

Technical Disclosure Commons

Defensive Publications Series

October 2020

A Method For Iris Liveness Detection Using Passive Light Trigger

SUNPREET SINGH ARORA

Visa

KIM WAGNER

Visa

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

ARORA, SUNPREET SINGH and WAGNER, KIM, "A Method For Iris Liveness Detection Using Passive Light Trigger", Technical Disclosure Commons, (October 27, 2020)

https://www.tdcommons.org/dpubs_series/3701



This work is licensed under a [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/).

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

**A METHOD FOR IRIS LIVENESS DETECTION USING
PASSIVE LIGHT TRIGGER**

VISA INTERNATIONAL SERVICE ASSOCIATION

**INVENTORS: SUNPREET SINGH ARORA; AND
KIM WAGNER**

TECHNICAL FIELD

[0001] This disclosure relates to a passive liveness detection method for a camera-based iris biometric system.

BACKGROUND

[0002] One of the challenging security problems for biometric systems is to determine whether the captured biometric sample is of a genuine user's biometric trait (i.e. live biometric sample) or a synthetic artifact (i.e. fake/spoof biometric sample), for example, a printed photo or a replay of a 2-Dimensional (2D) digital recording. This step called liveness detection is typically a precursor to recognition. State-of-the-art biometric recognition systems use a variety of hardware or software-based mechanisms for liveness detection. As an example, a hardware-based mechanism for liveness detection projects several thousand Infrared (IR) dots on the face of the user being imaged to estimate 3D depth map. On the other hand, a software-based mechanism, for example, uses machine learning classifiers trained on live and fake data for liveness detection. The limitation of most hardware-based mechanisms is that they require specialized expensive hardware (for example, IR dot projector), and the limitation of typical software-based mechanisms is that they are designed to detect only a fixed set of fake artifacts, and are typically not generalizable to novel artifacts.

[0003] In order to overcome the above-mentioned shortcomings for an iris biometric system, the present invention uses a passive light source to produce a trigger that causes a detectable change in the eye being imaged for liveness detection.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Additional advantages and details are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0005] FIGURE 1a illustrates an exemplary environment for camera-based iris biometric system pertaining to liveness detection in accordance with some embodiments of the present disclosure. FIGURE 1b illustrates an exemplary environment for camera-based iris biometric

system pertaining to liveness detection and iris recognition in accordance with some embodiments of the present disclosure.

[0006] FIGURE 2 shows a detailed block diagram of a liveness detection system in accordance with some embodiments of the present disclosure.

[0007] FIGURE 3 illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

DESCRIPTION OF THE DISCLOSURE

[0008] It is to be understood that the present disclosure may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings and described in the following specification are simply exemplary and non-limiting embodiments or aspects. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0009] For purposes of the description hereinafter, the terms “end,” “upper,” “lower,” “right,” “left,” “vertical,” “horizontal,” “top,” “bottom,” “lateral,” “longitudinal,” and derivatives thereof shall relate to the disclosed subject matter as it is oriented in the drawing figures. However, it is to be understood that the disclosed subject matter may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings, and described in the following specification, are simply exemplary embodiments or aspects of the disclosed subject matter. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting unless otherwise indicated.

[0010] No aspect, component, element, structure, act, step, function, instruction, and/or the like used herein should be construed as critical or essential unless explicitly described as such. Also, as used herein, the articles “a” and “an” are intended to include one or more items and may be used interchangeably with “one or more” and “at least one.” Furthermore, as used herein, the term “set” is intended to include one or more items (e.g., related items, unrelated

items, a combination of related and unrelated items, and/or the like) and may be used interchangeably with “one or more” or “at least one.” Where only one item is intended, the term “one” or similar language is used. Also, as used herein, the terms “has,” “have,” “having,” or the like are intended to be open-ended terms. Further, the phrase “based on” is intended to mean “based at least partially on” unless explicitly stated otherwise.

[0011] As used herein, the terms “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. In some non-limiting embodiments or aspects, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0012] As used herein, the term “computing device” may refer to one or more electronic devices that are configured to directly or indirectly communicate with or over one or more networks. A computing device may be a mobile or portable computing device, a desktop computer, a server, and/or the like. Furthermore, the term “computer” may refer to any computing device that includes the necessary components to receive, process, and output data, and normally includes a display, a processor, a memory, an input device, and a network interface. A “computing system” may include one or more computing devices or computers. An “application” or “application program interface” (API) refers to computer code or other data stored on a computer-readable medium that may be executed by a processor to facilitate the interaction between software components, such as a client-side front-end and/or server-side back-end for receiving data from the client. An “interface” refers to a generated display, such as one or more graphical user interfaces (GUIs) with which a user may interact, either directly or indirectly (e.g., through a keyboard, mouse, touchscreen, etc.). Further, multiple computers, e.g., servers, or other computerized devices, such as an autonomous vehicle including a vehicle

computing system, directly or indirectly communicating in the network environment may constitute a “system” or a “computing system”.

