

AUTHENTICATION METHOD AND SYSTEM

TECHNICAL FIELD

[001] The present specification relates broadly, but not exclusively, to an identification document authentication method and to an identification document authentication system.

BACKGROUND

[002] electronic-Know Your Customer (eKYC) is a digital due diligence process performed by a business entity or service provider to verify the identity of its customers to prevent falsification of identity. eKYC processes typically include a series of checks conducted at the initial stage of the relationship with the customers to verify their identities. Many eKYC processes involve potential customers submitting copies of their official identification (ID) documents, e.g. ID card, driving license, passport, etc. The submitted documents may then be analyzed to verify the customers' identities.

[003] In a typical eKYC process, a customer is required to take a photograph of his/her ID document. The customer typically uses a mobile phone with a camera to take the photograph of his/her ID document. However, some attackers may use fraudulent ID documents or high resolution copies of genuine ID documents during the eKYC processes to commit identity fraud. Identity fraud is the use of another person's personal information, without authorization, to commit a crime or to deceive the other person or a third party.

[004] One of the most common forms of identity fraud during the eKYC process involves attackers illegally accessing a hardware component in the mobile phone and injecting a fraudulent image. For example, an attacker can hijack the hardware component (e.g. image processor) of a camera module to inject the fraudulent image into the mobile phone system. Alternatively, attackers can hack into an eKYC mobile application that is running on a mobile device to inject a fraudulent image into the system instead of taking a photo of the ID document using a camera of the mobile device. In other words, attackers do not physically place an ID document in front of a camera lens in the conventional manner but introduce the fraudulent image into the system by illegally accessing a hardware component and/or software.

[005] Such attacks are more difficult to detect because the fraudulent ID document image is usually a real image of an ID document and not a screenshot or printed copy.

[006] A need therefore exists to improve the manner in which an ID document can be authenticated.

SUMMARY

[007] Embodiments seek to provide an identification (ID) document authentication method and system which involves monitoring changes that are present in a plurality of images that are captured before a user presents the ID document for authentication. In particular, changes such as position and size/area of the ID document in the captured images are analyzed to detect a fraud attack.

[008] According to one embodiment, there is provided an authentication method, including: obtaining a sequence of surveillance images, each of the surveillance images comprising an identification (ID) document image, wherein the sequence of surveillance images is captured by a user device before an image capturing function of the user device is triggered for taking images by the user device; determining a size and a center position of the ID document image in each of the surveillance images; and authenticating an ID document based on the determined size and the determined center position of the ID document image in each of the surveillance images. The ID document is positively authenticated on a condition that both the size and the center position of the ID document image vary in each of the surveillance images.

[009] According to another embodiment, there is provided an authentication system, including: a receiver device configured to obtain a sequence of surveillance images, each of the surveillance images comprising an identification (ID) document image, wherein the sequence of surveillance images is captured by a user device before an image capturing function of the user device is triggered for taking images by the user device; an image processor configured to determine a size and a center position of the ID document image in each of the surveillance images; and an authenticating device configured to authenticate an ID document based on the determined size and the determined center position of the ID document image in each of the surveillance images. The ID document is positively authenticated on a condition that both the size and the center position of the ID document image vary in each of the surveillance images.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Embodiments are provided by way of example only, and will be better understood and readily apparent to one of ordinary skill in the art from the following written description, read in conjunction with the drawings, in which:

[0011] Figure 1 is a flow chart illustrating an example of an identification (ID) document authentication method, according to an embodiment.

[0012] Figure 2 shows a sequence of captured images and corresponding processed images wherein a background is removed to extract an ID document image, according to an embodiment.

[0013] Figure 3A shows an extracted ID document image with four corners of the image detected, according to an embodiment.

[0014] Figure 3B illustrates a method for determining coordinates of each corner of an ID document image, according to an embodiment.

[0015] Figure 4 shows a schematic diagram of a computer system suitable for use in executing at least some steps of the authentication method described herein.

[0016] Figure 5 is a schematic diagram illustrating an example of an authentication system, according to an embodiment.

