

AN AUTHENTICATION METHOD AND SYSTEM

TECHNICAL FIELD

5 **[001]** The present specification relates broadly, but not exclusively, to an authentication method and to an authentication system.

BACKGROUND

10

[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
15 identities. Many eKYC processes involve potential customers submitting photographs of their official identification (ID) documents, e.g. ID card, driving license, passport, etc. The photographs may then be analyzed to verify the customers' identities.

[003] In a typical eKYC process, a customer is required to take a photograph of
20 his/her ID document. However, some attackers may use fraudulent ID documents, screenshots of genuine ID documents or high resolution copies of genuine ID documents, during the eKYC processes.

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

SUMMARY

30 **[005]** Embodiments seek to provide an authentication method and an authentication system which involve obtaining at least two images of an ID document captured from different angles and verifying the multi-angle security feature(s) on the ID document. The ID document can be authenticated based on the identification of one or more multi-angle security feature(s) on the ID document images.

35

[006] According to one embodiment, there is provided an authentication method, comprising: obtaining a reference image, wherein the reference image is an image of

an identification (ID) document; obtaining a first image for comparison with the reference image, wherein the first image is an image of the ID document tilted at a first angle; generating a first difference image, wherein the first difference image is based on a comparison between the reference image and the first image; identifying a region of interest based on the first difference image, wherein the region of interest corresponds to a multi-angle security feature on the ID document; and authenticating the ID document based on the identification of the region of interest.

[007] According to another embodiment, there is provided an authentication system, comprising: a reference image obtaining device to obtain a reference image, wherein the reference image is an image of an identification (ID) document; a first image obtaining device to obtain a first image for comparison with the reference image, wherein the first image is an image of the ID document tilted at a first angle; a first difference image generating device to generate a first difference image, wherein the first difference image is based on a comparison between the reference image and the first image; a region of interest identification device to identify a region of interest based on the first difference image, wherein the region of interest corresponds to a multi-angle security feature on the ID document; and an authentication device to authenticate the ID document based on the identification of the region of interest.

[008] According to yet another embodiment, there is provided a computing system comprising: at least one processor; a non-transitory computer-readable storage medium 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 reference image, wherein the reference image is an image of an identification (ID) document; obtain a first image for comparison with the reference image, wherein the first image is an image of the ID document tilted at a first angle; generate a first difference image, wherein the first difference image is based on a comparison between the reference image and the first image; identify a region of interest based on the first difference image, wherein the region of interest corresponds to a multi-angle security feature on the ID document; and authenticate the ID document based on the identification of the region of interest.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] 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:

[0010] Figure 1 is a flow chart illustrating an example of an authentication method, according to an embodiment.

[0011] Figure 2, comprising Figure 2A and Figure 2B, is a schematic representation illustrating an example of an authentication method, according to another embodiment.

[0012] Figure 3 is a schematic diagram illustrating an example of an authentication system, according to an embodiment.

[0013] Figure 4 shows a schematic diagram of a computer system suitable for use in executing at least some steps of the authentication method.

[0014] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been depicted to scale. For example, the dimensions of some of the elements in the illustrations, block diagrams or flowcharts may be exaggerated in respect to other elements to help to improve understanding of the present embodiments.

DETAILED DESCRIPTION

[0015] 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.

[0016] 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.

[0017] 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.

[0018] 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.

[0019] 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 of the specification contained 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.

[0020] 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.

[0021] 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.

[0022] 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. However, some attackers may use replicates of ID documents during the eKYC processes. The replicates of ID documents may include high resolution copies of genuine ID documents, screenshots of genuine ID documents or fraudulent ID documents.

[0023] In an authentic ID document, security features are usually incorporated to reduce risk of counterfeiting or other forms of fraud. Multi-angle security features, such as hologram, multiple laser images, kineprint and optical variable ink, are widely used in ID documents as important security features. When viewed from different angles, the multi-angle security features may display different colours and/or images. Some types of ID documents may only have one kind of multi-angle security feature, while some types of ID documents may have more than one kind of multi-angle security features. Replicates of ID documents typically are unable to replicate the multi-angle security features on an authentic ID document. Therefore, verifying the multi-angle security features on ID documents may be useful in detecting attacks which use replicates of ID documents.