[0013] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting of the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it being understood that software and hardware can be designed to implement the systems and/or methods based on the description herein.

[0014] Some non-limiting embodiments or aspects are described herein in connection with thresholds. As used herein, satisfying a threshold may refer to a value being greater than the threshold, more than the threshold, higher than the threshold, greater than or equal to the threshold, less than the threshold, fewer than the threshold, lower than the threshold, less than or equal to the threshold, equal to the threshold, etc.

[0015] In an embodiment, the present disclosure may relate to a method for passive liveness detection. The method includes: detecting an initiation of transaction on one of a user device and a payment terminal in supervised/unsupervised payment environments, introducing a passive light trigger to record real-time involuntary biological response of user’s eye when the initiation of transaction is detected, comparing the recorded real-time involuntary biological response of the user’s eye to similar biological response of the user’s eye recorded at the time of enrollment and/or a previous successful transaction by a user stored in a database, and determining if the recorded real-time involuntary biological response of the presented eye is of a real user or spoof based on the comparison.

[0016] In an embodiment, the present disclosure may relate to a camera-based iris biometric system for passive liveness detection. The biometric system may include a processor and a memory communicatively coupled to the processor, wherein the memory stores processor-executable instructions, which on execution, cause the processor to detect an initiation of transaction on one of a user device and a payment terminal in supervised/unsupervised payment environments, introduce a passive light trigger to record real-time involuntary biological response of user’s eye when the initiation of transaction is

detected, compare the recorded real-time involuntary biological response of the user's eye to similar biological response of the user's eye recorded at the time of enrollment and/or a previous successful transaction by the user stored in a database, and determine if the recorded real-time involuntary biological response of the user's eye is real or spoof based on the comparison.

[0017] Typically, biometric systems may operate in two stages: enrollment stage and recognition stage. During the enrollment stage, a biometric sample of a user may be captured using a specific sensing mechanism such as visible or Infrared (IR) camera for face and/or iris, microphone for voice and the like. The biometric sample may refer to iris of user's eye. A mathematical representation may be generated from the captured biometric sample using a template generator. The mathematical representation may, also, be referred as a (biometric) template, which is a digital representation of the unique features obtained from the captured biometric sample of the user. Thereafter, the captured biometric sample and respective template may be stored in a database. The stored template are then used in the biometric authentication and identification process. The recognition stage may include two scenarios: (1) a claim of identity may be made by a user (also, referred as verification process) and (2) the identity of a user may need to be explicitly established (also, referred as identification process). In both these scenarios, a biometric sample from the user may be required. During the recognition stage, the biometric sample of the user may be captured. Subsequently, a template may be generated from the captured biometric sample and compared against the templates stored in the database. This comparison operation may yield similarity score between the captured biometric sample and the biometric sample stored in the database 113 for that user. The similarity score may be further compared against a predefined threshold value to determine if the comparison operation resulted in a match or not. The predefined threshold value may be based on permissible error (for example, 1 in 1000 or 1 in 10000 false accepts). If the comparison results in a match, then the verification process or the identification process may be considered successful and the user may be allowed to proceed with next step. However, if the comparison result is not a match, then the verification process or the identification process may be considered unsuccessful and the user may not be allowed to proceed with the next step. The drawback of the above-mentioned steps used in the process for verification and identification is that it fails to recognize during the recognition stage whether the captured biometric sample is from a genuine user's biometric trait or a synthetic artifact, for example, printed photo or

replay of a 2D digital recording. As a result, the biometric systems may be prone to serious security risks.

[0018] The present invention overcomes the above-mentioned shortcomings by introducing an additional step, which is performed prior or precursor to the recognition stage. This step is called passive liveness detection. The passive liveness detection is explained below with reference to FIGURE 1a.

[0019] FIGURE 1a illustrates an exemplary environment for camera-based iris biometric system pertaining to liveness detection in accordance with some embodiments of the present disclosure.

[0020] As shown in FIGURE 1a, the environment includes a biometric sample 101, a liveness detection system 103, a template generator 107, a comparator 109 and a database 113. The liveness detection system 103 may, also, be referred as a liveness detector. In one embodiment, the liveness detection system 103 may be part of user device such as a mobile phone, a personal computer or a laptop. When the liveness detection system 103 is a part of user device, the liveness detection system 103 may use the in-built camera and/or additional features of the user device. In another embodiment, the liveness detection system 103 may be part of a payment terminal in supervised/unsupervised payment environment. When the liveness detection system 103 is part of payment terminal, the liveness detection system 103 may comprise camera device to capture the biometric sample 101. The biometric sample 101 may include, but not limited to, one or both irises of user eyes.