DETAILED DESCRIPTION

[0017] Embodiments will be described, by way of example only, with reference to the drawings. Like reference numerals and characters in the drawings refer to like elements or equivalents.

[0018] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An

algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0019] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “receiving”, “scanning”, “calculating”, “determining”, “replacing”, “generating”, “initializing”, “outputting”, or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0020] The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes, or may comprise a computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer suitable for executing the various methods / processes described herein will appear from the description below.

[0021] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings described herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the invention.

[0022] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored

on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM mobile telephone system. The computer program when loaded and executed on such a computer effectively results in an apparatus that implements the steps of the preferred method.

[0023] electronic-Know Your Customer (eKYC) is a digital due diligence process performed by a business entity or service provider to verify the identity of its customers to prevent falsification of identity. Authentication can be considered as a form of fraud detection in which legitimacy of users are verified and potential fraudsters may be detected before fraudulent acts are carried out. Effective authentication can enhance data security of systems so that digital data is protected from unauthorized users.

[0024] In a typical eKYC process, a customer is required to take a photograph of his/her identification (ID) document, e.g. ID card, driving license, passport, etc. One of the most common forms of identity fraud during the eKYC process involves attackers illegally accessing a hardware component in the mobile phone and injecting a fraudulent image. For example, an attacker can hijack the hardware component (e.g. image processor) of a camera module to inject the fraudulent image into the mobile phone system. Alternatively, attackers can hack into an eKYC mobile application that is running on a mobile device to inject a fraudulent image into the system instead of taking a photo of the ID document using a camera of the mobile device. In other words, attackers introduce the fraudulent image into the system by illegally accessing a hardware component and/or software.

[0025] Embodiments seek to provide an identification (ID) document authentication method and system which involve monitoring changes that are present in a plurality of images that are captured before a user presents the ID document for authentication. In particular, changes such as position and size/area of the ID document in the captured images are analyzed to detect a fraud attack. Variations of position and size/area of the ID document provide strong features for recognizing a fraud attack. In addition or alternatively, other changes can be monitored. For example, changes in shape and /or color of the ID document in the captured images can be monitored and analyzed to detect a fraud attack.

[0026] Conventionally, a camera module of a mobile device only captures images after a user presses the capture button on a user interface of a camera/video application (i.e. triggers an image capturing function of the camera). In contrast, in embodiments described herein, a plurality of “surveillance” images are captured before a user presents the ID document for authentication. In other words, the “surveillance” images are captured before the user presses the capture button. Hardware and/or software of the mobile phone can be configured to capture the “surveillance” images. For example, once the user launches an eKYC application on his mobile device, capturing of the “surveillance” images automatically begins. As another example, once the user launches a camera/video application on the mobile device, capturing of the “surveillance” images begins even though the user has not pressed the image/video capture button. Capturing of the “surveillance” images may cease when the user presses the image/video capture button.

[0027] Variations in the position and size/area of the ID document in the “surveillance” images provide an indication of a legitimate authorization attempt (i.e. not a fraud attack). On the other hand, if there are no changes in the position and size/area of the ID document in the “surveillance” images or if a presence of an ID document is not detected in the “surveillance” images, it may be an indication that an “injection” fraud attack has occurred.

[0028] The techniques described in the present specification produce one or more technical effects. In particular, by implementing an identification (ID) document authentication method and system which involves monitoring changes in a plurality of “surveillance” images (e.g. position and size/area of the ID document in the “surveillance” images) that are captured before a user presents the ID document for authentication, it is possible to detect “injection” attacks, and provide a versatile and robust fraud detection mechanism that does not require a specific security feature to be present on an ID document (e.g. hologram).

[0029] In this context, “injection” attacks refers to attackers illegally accessing a hardware component in the mobile phone and injecting a fraudulent image. For example, an attacker can hijack the hardware component (e.g. image processor) of a camera module to inject the fraudulent image into the mobile phone system. Alternatively, attackers can hack into an eKYC mobile application that is running on a mobile device to inject a fraudulent image into the system instead of taking a photo of the ID document

using a camera of the mobile device. In other words, attackers introduce the fraudulent image into the system by illegally accessing a hardware component and/or software.

