

AN IDENTIFICATION DOCUMENT 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 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 his/her ID document. However, some attackers may use fraudulent 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 authenticated.

SUMMARY

[005] Embodiments seek to provide an identification (ID) document authentication method and an ID document authentication system which involve verifying the multi-angle security features of ID documents to detect attacks which use replicates of ID documents. The replicates of ID documents may include high resolution copies of genuine ID documents or fraudulent ID documents.

[006] According to one embodiment, there is provided an identification (ID) document authentication method, comprising: aligning a first ID document image and a second ID document image; cropping a first region of interest from the aligned first ID document image, wherein the first region of interest comprises a multi-angle security feature; performing a search to locate a second region of interest on the aligned second ID document image, wherein the second region of interest corresponds to the first region of interest; calculating a similarity score between the first region of interest and the second region of interest; and determining the authenticity of the ID document based on a comparison between the similarity score and a similarity threshold.

[007] According to another embodiment, there is provided an identification (ID) document authentication system, comprising: an alignment device configured to align a first ID document image and a second ID document image; an image cropping device configured to crop a first region of interest from the aligned first ID document image, wherein the first region of interest comprises a multi-angle security feature; a search device configured to perform a search to locate a second region of interest on the aligned second ID document image, wherein the second region of interest corresponds to the first region of interest; a score calculation device configured to calculate a similarity score between the first region of interest and the second region of interest; and an authentication device configured to determine the authenticity of the ID document based on a comparison between the similarity score and a similarity threshold.

BRIEF DESCRIPTION OF THE DRAWINGS

[008] 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:

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

[0010] Figure 2 is a schematic representation illustrating the example ID document authentication method of Figure 1.

[0011] Figure 3 is a schematic diagram illustrating an example of an ID document authentication system, according to an embodiment.

[0012] 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.

DETAILED DESCRIPTION

[0013] 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.

[0014] 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.

[0015] 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.

[0016] 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.

[0017] 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 disclosure 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 without departing from the spirit or scope of the invention.

[0018] 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.

[0019] 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.

[0020] 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 or fraudulent ID documents.

[0021] 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 multi-angle security feature, while some types of ID documents may have more than one multi-angle security features. Replicates of ID documents typically are unable to replicate the multi-angle security features of an authentic ID document. Therefore, verifying the multi-angle security features of ID documents may be useful in detecting attacks which use replicates of ID documents.

[0022] 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. In the user verification process, the same user may take a photograph of his/her face (i.e. a “selfie”) for submission as a user verification image.

[0023] According to one embodiment, the user may be required to take at least two photographs of his/her ID document from different angles for submission as user enrollment images. There are many methods that can be used to detect attacks that use ID document images of different ID documents from the same user, or ID document images of the same type of ID document from different users. For example, the detection method can be comparison of text information in the ID document images, or comparison of the user’s portraits in the ID document images using face recognition technologies. However, the main focus of the present specification is on the authentication of an ID document based on images of the same ID document.

[0024] In order to reduce the success rate of attacks that use replicates of ID documents, an ID document authentication method which involves comparing the similarity between regions of multi-angle security features on images of the ID documents may be implemented. The method may include a set of instructions to perform a sliding window search operation to locate the region of multi-angle security

features on the second image of the ID document submitted by the user. The regions of multi-angle security features on the first image and second image of the ID document can then be compared to determine if the ID document is authentic.

[0025] As mentioned above, replicates of ID documents typically do not replicate the multi-angle security features of an authentic ID document. Current ID document anti-fraud methods may not be able to fully utilize the multi-angle security features of ID documents to detect attacks which use replicates of ID documents. The techniques described in the present specification produce one or more technical effects. In particular, by computing the similarity between regions of multi-angle security features on the first image and second image of the ID document, the ID document authentication method and system may reduce the success rate of attacks to the eKYC process. If the regions of multi-angle security features on the first image and second image of the ID documents are determined to be similar, the ID document can be identified as a replicate of an ID document.

[0026] Further, the ID document authentication method and system may provide higher accuracy in detecting attacks that use replicates of ID documents. If a replicate of an ID document without multi-angle security feature is used, the similarity score is expected to be relatively high. In some instances, the similarity score can be as high as 1. As such, a replicate of an ID document can be accurately identified using the ID document authentication method and system.