[0021] In the embodiment, the liveness detection system 103 may exchange data with the database 113 using wired or wireless communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, Radio Corporation of America (RCA) connector, stereo, IEEE®-1394 high speed serial bus, serial bus, Universal Serial Bus (USB), infrared, Personal System/2 (PS/2) port, Bayonet Neill-Concelman (BNC) connector, coaxial, component, composite, Digital Visual Interface (DVI), High-Definition Multimedia Interface (HDMI®), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (VGA), IEEE® 802.11b/g/n/x, Bluetooth, cellular e.g., Code-Division Multiple Access (CDMA), High-Speed Packet Access (HSPA+), Global System for Mobile communications (GSM®), Long-Term Evolution (LTE®), Worldwide interoperability for Microwave access (WiMax®), or the like.

The database 113 may be populated or stored with at least one of biometric sample and respective biometric data (i.e. a template or a digital representation) of a user. The biometric sample and biometric data stored in the database 113 may be referred as historic sample and historic data, respectively. Here, the historic sample and historic data may be previously recorded at the time of enrollment or previous transaction for liveness detection purposes.

[0022] The database 113 may, also, be updated at predefined intervals of time with at least one of biometric sample and respective biometric data of a new user.

[0023] The operation of biometric system pertaining to liveness detection may be explained as following. When a user is initiating a transaction from his/her user device, the liveness detection system 103 may identify if artifact (iris/eye) presented to the system 103 is of a real user or a spoof/fake. Here, the artifact may refer to a recorded real-time involuntary biological response of the user's eye to a passive light trigger. For identifying if the artifact (iris/eye) presented to the system 103 is of a real user or a spoof/fake, the liveness detection system 103 may first focus a light source of a pre-specified wavelength on user's eye. The pre-specified wavelength may be, but not limited to, an IR light wavelength. The IR wavelength range may be, but not limited, from 850 nm to 910 nm. The response of user's eye to the pre-specified wavelength may be recorded by the liveness detection system 103. The response may comprise at least one of micro-movements in iris, color changes in eye in visible and/or specular reflections in IR domain, unique patterns in iris and colored ring around iris in user's eyes. These responses are characteristic biological responses of a live biometric sample to a passive challenge mechanism (for example, a light of a pre-specified wavelength). For recording the response, the liveness detection system 103 may use appropriate camera lens shutter speed, aperture, and image sensor sensitivity settings of the in-built camera of the user device or the camera at a payment terminal depending upon where iris is captured. Once the response is recorded, the recorded real-time involuntary biological response may be subjected to processing to obtain measurement data. The measurement data may be a digital representation of the unique features obtained from the response of user's eye. The measurement data may be compared with historic data of the user stored in the database 113. The historic data of the user may refer to previously recorded biological response of the user to similar light trigger captured at the time of enrollment or previous transaction for liveness detection purposes. In an embodiment, if the comparison of the measurement data and the historic data of the user is equal or greater than a predefined threshold, then the liveness detection system 103 may

consider user initiating the transaction to be a real user and consequently, may allow the user to proceed with subsequent step in the transaction. In another embodiment, a machine learning classifier such as support vector machines, neural network and the like may be used to yield the comparison result. However, if the comparison of the measurement data and the historic data of the user is less than the predefined threshold, then the liveness detection system 103 may consider user initiating the transaction to be a spoof and consequently, may prevent the user from proceeding with the transaction, shown as reference 105. This process of checking by the liveness detection system 103 to identify if the user initiating the transaction is a real user or a spoof is typically performed prior to the recognition stage. In another embodiment, the measurements/features derived primarily for liveness detection may be used, in addition to iris biometric templates, to aid in biometric recognition itself. One potential way to achieve this is by combining the biometric comparison score with liveness score, as shown in Figure 1b.

[0024] FIGURE 2 shows a detailed block diagram of a liveness detection system in accordance with some embodiments of the present disclosure.

[0025] In the embodiment, the liveness detection system 103 may identify if the artifact (iris/eye) presented to the system 103 by the user initiating the transaction is of a real user or a spoof/fake. The liveness detection system 103 may include an I/O interface 201, a processor 203 and a memory 205. The I/O interface 201 may be configured to record responses that are characteristic biological responses of a live biometric sample (eye/iris) to a passive challenge mechanism. Analogously, the I/O interface 201 may be configured to communicate if the artifact (iris/eye) presented to the system 103 by the user initiating the transaction is of a real user or a spoof/fake based on recorded responses. The I/O interface 201 may employ wired or wireless communication protocols/methods.

[0026] The biometric sample 101 and responses of the biometric sample 101 may be stored in the memory 205 in the form of a 1D vector or a 2D matrix. The memory 205 may be communicatively coupled to the processor 203 of the liveness detection system 103. The memory 205 may, also, store processor instructions which may cause the processor 203 to execute the instructions for passive liveness detection. The memory 205 may include, without limitation, memory drives, removable disc drives, etc. The memory drives may further include

a drum, magnetic disc drive, magneto-optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

[0027] The processor 203 may include at least one data processor for passive liveness detection. The processor 203 may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0028] The liveness detection system 103, in addition to the I/O interface 201 and processor 203 described above, may include data 207 and one or more modules 213, which are described herein in detail. In the embodiment, the data 207 may be stored within the memory 205. The data 207 may include, for example, image data 209 and other data 211.