[0030] Figure 1 is a flow chart 100 illustrating an example of an identification (ID) document authentication method, according to an embodiment. At step 102, a sequence of surveillance images is obtained. For example, an authentication device that is in communication with a user device obtains the sequence of surveillance images. Each of the surveillance images in the sequence of surveillance images includes an image of an ID document (hereinafter “ID document image”). In an implementation, the sequence of surveillance images comprises two or more surveillance images.

[0031] The sequence of surveillance images is captured by a user device before an image capturing function of the user device is triggered for taking images by the user device. For example, a first surveillance image in the sequence of surveillance images can be captured after an authentication mobile application is launched on the user device. The authentication mobile application may be an eKYC application. As another example, once a user launches a camera/video application on the mobile device, capturing of the sequence of surveillance images begins even though the user has not pressed the image/video capture button.

[0032] A final surveillance image in the sequence of surveillance images is captured before the image capturing function of the user device is triggered. In other words, capturing of the sequence of surveillance images may cease when the user presses the image/video capture button on a user interface of the camera/video application.

[0033] Each image in the sequence of surveillance images may be captured within a predetermined time window (e.g. 7 seconds). The time interval of capturing each surveillance image may be 1 per second, i.e. 7 images in a 7 seconds time window. After expiry of the predetermined time window, a new sequence of surveillance images may be captured and the previous sequence of surveillance images may be overwritten in a memory module of the camera module or mobile device. The latest sequence of surveillance images in the memory module is used for fraud detection.

[0034] At step 104, a size and a center position of the ID document image in each of the surveillance images is determined. The authentication device can be configured to determine the size and the center position of the ID document images. In an implementation, before determining the size and the center position of the ID document image in each of the surveillance images, a background in each of the surveillance

images is removed such that the ID document image can be extracted from each of the surveillance images.

[0035] With reference to Figure 2, a sequence of surveillance images 202 is captured from time t_1 to t_5 . In each image, the background is removed such that the ID document image is extracted as shown in images 204. If there is an image of an ID document in the image (e.g. the images taken at t_2 , t_3 , t_4 and t_5), the center position and area/size of the ID document image is calculated - I_1_c , I_1_s , ... I_5_c , I_5_s , where I_1 denotes image 1 captured at time t_1 , etc., “c” denotes center position and “s” denotes area/size. If there is no image of an ID document in the image (e.g. the image taken at t_1), the image may be discarded. If there is no image of an ID document in all of the images, it may be an indication that an “injection” fraud attack has occurred.

[0036] In an implementation, after removing the background in each of the surveillance images to extract the ID document image from each of the surveillance images, coordinates of each corner of the ID document image can be determined. In this manner, the size and the center position of the ID document image in each of the surveillance images can be determined based on the respective determined coordinates of each corner of the ID document image.

[0037] For example, as shown in Figure 3A, the four corners of an image is detected as p_1 , p_2 , p_3 and p_4 . The center position can be calculated as $I_c = [(p_1_x + p_2_x)/2, (p_2_y + p_3_y)/2]$. The area can be calculated as $I_s = (p_2_x - p_1_x) * (p_3_y - p_2_y)$.

[0038] In an implementation, deep learning object detection and object classification techniques can be used to extract the ID document image from each of the surveillance images and/or determining coordinates of each corner of an ID document image. For example, through deep learning, regions of interest of an ID document can be identified and the ID document can be cropped out.

[0039] Figure 3B illustrates a method for determining coordinates of each corner of an ID document image, according to an embodiment. In the example scenario 300, a captured image 300a, a processed image 300b and a refined image 300c are discussed.

[0040] The captured image 300a can include an ID card portion 302 and a background image portion 304. The ID card portion 302 can be based on an “x” by “y” resolution

(e.g., a 400 by 300 resolution; a 400 X 300 resolution where “x” = 300 and “y” = 400) and can be associated with one or more corner points.

[0041] Additionally, the ID card portion 302 associated with the captured image 300a can, for example, be visually perceived to be skewed (e.g., in an example situation where the ID card was poorly positioned and image is taken/captured when the ID card was positioned at an extreme angle).