[0024] Current ID document anti-fraud methods/systems may require a user to take a photograph of his/her ID document. Multi-angle security feature(s) on the ID document may not be observed on the captured image due to an unchanged angle and/or unchanged light source. As such, accuracy in authenticating ID documents may be low

by verifying multi-angle security features on ID documents based on only one captured image.

5 **[0025]** Embodiments described in the present specification may involve an eKYC process that includes two general processes: a user enrollment process and a user verification process. In the user enrollment process, a user may be required to take photographs of his/her ID document from different angles for submission as user enrollment images. A captured image may comprise an ID document image and a background image. According to one embodiment, the user may be required to take at
10 least two photographs of his/her ID document from different angles for submission as user enrollment images.

15 **[0026]** As mentioned above, replicates of ID documents typically do not replicate the multi-angle security feature(s) of an authentic ID document. Current ID document anti-fraud methods may not be able to fully utilize the multi-angle security features on ID documents to detect attacks which use replicates of ID documents.

20 **[0027]** In order to reduce the success rate of attacks that use replicates of ID documents, an authentication method and/or system which involve obtaining at least two images of an ID document captured from different angles and verifying the multi-angle security feature(s) on the ID document may be implemented. The ID document can be authenticated based on the identification of one or more multi-angle security feature(s) on the ID document images.

25 **[0028]** The techniques described in the present specification produce one or more technical effects. The authentication method and system can reduce the success rate of attacks to the eKYC process by obtaining at least two ID document images and verifying the multi-angle security feature(s) on the ID document based on the at least two ID document images. If no multi-angle security feature is identified on the ID
30 document images, the ID document can be determined to be a replicate of an ID document.

35 **[0029]** Further, the authentication method and system may provide higher accuracy in authenticating an ID document. In particular, by obtaining at least two ID document images (e.g. a reference image of the ID document and an image of the ID document tilted at an angle) and comparing the images, multi-angle security feature(s) on the ID

document can be accurately observed and/or identified. As such, an authentic ID document can be determined accurately.

5 **[0030]** As mentioned above, in the user enrollment process of an eKYC process, a user may be required to take photographs of his/her ID document from different angles for submission as user enrollment images. A captured image may comprise an ID document image and a background image. Image processing method(s) and/or system(s) may be implemented on the captured images to remove the background images and to align ID document images. Alignment of an ID document image may be
10 based on one or more corner points of the ID document image. For example, four corner points of an aligned ID document image may correspond to four corner points of a rectangle or a square.

15 **[0031]** For example, the ID document image 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. Input signal(s) associated with the captured image can be communicated to database(s) for processing the captured image by manner of predicative processing. The predicative processing may be based on a Convolutional Neural Network. Information concerning the corner point(s) of the
20 ID document image may be predicted. Detection signal(s) corresponding to predicted information concerning the corner points can be received by apparatus(es) for processing (e.g., perspective transformation-based processing) to generate output signal(s) which can correspond to a processed captured image.

25 **[0032]** The processed captured image can be associated with a processed ID document image. Additionally, the aforementioned background image can be substantially reduced/eliminated as compared to the captured image. The processed ID document image can be associated with one or more corner points. Information concerning the corner point(s) of the processed ID document image can be
30 derived/obtained/determined based on, for example, perspective transformation-based processing in respect of the corner point(s) of the ID document image. Accordingly, an aligned ID document image may be obtained.

35 **[0033]** Figure 1 is a flow chart 100 illustrating an example of an authentication method, according to an embodiment. At step 102, a reference image is obtained. The reference image is an image of an identification (ID) document. At step 104, a first image for comparison with the reference image is obtained. The first image is an

image of the ID document tilted at a first angle. At step 106, a first difference image is generated. The first difference image is based on a comparison between the reference image and the first image. At step 108, one or more regions of interest based on the first difference image is/are identified. The region(s) of interest corresponds to one or more multi-angle security features on the ID document. At step 110, the ID document is authenticated based on the identification of the region(s) of interest.

[0034] In order to obtain a reference image, a user may be required to take a photograph of his/her ID document when the ID document is tilted between -10 degrees and 10 degrees about a tilt axis. The tilt axis may correspond to a width of the ID document or a height of the ID document. For example, the user may place his/her ID document on a flat surface such as a tabletop, and take a photograph of the plan view of the ID document. The captured image may comprise an ID document image and a background image. Image processing method(s) and/or system(s) may be implemented on the captured image to remove the background image and to align the ID document image. The aligned ID document image may be resized to obtain the reference image. For example, the aligned ID document image may be resized to 300x200, where 300 denotes the width and 200 denotes the height of the reference image.