[0029] The image data 209 may include at least one of biometric sample 101 and responses of the biometric sample 101 of a user in the form of images.

[0030] The other data 211 may store data, including temporary data and temporary files, generated by one or more modules 213 for performing the various functions of the liveness detection system 103.

[0031] In the embodiment, the data 207 in the memory 205 are processed by the one or more modules 213 present within the memory 205 of the liveness detection system 103. In the embodiment, the one or more modules 213 may be implemented as dedicated hardware units. As used herein, the term module refers to an Application Specific Integrated Circuit (ASIC), an electronic circuit, a Field-Programmable Gate Arrays (FPGA), Programmable System-on-Chip (PSoC), a combinational logic circuit, and/or other suitable components that provide the described functionality. In some implementations, the one or more modules 213 may be communicatively coupled to the processor 203 for performing one or more functions of the liveness detection system 103. The said modules 213 when configured with the functionality defined in the present disclosure will result in a novel hardware.

[0032] In one implementation, the one or more modules 213 may include, but are not limited to, a trigger module 215, a capture module 217 and a measurement module 219. The

one or more modules 213 may, also, include other modules 221 to perform various miscellaneous functionalities of the liveness detection system 103.

[0033] The trigger module 215 may detect an initiation of transaction on one of a user device and a payment terminal in supervised/unsupervised payment environments. When the initiation is detected, the trigger module 215 may introduce a passive light trigger to record real-time involuntary biological response of user's eye. The passive light trigger may be a light source of a pre-specified wavelength to trigger a small response in the eye of a use. This response may be at least one of movement of iris dilator, dilation of sphincter muscles and contraction of the pupil. This response is involuntary biological responses and not an explicit action that the user needs to do. As a result, this response to the light source is completely passive to the user, which the user may not be aware.

[0034] The capture module 217 may record/capture the real-time involuntary biological response triggered by the trigger module 215. The capture module 217 may capture the response using an iris camera by increasing its shutter speed, decreasing its aperture and tuning the Image Sensor Sensitivity (ISO) appropriately to compensate for the higher shutter speed so that additional noise is not introduced in the image capture process, for example, increasing the shutter speed by a factor of two or four and decreasing the camera aperture by the same factor to keep same exposure. The capture module 217 may capture multiple images in a short amount of time at high shutter speed.

[0035] The measurement module 219 may compare the recorded real-time involuntary biological response of the user's eye to similar biological response of the user's eye recorded at the time of enrollment and/or a previous successful transaction by the user stored in the database 113 and subsequently, determine if the recorded real-time involuntary biological response of the user's eye presented to the system 103 is of a real user or a spoof/fake based on the comparison. In detail, the measurement module 219 may perform following steps: (a) segmenting iris region from the captured image in to multiple frames using state of the art iris segmentation methods, (b) detecting landmarks in the segmented iris region in a first frame using a key point detection method such as Scale Invariant Feature Transform (SIFT) algorithm or Histogram of Oriented Gradients (HOG), (c) tracking the detected landmarks key points in subsequent frames to measure iris dilator movement and sphincter muscle movement and (d) saving the measurements as a (biometric) template in the database 113. The measurement

module 219 may compare the template with historic data of the user stored in the database 113 to determine if the user initiating transaction is real or spoof based on the comparison. This comparison operation may yield similarity score between the template and the historic data, which may be further compared against a predefined threshold value to determine if the comparison operation resulted in a match or not 111. The predefined threshold value may be based on permissible error (for example, 1 in 1000 or 1 in 10000 false accepts). If the similarity score is equal or greater than the predefined threshold value, then the liveness detection system 103 may consider user initiating the transaction to be a real user and consequently, may allow the user to proceed with subsequent step in the transaction. However, if the similarity score is less than the predefined threshold, then the liveness detection system 103 may consider user initiating the transaction to be a spoof and consequently, may prevent the user from proceeding with the transaction.

[0036] Some of the advantages of the present disclosure are listed below.

[0037] The present disclosure overcomes the need for complex and expensive hardware-based mechanism that includes projecting several thousand IR dots on a face being imaged to estimate 3D depth map for passive liveness detection.

[0038] The present disclosure overcomes the limitation of software-based mechanism that can detect only a fixed set of fake artifacts for passive liveness detection.