[0042] The captured image 300a can be processed (e.g., using a trained CNN) so as to predict information concerning the corner point(s) of the ID card portion 302, as denoted by p1, p2, p3 and p4.

[0043] The processed image 300b can be associated with a processed ID card portion 306. Additionally, the aforementioned background image portion 304 can be substantially reduced/eliminated as compared to that per captured image 300a. Furthermore, the processed ID card portion 306 can be considered to be visually perceivable to be less skewed as compared to the ID card portion 302.

[0044] The processed ID card portion 306 can be associated with one or more corner points. For example, the processed ID card portion 306 can be associated with four corner points as denoted by p1', p2', p3' and p4'. p1, p2, p3 and p4 can be processed by manner of perspective transformation-based processing to produce p1', p2', p3' and p4' respectively.

[0045] In the 400 by 300 resolution based context per the example scenario 300, p1' can be predefined as (0, 0), p2' can be predefined as (400, 0), p3' can be predefined as (400, 300) and p4' can be predefined as (0, 300).

[0046] In certain implementations, still further improvement may be required/desired in respect of the processed image 300b. For example, the processed image 300b can be considered to be still of inadequate/unacceptable/non-ideal quality. Hence, a refined image 300c, which can be considered to be of a higher quality (e.g., more accurate/ more intelligible) compared to the processed image 300b, can be generated.

[0047] The refined image 300c can be associated with or can correspond substantially to a refined ID card portion 308. One or more refinement/adjustment parameters can be

applied. An adjustment/refinement can be, for example, in relation to the width and/or height associated with the ID card portion 302.

[0048] Specifically, the ID card portion 302 can be associated with a width (as denoted by “w”) and a height (as denoted by “h”). For example, in regard to the corner points “p1,” “p2,” “p3” and “p4” associated with the ID card portion 302, a predetermined adjustment/refinement factor of a multiplication of 0.1 and w (i.e. $0.1 * w$) can be applied in respect of “x” and a predetermined adjustment/refinement factor of a multiplication of 0.1 and h (i.e. $0.1 * h$) can be applied to “y” as follows:

- $p1(x, y) = p1(x - 0.1 * w, y - 0.1 * h)$
- $p2(x, y) = p2(x + 0.1 * w, y - 0.1 * h)$
- $p3(x, y) = p3(x + 0.1 * w, y + 0.1 * h)$
- $p4(x, y) = p4(x - 0.1 * w, y + 0.1 * h)$

[0049] In the 400 by 300 resolution based context per the example scenario 300, $p1(x, y)$ can be predefined as (0, 0) (e.g., $x=0$; $y=0$), $p2(x, y)$ can be predefined as (400, 0) (e.g., $x=400$; $y=0$), $p3(x, y)$ can be predefined as (400, 300) (e.g., $x=400$; $y=300$) and $p4(x, y)$ can be predefined as (400, 0) (e.g., $x=400$; $y=0$).

[0050] $p1(x, y)$, $p2(x, y)$, $p3(x, y)$ and/or $p4(x, y)$ can be processed (e.g., using a trained CNN) to generate refined predictive corner point(s) $p1''$, $p2''$, $p3''$ and/or $p4''$ respectively. $p1''$, $p2''$, $p3''$ and/or $p4''$ can be processed by manner of perspective transformation-based processing to produce $pp1$, $pp2$, $pp3$ and/or $pp4$ respectively.

[0051] The refined ID card portion 308 can be associated with/can include one or more corner point(s) which can be denoted by $pp1$, $pp2$, $pp3$ and/or $pp4$. In the 400 by 300 resolution based context per the example scenario 300, $pp1$ can be predefined as (0, 0), $pp2$ can be predefined as (400, 0), $pp3$ can be predefined as (400, 300) and $pp4$ can be predefined as (400, 0).

