ALLNAMES:(YOTI LTD)

37 results Offices all Languages en Stemming true Single Family Member false Include NPL false

Sort: Pub Date Desc Per page: 10 View: All 1 / 4 Machine translation

1. **3968194** DIGITAL IDENTITY EP - 16.03.2022

Int.Class G06F 21/33 **Appl.No** 21203787 **Applicant** YOTI HOLDING LTD **Inventor** LOUGHLIN-MCHUGH ELEANOR SIMONE FREDERIKA

A digital identity system is provided, comprising a computer interface for receiving electronic messages and one or more hardware processors configured to execute an enrolment module, a credential creation module, and a validation service. The enrolment module is configured to receive a data item captured from an identity document, and create a digital identity comprising the data item. The credential creation module is configured to transmit to a user device via the computer interface a credential for storing at the user device, the credential being bound to the digital identity. The validation service is configured to receive an electronic message comprising the credential and identifying a target device, validate the credential, and if the credential is valid, use the credential to transmit from the digital identity system to the target device, an electronic message so as to render the data item of the digital identity available to the target device.

2. **2598028** AGE ESTIMATION GB - 16.02.2022

Int.Class G06V 40/16 **Appl.No** 202108530 **Applicant** YOTI HOLDING LTD **Inventor** FRANCISCO ANGEL GARCIA RODRIGUEZ

A neural network processes captured image and audio data to compute human age estimate data. A facial feature extractor of the neural network comprises a plurality of neural network processing layers configured to process the image data to compute a facial feature set, which encodes human facial features exhibited in the captured image data. A voice feature extractor of the neural network comprises a plurality of neural network processing layers configured to process the audio data to compute a voice feature set, which encodes human voice features exhibited in the captured audio data. A combined feature set is computed by combining the voice and facial feature sets. An age estimator comprising at least one neural network processing layer is configured to process the combined feature set to compute the human age estimate data.

3. **3951750** LIVENESS DETECTION SAFE AGAINST REPLAY ATTACK EP - 09.02.2022

Int.Class G06F 21/32 **Appl.No** 21198719 **Applicant** YOTI HOLDING LTD **Inventor** TREMOULHEAC BENJAMIN ROBERT

A computer-implemented liveness detection method comprising implementing, by a liveness detection system, the following steps: selecting at random a first set of one or more parameters of a first liveness test; transmitting, to a user device available to an entity, the first parameter set, thereby causing the user device to perform the first liveness test according to the first parameter set; receiving from the user device results of the first liveness test; receiving results of a second liveness test pertaining to the entity; detecting whether a timeout condition has occurred, the timeout condition caused by an unacceptable delay in receiving the results relative to a timing of the transmitting step; and if the timeout condition occurs, refusing the entity access to a remote computer system, otherwise determining whether the entity is a living being using the results of the liveness tests.

4. **3888001** ANTI-SPOOFING EP - 06.10.2021

Int.Class G06K 9/00 **Appl.No** 19816642 **Applicant** YOTI HOLDING LTD **Inventor** NIKITIDIS SYMEON

A method of configuring an anti-spoofing system to detect if a spoofing attack has been attempted, in which an image processing component of the anti-spoofing system is trained to process 2D verification images according to a set of image processing parameters, in order to extract depth information from the 2D verification images. The configured anti-spoofing system comprises an anti-spoofing component which uses an output from the processing of a 2D verification image by the image processing component to determine whether an entity captured in that image corresponds to an actual human or a spoofing entity. The image processing parameters are learned during the training from a training set of captured 3D training images of both actual humans and spoofing entities, each 3D training image comprising 2D image data and corresponding depth data, by: processing the 2D image data of each 3D training image according to the image processing parameters, so as to compute an image processing output for comparison with the corresponding depth data of that 3D image; and adapting the image processing parameters in order to match the image processing outputs to the corresponding depth data, thereby training the image processing component to extract depth information from 2D verification images.

5. **2593301** ANTI-SPOOFING GB - 22.09.2021

Int.Class G06K 9/00 **Appl.No** 202105432 **Applicant** YOTI HOLDING LTD **Inventor** FRANCISCO ANGEL GARCIA RODRIGUEZ

Anti-spoofing technology is provided for verifying a user of a fixed computer terminal. Image data of at least one verification image is received, as captured by an image capture device of the fixed computer terminal at a time corresponding to a request for access to a restricted function of the fixed computer terminal. User verification is applied to determine whether to grant access to the restricted function of the fixed computer terminal. A differential feature descriptor is determined, which encodes feature differences between the verification image data and image data of at least one unobstructed background image as captured by the image capture device. An anti-spoofing classifier processes the differential feature descriptor to classify it in relation to real and spoofing classes. Access to the restricted function of the fixed computer terminal is refused or granted based on the classification of the differential feature descriptor by the anti-spoofing classifier.