[0039] FIGURE 3 illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0040] In an embodiment, the computer system 300 may be used to implement the liveness detection system 103. The computer system 300 may include a central processing unit (“CPU” or “processor”) 302. The processor 302 may include at least one data processor for passive liveness detection. The processor 302 may include specialized processing units such as, integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0041] The processor 302 may be disposed in communication with one or more input/output (I/O) devices (312 and 313) via I/O interface 301. The I/O interface 301 employ

communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, radio corporation of America (RCA) connector, stereo, IEEE-1394 high speed serial bus, serial bus, universal serial bus (USB), infrared, personal system/2 (PS/2) port, bayonet neill-concelman (BNC) connector, coaxial, component, composite, digital visual interface (DVI), high-definition multimedia interface (HDMI), radio frequency (RF) antennas, S-Video, video graphics array (VGA), IEEE 802.11b/g/n/x, Bluetooth, cellular e.g., code-division multiple access (CDMA), high-speed packet access (HSPA+), global system for mobile communications (GSM), long-term evolution (LTE), worldwide interoperability for microwave access (WiMax), or the like, etc.

[0042] Using the I/O interface 301, the computer system 300 may communicate with one or more I/O devices such as input devices 312 and output devices 313. For example, the input devices 312 may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output devices 313 may be a printer, fax machine, video display (e.g., cathode ray tube (CRT), liquid crystal display (LCD), light-emitting diode (LED), plasma, plasma display panel (PDP), organic light-emitting diode display (OLED) or the like), audio speaker, etc.

[0043] In some embodiments, the processor 302 may be disposed in communication with a communication network 309 via a network interface 303. The network interface 303 may communicate with the communication network 309. The network interface 303 may employ connection protocols including, without limitation, direct connect, ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network 309 may include, without limitation, a direct interconnection, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. Using the network interface 303 and the communication network 309, the computer system 300 may communicate with a database 314, which may be the enrolled templates database 113. The network interface 303 may employ connection protocols include, but not limited to, direct connect, ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc.

[0044] The communication network 309 includes, but is not limited to, a direct interconnection, a peer to peer (P2P) network, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi and such. The communication network 309 may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, hypertext transfer protocol (HTTP), transmission control protocol/internet protocol (TCP/IP), wireless application protocol (WAP), etc., to communicate with each other. Further, the communication network 309 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0045] In some embodiments, the processor 302 may be disposed in communication with a memory 305 (e.g., RAM, ROM, etc. not shown in FIGURE 3) via a storage interface 304. The storage interface 304 may connect to memory 305 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as, serial advanced technology attachment (SATA), integrated drive electronics (IDE), IEEE-1394, universal serial bus (USB), fiber channel, small computer systems interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, redundant array of independent discs (RAID), solid-state memory devices, solid-state drives, etc.

[0046] The memory 305 may store a collection of program or database components, including, without limitation, user interface 306, an operating system 307, etc. In some embodiments, computer system 300 may store user/application data, such as, the data, variables, records, etc., as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle or Sybase.

[0047] The operating system 307 may facilitate resource management and operation of the computer system 300. Examples of operating systems include, without limitation, AppleTM MacintoshTM OS XTM, UNIXTM, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSDTM, Net BSDTM, Open BSDTM, etc.), Linux distributions (e.g., Red HatTM, UbuntuTM, K-UbuntuTM, etc.), International Business Machines (IBMTM) OS/2TM, Microsoft WindowsTM (XPTM, Vista/7/8, etc.), Apple iOSTM, Google AndroidTM, BlackberryTM operating system (OS), or the like. In some embodiments, the computer system 300 may

implement web browser 308 stored program components. Web browser 308 may be a hypertext viewing application, such as Microsoft™ Internet Explorer™, Google Chrome™, Mozilla Firefox™, Apple™ Safari™, etc. Secure web browsing may be provided using secure hypertext transport protocol (HTTPS), secure sockets layer (SSL), transport layer security (TLS), etc. Web browsers 308 may utilize facilities such as AJAX, DHTML, Adobe™ Flash, Javascript, Application Programming Interfaces (APIs), etc.

[0048] According to some non-limiting embodiments or aspects, a computer program product including at least one non-transitory computer-readable medium including one or more instructions for passive liveness detection that, when executed by at least one processor, cause the at least one processor to: detect an initiation of transaction on one of a user device and a payment terminal in supervised/unsupervised payment environments, introduce a passive light trigger to record real-time involuntary biological response of user's eye when the initiation of transaction is detected, compare the recorded real-time involuntary biological response of the user's eye to similar biological response of the user's eye recorded at the time of enrollment and/or a previous successful transaction by the user stored in a database, and determine if the recorded real-time involuntary biological response of the user's eye is real or spoof based on the comparison.

[0049] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items, or meant to be limited to only the listed item or items. It must also be noted that as used herein, the singular forms "a," "an," and "the" include plural references unless the context clearly dictates otherwise.