[0027] The ID document authentication method and system may also provide higher efficiency in detecting attacks that use replicates of ID documents. It may be possible to train a model to detect attacks that use replicates of ID documents. However, practically, it may be time consuming and difficult to collect a relatively large number of ID document images that are in different angles. It may also be time consuming and difficult to collect relatively large amount of labeled training data for each multi-angle security feature of the ID documents, in order to train the model to obtain accuracy in detecting the attacks. In contrast to training a model, the ID document authentication method and system provided in the present specification may not require a large amount of training data. A threshold to determine the similarity between regions of multi-angle security features on the first image and second image of the ID document may be set with a relatively small number of data. An optimal number of steps which can be implemented with relatively high speed may also be used.

[0028] 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 first ID document image and a second ID document image are aligned. At step 104, a first region of interest from the aligned first ID document image is cropped. The first region of interest comprises a multi-angle security feature. At step 106, a search to locate a second region of interest on the aligned second ID document image is performed. The second region of interest corresponds to the first region of interest. At step 108, a similarity score between the first region of interest and the second region of interest is calculated. At step 110, the authenticity of the ID document is determined based on a comparison between the similarity score and a similarity threshold.

[0029] Figure 2 is a schematic representation 200 illustrating the example ID document authentication method of Figure 1. As mentioned above, the user may be required to take at least two photographs of his/her ID document from different angles for submission as user enrollment images. As shown in Figure 2, the first ID document image 202 and the second ID document image 204 may be images of an ID document captured at different angles.

[0030] According to an embodiment, the step 102 of aligning a first ID document image 202 and a second ID document image 204 may comprise performing image regression of the first ID document image 202 to determine first coordinates of four corner points of the first ID document image 202, and performing the image regression of the second ID document image 204 to determine second coordinates of four corner points of the second ID document image 204. The step 102 of aligning a first ID document image 202 and a second ID document image 204 may further comprise performing image warping of the first ID document image 202 based on the first coordinates of four corner points, and performing the image warping of the second ID document image 204 based on the second coordinates of four corner points. For the image regression, an ID document image can be an input and coordinates of four corner points of the ID document image is a possible output. For the image warping, the ID document image and the coordinates of four corner points of the ID document image can be the inputs, and an aligned ID document image is a possible output. Further, the image warping may be performed using opencv warping.

[0031] The step 104 of cropping the first region of interest 208 from the aligned first ID document image 206 may comprise determining an ID document type based on a classification model, selecting an ID document template corresponding to the

determined ID document type, defining a frame based on the identified ID document template, and cropping the first region of interest 208 from the aligned first ID document image 206 based on the defined frame.

[0032] The classification model for determining the ID document type may be trained using a dataset of ID document images of different ID documents. The trained classification model may be able to determine the ID document type based on an ID document image transmitted to it, without having to extract features of the ID document and match the features to a dataset. In some implementations, the trained classification model may be able to determine the ID document type based on the unaligned first ID document image 202 and the unaligned second ID document image 204 transmitted to it. In other words, the ID document type may be determined before aligning the first ID document image 202 and the second ID document image 204.

[0033] Generally, ID documents of the same type can have the same template. There can be many methods to obtain the template of an ID document type. For example, to obtain the template of a Hong Kong ID document, an image of a Hong Kong ID document can be captured or taken from available sources. With reference to step 102 of Figure 1, the image of the Hong Kong ID document can be aligned to obtain the template of the Hong Kong ID document.

[0034] Further, there can be many methods to define the frame for cropping the first region of interest 208 from the aligned first ID document image 206 for a particular ID document type. For example, research can be done using available sources to determine the security feature, including multi-angle security feature, of the Hong Kong ID document. Through the research, approximate location of the multi-angle security feature on the Hong Kong ID document can also be determined. With the template of the Hong Kong ID document obtained in the above mentioned method, the coordinates of the location of the multi-angle security feature on the Hong Kong ID document can be marked out. For example, the image size of the aligned ID document images may be 250 x 400 (height x width), and the coordinates (x, y) of the location of the multi-angle security feature can be (20, 135) at the top left and (120, 210) at the bottom right. These coordinates may define the frame for cropping the region of interest. For example, given a Hong Kong ID document image, after aligning the image to the image size of 250 x 400 (height x width), the region of interest can be cropped using the defined frame.

[0035] The step 106 of performing the search to locate the second region of interest 214 on the aligned second ID document image 210 may comprise varying a size of a search window 212 in a first set of steps. Each step in the first set of steps may comprise varying a position of the search window 212 in a second set of steps. A comparison score may be calculated at each step of the second set of steps, and a highest comparison score may be output as the similarity score. Calculating the comparison score may comprise converting the first region of interest 208 to a first grayscale image 216. The first grayscale image 216 may be represented by a first region of interest greyscale image matrix. Calculating the comparison score may also comprise converting the second region of interest 214 to a second grayscale image 218. The second grayscale image 218 may be represented by a second region of interest greyscale image matrix. Further, calculating the comparison score may comprise performing normalization for the first region of interest greyscale image matrix and the second region of interest greyscale image matrix, and performing a dot product operation on the normalized first region of interest greyscale image matrix and the normalized second region of interest greyscale image matrix. Normalization and dot product operation may be relatively quick methods to measure the distance between two images.