6. **3859717** LIVENESS DETECTION EP - 04.08.2021

Int.Class G06F 21/32 **Appl.No** 21165242 **Applicant** YOTI HOLDING LTD **Inventor** TREMOULHEAC BENJAMIN ROBERT

There is provided a computer implemented method of regulating access to a computer system. A request for access and a moving image of a user's skin captured with an image capture device of a user device is received from the user device. A heartbeat detection algorithm is applied to the image for detecting skin-colour changes indicative of a heartbeat, which determines multiple time series of colour values, each for a different location on the user's skin, and determines whether the time series exhibit variations are indicative of a heartbeat. The request for access is refused unless the heartbeat detection algorithm detects a series of skin-colour changes in the moving image indicative of a heartbeat. The heartbeat detection algorithm uses the multiple time series to determine a spectrum of skin colour change frequencies exhibited by the user's skin, wherein the request is rejected if the spectrum is classified as fraudulent.

7. **2588538** ANTI-SPOOFING GB - 28.04.2021

Int.Class G06K 9/00 **Appl.No** 202018751 **Applicant** YOTI HOLDING LTD **Inventor** SYMEON NIKITIDIS

A method of configuring an anti-spoofing system to detect if a spoofing attack has been attempted, in which an image processing component of the anti-spoofing system is trained to process 2D verification images according to a set of image processing parameters, in order to extract depth information from the 2D verification images. The configured anti-spoofing system comprises an anti-spoofing component which uses an output from the processing of a 2D verification image by the image processing component to determine whether an entity captured in that image corresponds to an actual human or a spoofing entity. The image processing parameters are learned during the training from a training set of captured 3D training images of both actual humans and spoofing entities, each 3D training image comprising 2D image data and corresponding depth data, by: processing the 2D image data of each 3D training image according to the image processing parameters, so as to compute an image processing output for comparison with the corresponding depth data of that 3D image; and adapting the image processing parameters in order to match the image processing outputs to the corresponding depth data, thereby training the image processing component to extract depth information from 2D verification images.

8. **3807794** AGE VERIFICATION EP - 21.04.2021

Int.Class G06F 21/32 **Appl.No** 19739522 **Applicant** YOTI HOLDING LTD **Inventor** RODRIGUEZ FRANCISCO ANGEL GARCIA

Image processing systems and methods are provided for authorizing the performance at a computer terminal of an age-restricted activity. An estimated human age is determined based on human characteristics of a structure detected in an image captured at the computer terminal. It is determined whether the structure exhibits at least one liveness characteristic indicating the human characteristics from which the estimated human age is determined have been captured directly from a living human at the computer terminal. A positive determination is made as to whether performance of the age-restricted activity is authorized if the estimated human age meets a predetermined age requirement and the structure is determined to exhibit at least one liveness characteristic, and a negative determination is made if: i] the estimated human age does not meet the predetermined age requirement; and/or ii] the structure is not determined to exhibit at least one liveness characteristic.

9. **3794475** GENERATING ELECTRONIC SIGNATURES EP - 24.03.2021

Int.Class G06F 21/32 **Appl.No** 19726983 **Applicant** YOTI HOLDING LTD **Inventor** HUSSAIN ALTTAF

According to a first aspect of the present invention, there is provide a method of electronically signing content. Content to be signed and an attribute sharing item are presented at a signing device associated with a signer. It is detecting that the signer has accessed the attribute sharing item to provide one or more identity attributes which uniquely identify the signer. It is also detecting that the signer has initiated a signing action at the signing device. The signing action and the identity attributes are transmitted to a signing service which is configured to create an electronic signature including encrypting the content to be signed and the one or more identity attribute.

10. **2587075** PROVING IDENTITY GB - 17.03.2021

Int.Class G06F 21/34 **Appl.No** 202009471 **Applicant** YOTI HOLDING LTD **Inventor** CYRILLE QUEMIN

A proof of identity device including electronic storage configured to store a plurality of identity payloads, the proof identity device maybe a smartcard or tag. Each payload having an independently verifiable payload signature as determined by cryptographically signing that identity payload individually. Wherein each identity payload is associated with an identified attribute type and includes an identity attribute of that attribute type. The attributes may include name, biometric such as facial image, age, nationality. Performing an identity sharing function by processing a received interrogation signal, from an identity-requesting device, to determine therefrom at least one requested attribute type, accessing the electronic storage to match the requested attribute type to the attribute type associated with one of the stored identity payloads, and providing that identity payload and its payload signature to the identity requesting device directly. The device may provide both identity-sharing and electronic payment functions.