[0035] In order to obtain the first image for comparison with the reference image, the user may be required to take another photograph of his/her ID document when the ID document is tilted at a first angle about the aforementioned tilt axis. The captured image may comprise an ID document image and a background image. Image processing method(s) and/or system(s) may be implemented on the captured image to remove the background image and to align the ID document image. The aligned ID document image may be resized to obtain the first image for comparison with the reference image. For example, the aligned ID document image may also be resized to 300x200, where 300 denotes the width and 200 denotes the height of the first image.

[0036] As mentioned above and with reference to Figure 1, at step 108, a region(s) of interest based on the first difference image is identified. The region(s) of interest corresponds to a multi-angle security feature(s) on the ID document. In some scenarios, there may be one region of interest identified based on the first difference image. In some other scenarios, there may be more than one regions of interest identified based on the first difference image. There may also be scenarios whereby no region of interest is identified based on the first difference image. For the scenarios

whereby one or more region(s) of interest based on the first difference image is identified, each region of interest may correspond to one or more multi-angle security feature(s). For example, a region of interest identified may comprise two holograms.

5 **[0037]** According to one embodiment, the authentication method may further comprise obtaining a second image for comparison with the reference image. The second image may be an image of the ID document tilted at a second angle. The authentication method may also comprise generating a second difference image. The second difference image may be based on a comparison between the reference image and the
10 second image. Further, the authentication method may comprise identifying one or more additional regions of interest based on the second difference image. The additional region(s) of interest may correspond to one or more additional multi-angle security features on the ID document. The authentication method may further comprise authenticating the ID document based on the identification of the region(s) of interest
15 and the additional region(s) of interest. In this manner, the robustness of the authentication method may be increased.

[0038] As mentioned, the additional region(s) of interest may correspond to an additional multi-angle security feature(s) on the ID document. In some scenarios, there
20 may be one additional region of interest identified based on the second difference image. In some other scenarios, there may be more than one additional regions of interest identified based on the second difference image. There may also be scenarios whereby no additional region of interest is identified based on the second difference image. For the scenarios whereby one or more additional region(s) of interest based on
25 the second difference image is identified, each additional region of interest may correspond to one or more additional multi-angle security feature(s). For example, an additional region of interest identified may comprise two additional holograms.

[0039] The reference image may be an image of the ID document tilted between -10
30 degrees and 10 degrees about a tilt axis. The tilt axis may correspond to a width of the ID document or a height of the ID document.

[0040] According to one embodiment, the first angle which the ID document is tilted at may be between 15 degrees and 45 degrees in a first direction about the tilt axis.

35 **[0041]** The second angle which the ID document is tilted at may be between 15 degrees and 45 degrees in a second direction about the tilt axis. The second direction may be opposite from the first direction.

[0042] In some implementations, the authentication method may further comprise performing image pre-processing on the first image and/or second image. The sharpness of the first image and/or second image may be improved and accuracy of identifying region(s) of interest and/or additional region(s) of interest may be increased. The image pre-processing may be performed using a filter2D function in opencv.

[0043] According to one embodiment, sizes of the reference image and the first image may be same. The comparison between the reference image and the first image to generate the first difference image can be based on a pixel-by-pixel comparison between the reference image and the first image. In some implementations, sizes of the reference image and the second image may be same. The comparison between the reference image and the second image to generate the second difference image can be based on a pixel-by-pixel comparison between the reference image and the second image.

[0044] The authentication method may further comprise performing image processing, using an image erosion method or an image dilation method, on the first difference image. By using the image erosion method, pixels on object boundaries in an image may be removed. In other words, pixels on boundaries of the region(s) of interest identified based on the first difference image may be removed. By using the image dilation method, pixels may be added to boundaries of objects in an image. In other words, pixels may be added to boundaries of the region(s) of interest identified based on the first difference image. The image processing using the image erosion method or the image dilation method may also be performed on the second difference image.