[0036] In some implementations, the search to locate the second region of interest 214 on the aligned second ID document image 210 may be a sliding search. The second region of interest 214 on the aligned second ID document image 210 located by the search may be the same region of interest as the first region of interest 208 on the aligned first ID document image 206, and the highest comparison score may be generated which may be output as the similarity score. The same region of interest may refer to the same size of the first and second regions of interest 208, 214, and also the same location of the first and second regions of interest 208, 214 on the aligned first and second ID document images 206, 210, respectively. The comparison score may be calculated based on the first and second regions of interest 208, 214 that are of the same size.

[0037] In some implementations, an opencv function `cv2.cvtColor()` may be used to convert the first region of interest 208 to a first grayscale image 216, and to convert the second region of interest 214 to a second grayscale image 218. The first and second region of interest greyscale image matrices may be 2-dimension matrices. Normalization for the first region of interest greyscale image matrix may be performed

by subtracting the means of the matrix from the matrix, followed by dividing the result by the standard deviation of the matrix. Normalization for the second region of interest greyscale image matrix may be performed using the same method.

[0038] As mentioned above, the step 106 of performing the search to locate the second region of interest 214 on the aligned second ID document image 210 may comprise varying a size of a search window 212 in a first set of steps. The first set of steps to vary the size of the search window 212 may go through the possible size ratios between the first region of interest 208 and the second region of interest 214. Size of the region of interest may not change for ID document images captured from different angles. However, aligning the ID document images may result in slight differences between the size of the first region of interest 208 and the size of the second region of interest 214. In other words, the size ratio between the first region of interest 208 and the second region of interest 214 may be almost 1:1, but may not be exactly 1:1. The first set of steps to vary the size of the search window 212 may go through a size ratio range of (0.9, 1.1), with an increase of 0.01 for each step. At each step, the search window 212 may be resized by the size ratio. For example, after resizing, the size of the search window 212 may be $h_0 \times w_0$ (height x width). In some implementations, the search window 212 size ratio range of (0.9, 1.1) may be fixed for an ID document type.

[0039] As mentioned above, each step in the first set of steps to vary the size of the search window 212 may comprise varying a position of the search window 212 in a second set of steps. The second set of steps may go through the possible locations of the second region of interest 214 on the aligned second ID document image 210. For example, with reference to the defined frame for cropping the region of interest as mentioned above, the aligned second ID document image 210 may be of a size 300 x 400 (height x width), and the defined frame may approximately be located at coordinates of ($y = 180$, $x = 40$). The second set of steps to vary the position of the search window 212 may go through a range of (170, 190) for the y-coordinate, and a range of (30, 50) for the x-coordinate, with an increase of 1 for each step. At each step, the second region of interest 214 that is of the size of the resized search window 212 ($h_0 \times w_0$ with reference to the example of resizing the search window 212 as mentioned above) may be cropped from the aligned second ID document image 210 at that location. In some implementations, the search range for y-coordinate and x-coordinate may be fixed for an ID document type.

[0040] As mentioned above, a comparison score may be calculated at each step of the second set of steps, and a highest comparison score may be output as the similarity score. In some implementations, the second step of steps may further comprise a variable to store a highest comparison score calculated in the second set of steps. For example, the variable may be termed as MAX variable. At each step in the second set of steps, if the calculated comparison score is higher than MAX variable, MAX variable may be updated with the higher comparison score. On the other hand, if the calculated comparison score is lower than MAX variable, MAX variable may remain unchanged. After completion of the second set of steps, the MAX variable may be the highest comparison score and may be output as the similarity score.

[0041] If a large number of steps is set for the first and second set of steps, the overall process of the ID document authentication method may be relatively slow. To provide accuracy and speed, the first and second set of steps may be designed with 20 steps each. In other words, the total number of steps may be 400.

[0042] According to an embodiment, the step 110 of determining the authenticity of the ID document may comprise authenticating the ID document on a condition that the similarity score is lower than the similarity threshold.