[0052] The refined image 300c should ideally be without a background image portion 304. In this regard, the refined image 300c can, for example, substantially correspond to the refined ID card portion 308 (i.e., without a background image portion 304/ the background image portion 304, if any, is considered to be negligible). Hence, in the refined image 300c, the aforementioned background image portion 304 (per the captured image 300a and/or the processed image 300b) can be considered to have been at least

substantially eliminated (or negligible). Furthermore, the refined ID card portion 308 can, for example, be considered to be visually perceivable to be less skewed as compared to the processed ID card portion 306. Specifically, extent of skew associated with the refined ID card portion 308 can be lesser as compared to the processed ID card portion 306.

[0053] Referring back to Figure 1, at step 106, an ID document is authenticated based on the determined size and the determined center position of the ID document image in each of the surveillance images. The authentication device can be configured to authenticate the ID document. The ID document is positively authenticated on a condition that both the size and the center position of the ID document image varies in each of the surveillance images.

[0054] It is expected that for a legitimate authorization attempt (i.e. not a fraud attack), the size and the center position of the ID document image varies because the user has to move the mobile device such that the ID document is centered in the image capturing frame of the camera application that is running on the mobile device. Once the ID document is centered in the image capturing frame, the user triggers the image capturing function for authentication. In other words, a non-varying size and center position of the ID document image in each of the images implies that a user has immediately managed to center the ID document in the image capturing frame and kept the position for a period of time (e.g. the predetermined time window described above), which is unlikely and may suggest an “injection” attack.

[0055] In an implementation, for increased robustness of the authentication process, the ID document can be positively authenticated on a further condition that the size of the ID document image either monotonically increases throughout the sequence of surveillance images or monotonically decreases throughout the sequence of surveillance images. It is expected that for a legitimate authorization attempt (i.e. not a fraud attack), the size of the ID document image either monotonically increases throughout the sequence of surveillance images or monotonically decreases throughout the sequence of surveillance images because the user either continuously zooms in or out such that the ID document is centered in the image capturing frame of the camera application that is running on the mobile device. It is unlikely that a user zooms in, then zooms out and zooms in again, etc.

[0056] In an implementation, for even greater robustness of the authentication process, the ID document can be positively authenticated on a further condition that the center position of the ID document image varies in a single direction throughout the sequence of surveillance images.

[0057] In an implementation, a decision function can be designed to check the authenticity of the ID document. The function can be formulated as $F(I1_c, I1_s, \dots I4_c, I4_s)$. For example, if a user gradually zooms in on an ID document (e.g. as shown in Figure 2, reference numeral 202), F is true when I_s continuously becomes bigger throughout the sequence of surveillance images, i.e. $I1_s < I2_s < I3_s < I4_s$, meanwhile, the direction of $I1_c, I2_c, I3_c$, and $I4_c$ is the same. On the other hand, if a user initially puts the ID document very close to the camera lens and gradually zooms out, the area becomes smaller and smaller throughout the sequence of surveillance images, i.e. I_s becomes smaller, e.g. $I1_s > I2_s > I3_s > I4_s$.

[0058] In this context, the “direction” of $I1_c, I2_c, I3_c$, and $I4_c$ refers to a location of an ID document throughout the sequence of surveillance images. For example, in Figure 2, the ID document is initially on the bottom-left side of the image and gradually moves to upwards and right until it is approximately in the center. The four arrows (denoted by reference numeral 206) shown in Figure 2 indicate the direction of movement of the ID document throughout the sequence of surveillance images. The direction of movement is substantially the same throughout the sequence of surveillance images. In other words, the center position of the ID document image varies in a single direction throughout the sequence of surveillance images. It is expected that for a legitimate authorization attempt (i.e. not a fraud attack), the direction does not change, i.e. the card moves leftwards then abruptly moves rightwards, etc. In other words, the user moves the mobile device in a single general direction such that the ID document is centered in the image capturing frame of the camera application that is running on the mobile device.

[0059] If the monitor image are collected from left to right (e.g. as shown in Figure 2), then the condition to be satisfied is $I1_c_x < I2_c_x < I3_c_x < I4_c_x$, the $I1_c_x$, which denotes the value of the x-axis. If F is true, it is an indication that the ID card is a real one; otherwise, the ID is from an “injecting” attack.

[0060] In an implementation, the direction is calculated (i.e. it is determined that the images are “moving” from left-right and/or up-down) based on a center position of the monitor image.