[0045] In some implementations, the multi-angle security feature(s) corresponding to the region(s) of interest identified based on the first difference image may be marked up. The multi-angle security feature(s) may be of a lighter shade as compared to the other portions of the first difference image. A center point of each of the multi-angle security feature may be identified and a distance from the center point to the boundary of the multi-angle security feature may be determined. A shape, for example a circle, may be plotted based on the center point and the distance from the center point to the boundary of the multi-angle security feature. Each shape plotted may indicate a multi-angle security feature. For example, two circles plotted may indicate two multi-angle security features (e.g. two holograms). For better visualization, the shape may be plotted in a colour that contrasts with the colour(s) present in the first difference image.

For example, the shape may be plotted in red. The additional multi-angle security feature(s) corresponding to the additional region(s) of interest identified based on the second difference image may be marked up in a similar manner.

5 **[0046]** The authentication method may further comprise generating a binary image based on the region of interest identified. A first area of the binary image corresponding to the region of interest may be associated with a first pixel value, and a second area of the binary image outside a boundary of the first area may be associated with a second pixel value. The first pixel value may be different from the second pixel value. Another
10 binary image based on the additional region(s) of interest identified may be generated in a similar manner.

[0047] The size of the binary image(s) generated may be the same as that of the reference image, the first image and/or the second image. If no region of interest is
15 identified, the binary image(s) may be associated with only the second pixel value. The first pixel value may be 128 and the second pixel value may be 0. As mentioned above, shape(s) indicating multi-angle security feature(s) may be plotted. In some implementations, the area(s) enclosed by the shape(s) may be associated with the first pixel value while the remaining area of the binary image may be associated with the
20 second pixel value.

[0048] According to one embodiment, the multi-angle security feature(s) on the ID document can be one or more holograms. The additional multi-angle security feature(s) on the ID document can also be a hologram(s).

25 **[0049]** In some implementations, a video with the ID document tilted at different angles may be captured. The authentication method may be implemented on the video.

[0050] Figure 2, comprising Figure 2A and Figure 2B, is a schematic representation
30 200 illustrating an example of an authentication method, according to another embodiment. As mentioned above, in the user enrollment process of an eKYC process, a user may be required to take photographs of his/her ID document from different angles for submission as user enrollment images. A captured image may comprise an ID document image and a background image. As shown in Figure 2A, a captured
35 image 202 of an ID document tilted between -10 degrees and 10 degrees about a height of the ID document may be obtained. The captured image 202 may comprise an ID document image 204 and a background image 206. As shown in position 1 of Figure

2B, the captured image 202 may be an image of the ID document that is not tilted (i.e. 0 degree about the height of the ID document).

5 **[0051]** As mentioned above, image processing method(s) and/or system(s) may be implemented on the captured image 202 to remove the background image 206 and to align the ID document image 204. The aligned ID document image may be resized to 300x200 to obtain the reference image 208, whereby 300 denotes the width and 200 denotes the height of the reference image.

10 **[0052]** The user may be required to take another photograph of his/her ID document when the ID document is tilted between 15 degrees and 45 degrees about the height of the ID document and away from an image capturing device 216. As shown in Figure 2A and position 2 of Figure 2B, the user may tilt the right edge of the ID document away from the image capturing device 216 while holding the left edge of the ID
15 document in position.

[0053] The captured image 202' may comprise an ID document image 204' and a background image 206'. Similar to the manner in which the reference image 208 is obtained, image processing method(s) and/or system(s) may be implemented on the
20 captured image 202' to remove the background image 206' and to align the ID document image 204'. The aligned ID document image may also be resized to 300x200 to obtain the first image 208' for comparison with the reference image 208. As such, the reference image 208 and the first image 208' are of the same size 300x200.

25 **[0054]** With the reference image 208 and the first image 208' being the same size, a first difference image 210 may be generated based on a pixel-by-pixel comparison between the images. Image processing, using an image erosion method or an image dilation method, may be performed on the first difference image 210. As shown in Figure 2, a region of interest 212 with two holograms can be identified. The portions of
30 the first difference image 210 which correspond to the holograms may be of a lighter shade as compared to the other portions of the first difference image 210. A center point of each hologram may be identified and a radius from the center point to the boundary of each hologram may be determined. A circle may be plotted based on the center point and the radius to indicate the hologram. For better visualization, the circle
35 may be plotted in red.

[0055] A binary image 214 based on the region of interest 212 identified may be generated. The areas enclosed by the circles plotted may be associated with a pixel value of 128 and the remaining area of the binary image 214 may be associated with a pixel value of 0.

