compared to the first threshold and, if it exceeds said threshold, the video is considered as being a spoof of the replay video type, and the liveness score assigned to the frame is 0.
- 10 12. A process according to claim 10 or 11 in combination with claim 9, wherein the second threshold is lower than the first threshold, the motion intensity of the video is compared to the second threshold, and, if below said threshold, the video is considered as being a spoof of the print type and the liveness score assigned to the
- 15 frame is 0.
13. A computer program product, comprising software code adapted to perform the process according to any of the preceding claims when implemented by a processing unit.
- 20 14. A processing unit, characterized in that it is configured to implement the process according to any of claim 1 to 12.
- 25 15. An authentication or identification system, comprising a processing unit according to claim 14 and a video camera adapted to acquire a video of a biometric characteristic, and to transfer said video to the processing unit.