[0061] If the monitor image are “moving” from down to up, then the condition to be satisfied is $I1_c_y < I2_c_y < I3_c_y < I4_c_y$, the $I1_c_y$ denotes the value of the y-axis.

[0062] In an implementation, a deep learning method can be utilized to calculate the area and direction of the ID document images, instead of using image processing methods. A CNN Long Short-Term Memory Network can be adopted to predict a direction of the ID document, wherein the input is a video sequence, and the output is a predicted direction of the ID document.

[0063] Figure 4 shows a schematic diagram of a computer system suitable for use in executing at least some steps of the ID document authentication method.

[0064] The following description of the computer system / computing device 400 is provided by way of example only and is not intended to be limiting.

[0065] As shown in Figure 4, the example computing device 400 includes a processor 404 for executing software routines. Although a single processor is shown for the sake of clarity, the computing device 400 may also include a multi-processor system. The processor 404 is connected to a communication infrastructure 406 for communication with other components of the computing device 400. The communication infrastructure 406 may include, for example, a communications bus, cross-bar, or network.

[0066] The computing device 400 further includes a main memory 408, such as a random access memory (RAM), and a secondary memory 410. The secondary memory 410 may include, for example, a hard disk drive 412 and/or a removable storage drive 414, which may include a magnetic tape drive, an optical disk drive, or the like. The removable storage drive 414 reads from and/or writes to a removable storage unit 418 in a well-known manner. The removable storage unit 418 may include a magnetic tape, optical disk, or the like, which is read by and written to by removable storage drive 414. As will be appreciated by persons skilled in the relevant art(s), the removable storage unit 418 includes a computer readable storage medium having stored therein computer executable program code instructions and/or data.

[0067] In an alternative embodiment, the secondary memory 410 may additionally or alternatively include other similar devices for allowing computer programs or other instructions to be loaded into the computing device 400. Such devices can include, for example, a removable storage unit 422 and an interface 420. Examples of a removable storage unit 422 and interface 420 include a removable memory chip (such as an EPROM or PROM) and associated socket, and other removable storage units 422 and interfaces 420 which allow software and data to be transferred from the removable storage unit 422 to the computer system 400.

[0068] The computing device 400 also includes at least one communication interface 424. The communication interface 424 allows software and data to be transferred between computing device 400 and external devices via a communication path 426. In various embodiments, the communication interface 424 permits data to be transferred between the computing device 400 and a data communication network, such as a public data or private data communication network. The communication interface 424 may be used to exchange data between different computing devices 400 which such computing devices 400 form part an interconnected computer network. Examples of a communication interface 424 can include a modem, a network interface (such as an Ethernet card), a communication port, an antenna with associated circuitry and the like. The communication interface 424 may be wired or may be wireless. Software and data transferred via the communication interface 424 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by communication interface 424. These signals are provided to the communication interface via the communication path 426.

[0069] Optionally, the computing device 400 further includes a display interface 402 which performs operations for rendering images to an associated display 430 and an audio interface 432 for performing operations for playing audio content via associated speaker(s) 434.

[0070] As used herein, the term "computer program product" may refer, in part, to removable storage unit 418, removable storage unit 422, a hard disk installed in hard disk drive 412, or a carrier wave carrying software over communication path 426 (wireless link or cable) to communication interface 424. Computer readable storage media refers to any non-transitory tangible storage medium that provides recorded instructions and/or data to the computing device 400 for execution and/or processing.

Examples of such storage media include floppy disks, magnetic tape, CD-ROM, DVD, Blu-ray™ Disc, a hard disk drive, a ROM or integrated circuit, USB memory, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computing device 400. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs, instructions and/or data to the computing device 400 include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

[0071] The computer programs (also called computer program code) are stored in main memory 408 and/or secondary memory 410. Computer programs can also be received via the communication interface 424. Such computer programs, when executed, enable the computing device 400 to perform one or more features of embodiments discussed herein. In various embodiments, the computer programs, when executed, enable the processor 404 to perform features of the above-described embodiments. Accordingly, such computer programs represent controllers of the computer system 400.