5

[0056] To increase the robustness of the authentication method and/or system, the user may further be required to take an additional photograph of his/her ID document when the ID document is tilted between 15 degrees and 45 degrees about the height of the ID document and towards an image capturing device 216. As shown in Figure 2A and position 3 of Figure 2B, the user may tilt the left edge of the ID document away from the image capturing device 216 while holding the right edge of the ID document in position.

10

[0057] The captured image 202" may comprise an ID document image 204" and a background image 206". Similar to the manner in which the reference image 208 is obtained, image processing method(s) and/or system(s) may be implemented on the captured image 202" to remove the background image 206" and to align the ID document image 204". The aligned ID document image may also be resized to 300x200 to obtain the second image 208" for comparison with the reference image 208. In this manner, the reference image 208 and the second image 208" may be of the same size 300x200.

15

20

[0058] With the reference image 208 and the second image 208" being the same size, a second difference image 210' may be generated based on a pixel-by-pixel comparison between the images. Image processing, using an image erosion method or an image dilation method, may be performed on the second difference image 210'. As shown in Figure 2, a region of interest 212' with a hologram can be identified. The portion of the second difference image 210' which corresponds to the hologram may be of a lighter shade as compared to the other portions of the second difference image 210'. A center point of the hologram may be identified and a radius from the center point to the boundary of the hologram may be determined. A circle may be plotted based on the center point and the radius to indicate the hologram. For better visualization, the circle may be plotted in red.

25

30

[0059] A binary image 214' based on the region of interest 212' identified may be generated. The area enclosed by the circle plotted may be associated with a pixel

35

value of 128 and the remaining area of the binary image 214' may be associated with a pixel value of 0.

5 **[0060]** As shown in Figure 2, areas with a pixel value of 128 which correspond to the holograms can be observed in the binary images 214, 214'. The ID document can be determined to be authentic.

10 **[0061]** To increase the robustness of the authentication method, the areas with a pixel value of 128 observed in the binary images 214, 214' can be compared. If there are differences between the areas, the ID document can be determined to be authentic. For example, as shown in Figure 2, the positions of the areas on the binary images 214, 214' may be different and the ID document can be determined to be authentic.

15 **[0062]** 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
20 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.

25 **[0063]** Figure 3 is a schematic diagram 300 illustrating an example of an authentication system, according to an embodiment. The authentication system comprises a reference image obtaining device 302 to obtain a reference image. The reference image is an image of an identification (ID) document. The authentication system further comprises a first image obtaining device 304 to obtain a first image for comparison with
30 the reference image. The first image is an image of the ID document tilted at a first angle. The authentication system also comprises a first difference image generating device 306 to generate a first difference image. The first difference image is based on a comparison between the reference image and the first image. Further, the authentication system comprises a region of interest identification device 308 to identify
35 one or more regions of interest based on the first difference image. The region(s) of interest corresponds to one or more multi-angle security features on the ID document.

The authentication system also comprises an authentication device 310 to authenticate the ID document based on the identification of the region(s) of interest.

5 **[0064]** The first image obtaining device 304 can be the same device or a different device as the reference image obtaining device 302. The reference image obtaining device 302 may comprise an image capturing device (e.g. a camera of a mobile phone) and a processor for executing software routines associated with image processing method(s) and/or system(s). The same processor or a different processor may be used to execute software routines to perform resizing of images. The first image obtaining
10 device 304 may comprise the same image capturing device or a different image capturing device, and the same processor or a different processor for executing software routines associated with image processing method(s) and/or system(s). The same processor or a different processor may be used to execute software routines to perform resizing of images. Each of the first difference image generating device 306,
15 the region of interest identification device 308 and the authentication device 310 can be implemented using the same processor or a different processor for executing different sets of software routines to generate a first difference image, identify a region of interest based on the first difference image and authenticate the ID document based on the identification of the region of interest, respectively.

20

[0065] According to one embodiment, the authentication system may further comprise a second image obtaining device to obtain a second image for comparison with the reference image. The second image may be an image of the ID document tilted at a second angle. The authentication system may also comprise a second difference
25 image generating device to generate a second difference image. The second difference image may be based on a comparison between the reference image and the second image. Further, the authentication system may comprise an additional region of interest identification device to identify one or more additional regions of interest based on the second difference image. The additional region(s) of interest may correspond to
30 one or more additional multi-angle security features on the ID document. The authentication system may also comprise the authentication device to authenticate the ID document based on the identification of the region(s) of interest and the additional region(s) of interest.