[0050] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory. Examples include random access memory (RAM), read-only memory (ROM), volatile memory, nonvolatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0051] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

A METHOD FOR IRIS LIVENESS DETECTION USING PASSIVE LIGHT TRIGGER

ABSTRACT

The present disclosure relates to a passive liveness detection method for a camera-based iris biometric system. The method comprising: detecting an initiation of transaction on one of a user device and a payment terminal in supervised/unsupervised payment environments, introducing a passive light trigger to record real-time involuntary biological response of user's eye when the initiation of transaction is detected, comparing the recorded real-time involuntary biological response of the user's eye to similar biological response of the user's eye recorded at the time of enrollment and/or a previous successful transaction by the user stored in a database, and determining if the artifact being presented to the iris biometric system at the time of transaction is real or spoof based on the comparison. The present disclosure uses shutter speed and aperture of camera lens, and image sensor sensitivity settings coupled with a passive light trigger for liveness detection. This approach overcomes the need for specialized expensive hardware and the limitation of detecting a fixed set of fake artifacts (spoofs) for passive liveness detection.

FIGURE 1

1/4

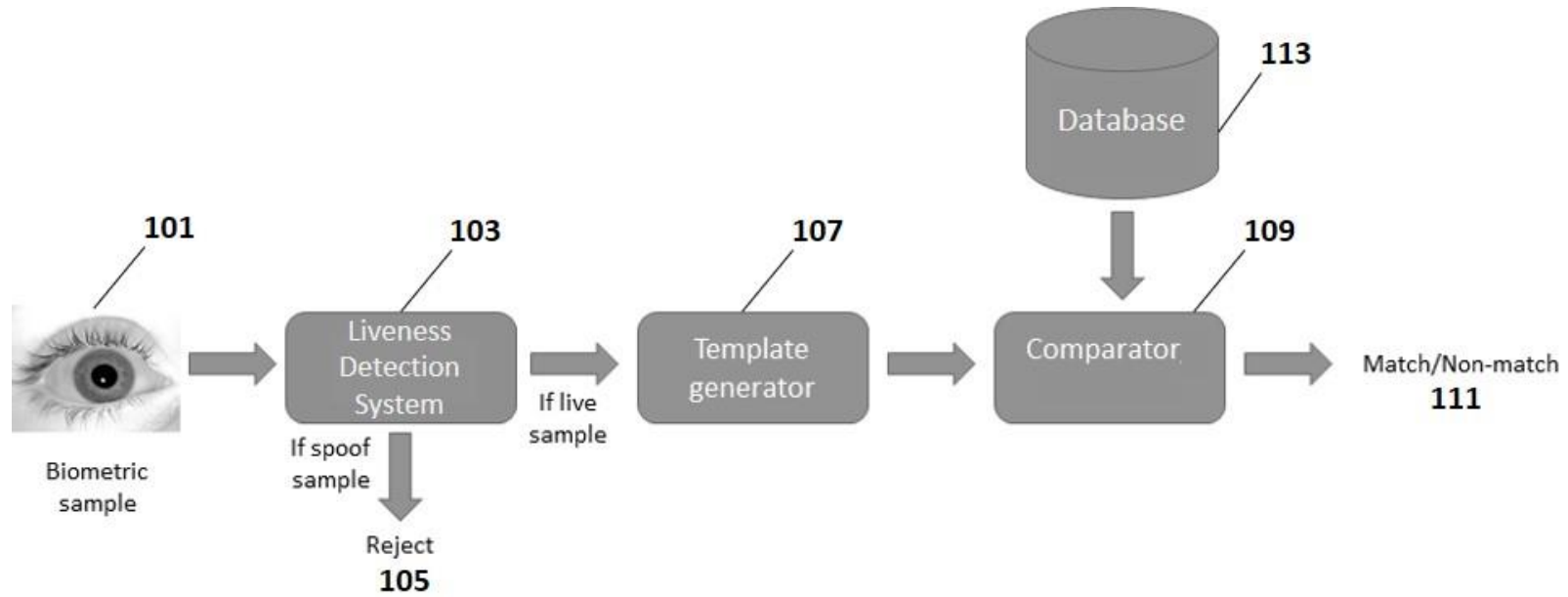


FIG. 1a

2/4

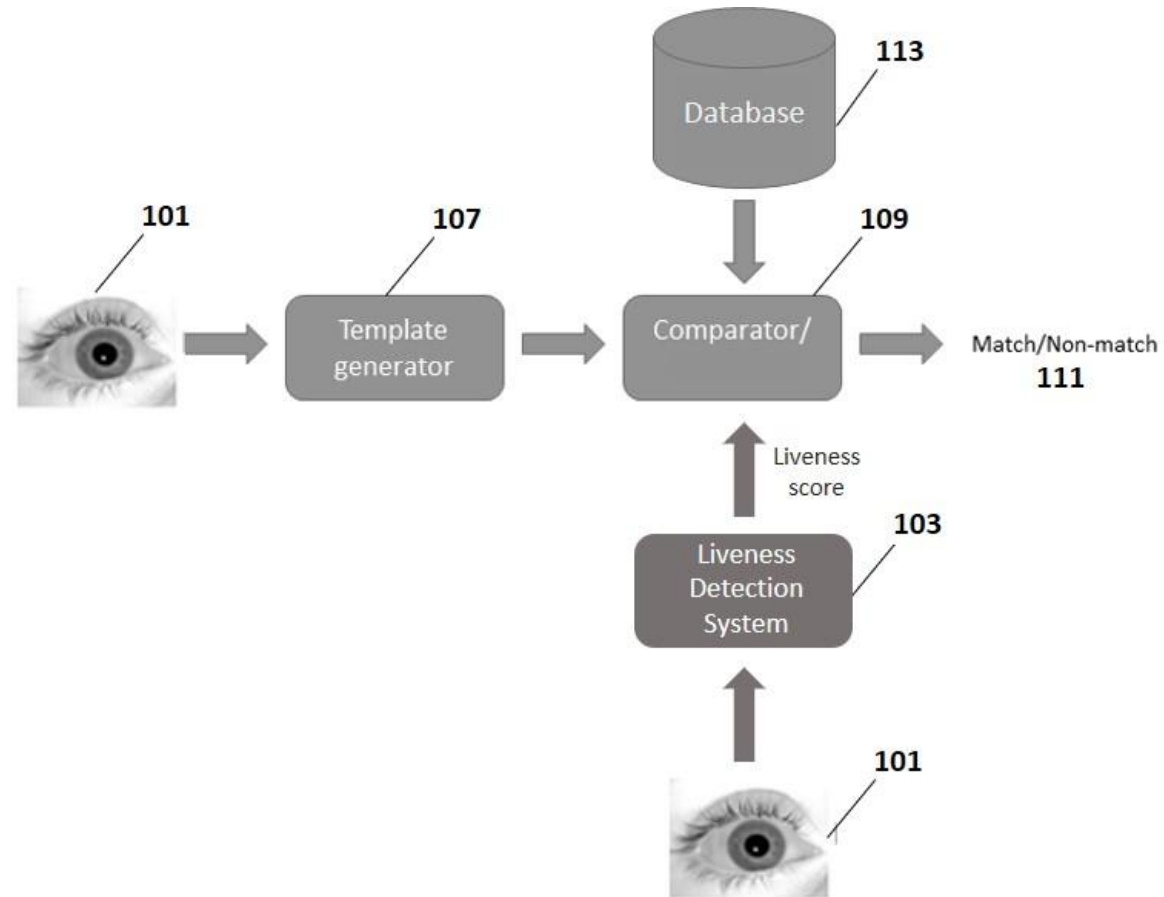


FIG. 1b

3/4

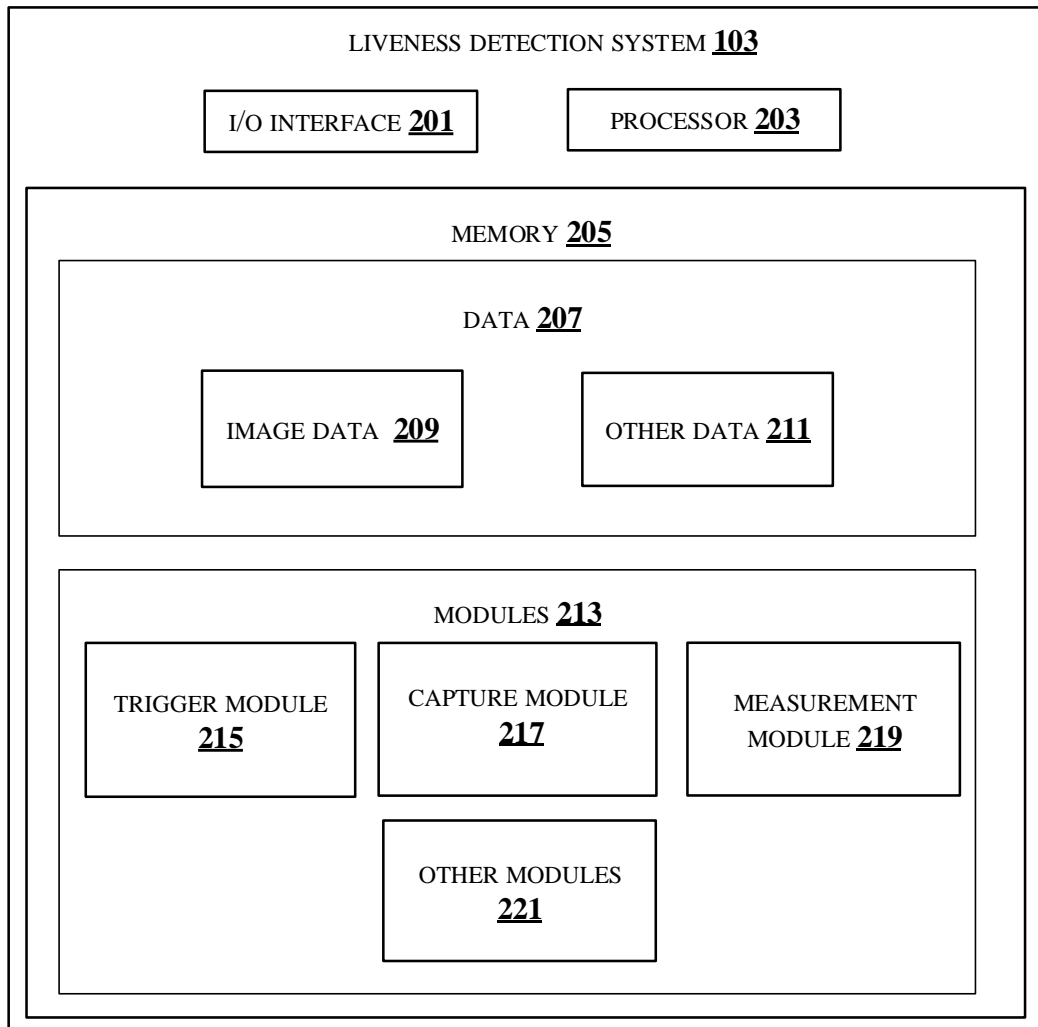


FIG. 2

4/4

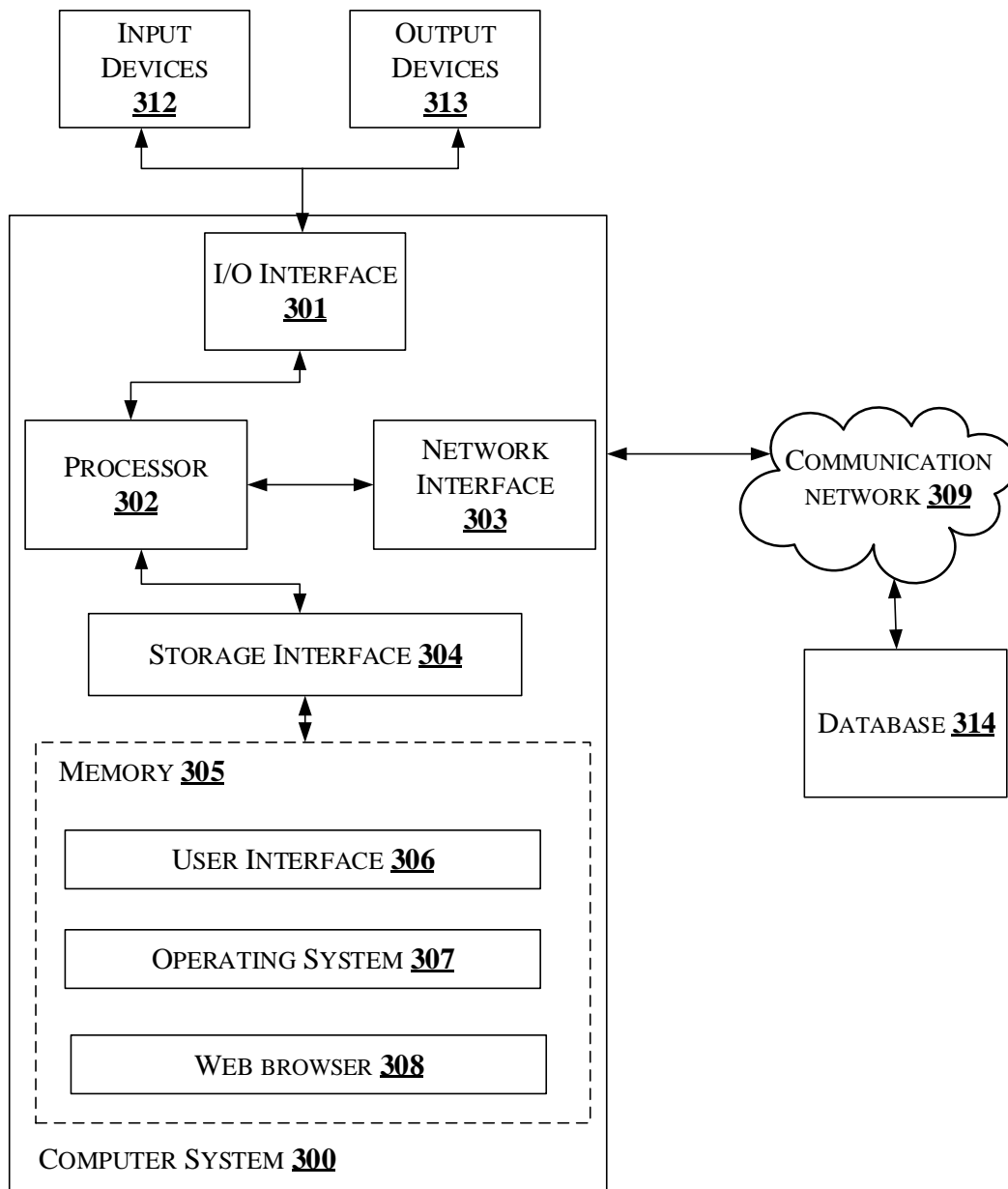


FIG. 3