[0072] Software may be stored in a computer program product and loaded into the computing device 400 using the removable storage drive 414, the hard disk drive 412, or the interface 420. Alternatively, the computer program product may be downloaded to the computer system 400 over the communications path 426. The software, when executed by the processor 404, causes the computing device 400 to perform functions of embodiments described herein.

[0073] It is to be understood that the embodiment of Figure 4 is presented merely by way of example. Therefore, in some embodiments one or more features of the computing device 400 may be omitted. Also, in some embodiments, one or more features of the computing device 400 may be combined together. Additionally, in some embodiments, one or more features of the computing device 400 may be split into one or more component parts.

[0074] According to an embodiment, there is provided an authentication system including: at least one processor (e.g. processor 404); one or more memories (e.g. memory 408 and/or 410) coupled to the at least one processor and storing programming instructions for execution by the at least one processor, the programming instructions

instruct the at least one processor to: obtain a sequence of surveillance images, each of the surveillance images comprising an identification (ID) document image, wherein the sequence of surveillance images is captured by a user device before an image capturing function of the user device is triggered for taking images by the user device; determine a size and a center position of the ID document image in each of the surveillance images; and authenticate an ID document based on the determined size and the determined center position of the ID document image in each of the surveillance images, wherein the ID document is positively authenticated on a condition that both the size and the center position of the ID document image vary in each of the surveillance images.

[0075] Figure 5 is a schematic diagram illustrating an identification (ID) document authentication system 500, according to an embodiment. The system 500 includes a receiver device 502, an image processor 504 and an authenticating device 506.

[0076] The receiver device 502 can be in communication with a user device 508, e.g. via wireless communication protocols known in the art. One or more intermediary elements/components (not shown in Figure 5) may be present to facilitate the communication. For example, the elements/components may be a base station, server, etc. The receiver device 502 is configured to receive / retrieve / obtain a sequence of surveillance images from the user device 508. Each of the surveillance images includes an identification (ID) document image. The sequence of surveillance images is captured by the user device 508 before an image capturing function of the user device 508 is triggered for taking images by the user device. A first surveillance image in the sequence of surveillance images is captured after an authentication application is launched on the user device 508. A final surveillance image in the sequence of surveillance images is captured before the image capturing function of the user device 508 is triggered.

[0077] The image processor 504 is configured to determine a size and a center position of the ID document image in each of the surveillance images. Before determining the size and the center position of the ID document image in each of the surveillance images, the image processor 504 can be further configured to remove a background in each of the surveillance images to extract the ID document image from each of the surveillance images.

[0078] After removing the background in each of the surveillance images, the image processor 504 can be further configured to: (i) determine coordinates of each corner of the ID document image; and (ii) determine the size and the center position of the ID

document image in each of the surveillance images based on the respective determined coordinates of each corner of the ID document image.

[0079] The authenticating device 506 is configured to authenticate an ID document based on the determined size and the determined center position of the ID document image in each of the surveillance images. In particular, the ID document is positively authenticated on a condition that both the size and the center position of the ID document image vary in each of the surveillance images. In an implementation, the authenticating device 506 may be configured to positively authenticate the ID document on a further condition that the size of the ID document image either monotonically increases throughout the sequence of surveillance images or monotonically decreases throughout the sequence of surveillance images. Alternatively or in addition, the authenticating device 506 may be configured to positively authenticate the ID document on a further condition that the center position of the ID document image varies in a single direction throughout the sequence of surveillance images.

[0080] This specification uses the term “configured to” in connection with systems, devices, and computer program components. For a system of one or more computers to be configured to perform particular operations or actions means that the system has installed on it software, firmware, hardware, or a combination of them that in operation cause the system to perform the operations or actions. For one or more computer programs to be configured to perform particular operations or actions means that the one or more programs include instructions that, when executed by data processing apparatus, cause the apparatus to perform the operations or actions. For special-purpose logic circuitry to be configured to perform particular operations or actions means that the circuitry has electronic logic that performs the operations or actions.