35 **[0066]** The second image obtaining device can be the same device or a different device as the reference image obtaining device 302 and/or the first image obtaining

device 304. The second difference image generating device can be the same device or a different device as first difference image generating device 306. The additional region of interest identification device can be the same device or a different device as the region of interest identification device 308. The authentication device to authenticate the ID document based on the identification of the region(s) of interest and the additional region(s) of interest can be the same device or a different device as the authentication device 310 to authenticate the ID document based on the identification of the region(s) of interest.

10 **[0067]** The reference image may be an image of the ID document tilted between -10 degrees and 10 degrees about a tilt axis. The tilt axis may correspond to a width of the ID document or a height of the ID document.

15 **[0068]** The first angle which the ID document is tilted at can be between 15 degrees and 45 degrees in a first direction about the tilt axis.

[0069] The second angle which the ID document is tilted at can be between 15 degrees and 45 degrees in a second direction about the tilt axis. The second direction may be opposite from the first direction.

20 **[0070]** According to one embodiment, sizes of the reference image and the first image may be same. The first difference image generating device may comprise a comparison device to perform a pixel-by-pixel comparison between the reference image and the first image to generate the first difference image.

25 **[0071]** The authentication system may further comprise an image processing device to perform image processing, using an image erosion method or an image dilation method, on the first difference image.

30 **[0072]** Further, the authentication system may comprise a binary image generating device to generate a binary image based on the region of interest identified. A first area of the binary image corresponding to the region of interest may be associated with a first pixel value, and a second area of the binary image outside a boundary of the first area may be associated with a second pixel value. The first pixel value can be different from the second pixel value.

35 **[0073]** According to one embodiment, the multi-angle security feature on the ID document can be one or more holograms.

[0074] According to one embodiment, a computing system for authentication of ID documents is provided. The computing system comprises at least one processor. The computing system also comprises a non-transitory computer-readable storage medium
5 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 reference image. The reference image is an image of an identification (ID) document. The programming instructions also instruct the at least one processor to obtain a first image for comparison with the reference image. The first
10 image is an image of the ID document tilted at a first angle. Further, the programming instructions instruct the at least one processor to generate a first difference image. The first difference image is based on a comparison between the reference image and the first image. The programming instructions also instruct the at least one processor to identify a region of interest based on the first difference image. The region of interest
15 corresponds to a multi-angle security feature on the ID document. The programming instructions further instruct the at least one processor to authenticate the ID document based on the identification of the region of interest.

20 **[0075]** Figure 4 shows a schematic diagram of a computer system suitable for use in executing at least some steps of the authentication method.

[0076] The following description of the computer system / computing device 400 is provided by way of example only and is not intended to be limiting.

25 **[0077]** 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
30 with other components of the computing device 400. The communication infrastructure 406 may include, for example, a communications bus, cross-bar, or network.

[0078] The computing device 400 further includes a main memory 408, such as a random access memory (RAM), and a secondary memory 410. The secondary
35 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.

[0079] 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.

[0080] 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 of 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.

[0081] 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.

[0082] 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.

[0083] 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.

[0084] 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.

[0085] 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.

5 **[0086]** It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the embodiments. 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 reference image, wherein the reference image is an image of an
5 identification (ID) document;
obtaining a first image for comparison with the reference image, wherein the
first image is an image of the ID document tilted at a first angle;
generating a first difference image, wherein the first difference image is based
on a comparison between the reference image and the first image;
10 identifying a region of interest based on the first difference image, wherein the
region of interest corresponds to a multi-angle security feature on the ID document;
and
authenticating the ID document based on the identification of the region of
interest.
15
2. The method as claimed in claim 1, further comprising:
obtaining a second image for comparison with the reference image, wherein the
second image is an image of the ID document tilted at a second angle;
generating a second difference image, wherein the second difference image is
20 based on a comparison between the reference image and the second image;
identifying an additional region of interest based on the second difference
image, wherein the additional region of interest corresponds to an additional multi-
angle security feature on the ID document; and
authenticating the ID document based on the identification of the region of
25 interest and the additional region of interest.
3. The method as claimed in claim 2, wherein the reference image is an image of
the ID document tilted between -10 degrees and 10 degrees about a tilt axis, and
wherein the tilt axis corresponds to a width of the ID document or a height of the ID
30 document.
4. The method as claimed in claim 3, wherein the first angle which the ID
document is tilted at is between 15 degrees and 45 degrees in a first direction about
the tilt axis.
35

5. The method as claimed in claim 4, wherein the second angle which the ID document is tilted at is between 15 degrees and 45 degrees in a second direction about the tilt axis, and wherein the second direction is opposite from the first direction.
- 5 6. The method as claimed in any one of the preceding claims, wherein:
sizes of the reference image and the first image are same; and
the comparison between the reference image and the first image to generate
the first difference image is based on a pixel-by-pixel comparison between the
reference image and the first image.
- 10 7. The method as claimed in any one of the preceding claims, further comprising:
performing image processing, using an image erosion method or an image
dilation method, on the first difference image.
- 15 8. The method as claimed in any one of the preceding claims, further comprising:
generating a binary image based on the region of interest identified, wherein a
first area of the binary image corresponding to the region of interest is associated with
a first pixel value, and a second area of the binary image outside a boundary of the first
area is associated with a second pixel value, and wherein the first pixel value is
20 different from the second pixel value.
9. The method as claimed in any one of the preceding claims, wherein the multi-angle security feature on the ID document is a hologram.
- 25 10. An authentication system, comprising:
a reference image obtaining device to obtain a reference image, wherein the
reference image is an image of an identification (ID) document;
a first image obtaining device to obtain a first image for comparison with the
reference image, wherein the first image is an image of the ID document tilted at a first
30 angle;
a first difference image generating device to generate a first difference image,
wherein the first difference image is based on a comparison between the reference
image and the first image;
a region of interest identification device to identify a region of interest based on
35 the first difference image, wherein the region of interest corresponds to a multi-angle
security feature on the ID document; and

an authentication device to authenticate the ID document based on the identification of the region of interest.

11. The system as claimed in claim 10, further comprising:

5 a second image obtaining device to obtain a second image for comparison with the reference image, wherein the second image is an image of the ID document tilted at a second angle;

a second difference image generating device to generate a second difference image, wherein the second difference image is based on a comparison between the
10 reference image and the second image;

an additional region of interest identification device to identify an additional region of interest based on the second difference image, wherein the additional region of interest corresponds to an additional multi-angle security feature on the ID document; and

15 the authentication device to authenticate the ID document based on the identification of the region of interest and the additional region of interest.

12. The system as claimed in claim 11, wherein the reference image is an image of the ID document tilted between -10 degrees and 10 degrees about a tilt axis, and
20 wherein the tilt axis corresponds to a width of the ID document or a height of the ID document.

13. The system as claimed in claim 12, wherein the first angle which the ID document is tilted at is between 15 degrees and 45 degrees in a first direction about
25 the tilt axis.

14. The system as claimed in claim 13, wherein the second angle which the ID document is tilted at is between 15 degrees and 45 degrees in a second direction about the tilt axis, and wherein the second direction is opposite from the first direction.

30 15. The system as claimed in any one of claims 10 to 14, wherein:

sizes of the reference image and the first image are same; and

the first difference image generating device comprises a comparison device to perform a pixel-by-pixel comparison between the reference image and the first image
35 to generate the first difference image.

16. The system as claimed in any one of claims 10 to 15, further comprising:
an image processing device to perform image processing, using an image erosion method or an image dilation method, on the first difference image.
- 5 17. The system as claimed in any one of claims 10 to 16, further comprising:
a binary image generating device to generate a binary image based on the region of interest identified, wherein a first area of the binary image corresponding to the region of interest is associated with a first pixel value, and a second area of the binary image outside a boundary of the first area is associated with a second pixel
10 value, and wherein the first pixel value is different from the second pixel value.
18. The system as claimed in any one of claims 10 to 17, wherein the multi-angle security feature on the ID document is a hologram.
- 15 19. A computing system comprising:
at least one processor;
a non-transitory computer-readable storage medium 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:
20 obtain a reference image, wherein the reference image is an image of an identification (ID) document;
obtain a first image for comparison with the reference image, wherein the first image is an image of the ID document tilted at a first angle;
generate a first difference image, wherein the first difference image is
25 based on a comparison between the reference image and the first image;
identify a region of interest based on the first difference image, wherein the region of interest corresponds to a multi-angle security feature on the ID document; and
authenticate the ID document based on the identification of the region of
30 interest.