[0081] It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

CLAIMS

1. An authentication method, comprising:
 - obtaining a sequence of surveillance images, each of the surveillance images comprising an identification (ID) document image, wherein the sequence of surveillance images is captured by a user device before an image capturing function of the user device is triggered for taking images by the user device;
 - determining a size and a center position of the ID document image in each of the surveillance images; and
 - authenticating an ID document based on the determined size and the determined center position of the ID document image in each of the surveillance images, wherein the ID document is positively authenticated on a condition that both the size and the center position of the ID document image vary in each of the surveillance images.
2. The method as claimed in claim 1, wherein the ID document is positively authenticated on a further condition that the size of the ID document image either monotonically increases throughout the sequence of surveillance images or monotonically decreases throughout the sequence of surveillance images.
3. The method as claimed in claim 1 or 2, wherein the ID document is positively authenticated on a further condition that the center position of the ID document image varies in a single direction throughout the sequence of surveillance images.
4. The method as claimed in any one of the preceding claims, wherein a first surveillance image in the sequence of surveillance images is captured after an authentication application is launched on the user device.
5. The method as claimed in claim 4, wherein a final surveillance image in the sequence of surveillance images is captured before the image capturing function of the user device is triggered for taking images by the user device.
6. The method as claimed in any one of the preceding claims, wherein before determining the size and the center position of the ID document image in each of the surveillance images, the method further comprises:
 - removing a background in each of the surveillance images to extract the ID document image from each of the surveillance images.

7. The method as claimed in claim 6, wherein after removing the background in each of the surveillance images to extract the ID document image from each of the surveillance images, the method further comprises:

determining coordinates of each corner of the ID document image; and

determining the size and the center position of the ID document image in each of the surveillance images based on the respective determined coordinates of each corner of the ID document image.

8. An authentication system, comprising:

a receiver device configured to obtain a sequence of surveillance images, each of the surveillance images comprising an identification (ID) document image, wherein the sequence of surveillance images is captured by a user device before an image capturing function of the user device is triggered for taking images by the user device;

an image processor configured to determine a size and a center position of the ID document image in each of the surveillance images; and

an authenticating device configured to authenticate an ID document based on the determined size and the determined center position of the ID document image in each of the surveillance images, wherein the ID document is positively authenticated on a condition that both the size and the center position of the ID document image vary in each of the surveillance images.

9. The system as claimed in claim 8, wherein the authenticating device is configured to positively authenticate the ID document on a further condition that the size of the ID document image either monotonically increases throughout the sequence of surveillance images or monotonically decreases throughout the sequence of surveillance images.

10. The system as claimed in claim 8 or 9, wherein the authenticating device is configured to positively authenticate the ID document on a further condition that the center position of the ID document image varies in a single direction throughout the sequence of surveillance images.

11. The system as claimed in any one of claims 8 to 10, wherein a first surveillance image in the sequence of surveillance images is captured after an authentication application is launched on the user device.

12. The system as claimed in claim 11, wherein a final surveillance image in the sequence of surveillance images is captured before the image capturing function of the user device is triggered for taking images by the user device.

13. The system as claimed in any one of claims 8 to 12, wherein the image processor is further configured to:

remove a background in each of the surveillance images to extract the ID document image from each of the surveillance images,
before determining the size and the center position of the ID document image in each of the surveillance images.

14. The system as claimed in claim 13, wherein the image processor is further configured to:

determine coordinates of each corner of the ID document image; and
determine the size and the center position of the ID document image in each of the surveillance images based on the respective determined coordinates of each corner of the ID document image,
after removing the background in each of the surveillance images.

15. An authentication system comprising:

at least one processor;

one or more memories coupled to the at least one processor and storing programming instructions for execution by the at least one processor, the programming instructions instruct the at least one processor to:

obtain a sequence of surveillance images, each of the surveillance images comprising an identification (ID) document image, wherein the sequence of surveillance images is captured by a user device before an image capturing function of the user device is triggered for taking images by the user device;

determine a size and a center position of the ID document image in each of the surveillance images; and

authenticate an ID document based on the determined size and the determined center position of the ID document image in each of the surveillance images, wherein the ID document is positively authenticated on a condition that both the size and the center position of the ID document image vary in each of the surveillance images.