[0043] The similarity threshold may be determined with data collected. For example, authentic ID document samples and replicates of ID documents samples may be collected. Using the ID document authentication method provided in the present specification, similarity scores of the authentic documents and replicates of ID documents can be calculated to determine the similarity threshold. For example, if similarity scores of authentic documents are in the range of (0.5, 0.7) and similarity scores of replicates of ID documents are in the range of (0.7, 0.9), 0.7 may be an appropriate similarity threshold to set.

[0044] In the scenario that the ID document to be authenticated is an authentic ID document with multi-angle security feature, the region of interest may display different images when viewed from different angles. On the other hand, in the scenario that the ID document to be authenticated is a replicate of an ID document, such as a high resolution copy of genuine ID document or a fraudulent ID document, the replicate of the ID document may not have multi-angle security feature. Therefore, the region of interest on the replicate of an ID document may display the same image even when viewed from different angles, and the similarity score calculated may be as high as 1.

As such, a similarity score that is lower than the similarity threshold may indicate that the first region of interest 208 is substantially different from the second region of interest 214, therefore the ID document may be authentic. Otherwise, the ID document may be a replicate of an ID document.

[0045] In some implementations, a graphics processing unit may be used for the ID document authentication method and system. The first set of steps as mentioned above may remain the same, whereby each step provides a resized search window by a ratio. The resized search window may be treated as the kernel in convolutional neural network (CNN). Instead of using a second set of steps to crop the second region of interest, possible crops of the second region of interest may be stacked to a $H \times W \times C$ matrix. H and W can be the height and width of the second region of interest, and C can be the number of possible crops. The $H \times W \times C$ matrix may be treated as the feature map in CNN. A 2-dimension convolution may be performed with the feature map and kernel obtained. For this implementation, a higher processing speed of up to 400% may be achieved.

[0046] 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.

[0047] Figure 3 is a schematic diagram 300 illustrating an example of an ID document authentication system, according to an embodiment. The ID document authentication system comprises an alignment device 302 configured to align a first ID document image and a second ID document image. The ID document authentication system also comprises an image cropping device 304 configured to crop a first region of interest from the aligned first ID document image. The first region of interest comprises a multi-angle security feature. The ID document authentication system further comprises a search device 306 configured to perform a search to locate a second region of interest on the aligned second ID document image. The second region of interest corresponds

to the first region of interest. Further, the ID document authentication system comprises a score calculation device 308 configured to calculate a similarity score between the first region of interest and the second region of interest. The ID document authentication system also comprises an authentication device 310 configured to determine the authenticity of the ID document based on a comparison between the similarity score and a similarity threshold. The first ID document image and the second ID document image may be images of an ID document captured at different angles.

[0048] According to an embodiment, the alignment device 302 may be further configured to perform image regression of the first ID document image to determine first coordinates of four corner points of the first ID document image. The alignment device 302 may also be configured to perform the image regression of the second ID document image to determine second coordinates of four corner points of the second ID document image. Further, the alignment device 302 may be configured to perform image warping of the first ID document image based on the first coordinates of four corner points, and to perform the image warping of the second ID document image based on the second coordinates of four corner points.

[0049] The image cropping device 304 may be further configured to determine an ID document type based on a classification model, select an ID document template corresponding to the determined ID document type, define a frame based on the identified ID document template, and crop the first region of interest from the aligned first ID document image based on the defined frame.

[0050] The search device 306 may be further configured to vary a size of a search window in a first set of steps. Each step in the first set of steps may comprise varying a position of the search window in a second set of steps. The score calculation device 308 may be further configured to calculate a comparison score at each step of the second set of steps, and a highest comparison score may be output as the similarity score. The score calculation device 308 may be further configured to convert the first region of interest to a first grayscale image. The first grayscale image may be represented by a first region of interest grayscale image matrix. The score calculation device 308 may also be configured to convert the second region of interest to a second grayscale image. The second grayscale image may be represented by a second region of interest grayscale image matrix. Further, the score calculation device 308 may be configured to perform normalization for the first region of interest grayscale image matrix and the second region of interest grayscale image matrix. The score calculation

device 308 may be further configured to perform a dot product operation on the normalized first region of interest greyscale image matrix and the normalized second region of interest greyscale image matrix.

[0051] According to an embodiment, the authentication device 310 may be further configured to authenticate the ID document on a condition that the similarity score is lower than the similarity threshold.

[0052] 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.

[0053] The following description of the computer system / computing device 400 is provided by way of example only and is not intended to be limiting.

[0054] 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.

[0055] 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.

[0056] 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.

[0057] 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.

[0058] 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.

[0059] 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.

[0060] 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.

[0061] 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.

[0062] 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.

[0063] 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 identification (ID) document authentication method, comprising:
 - aligning a first ID document image and a second ID document image;
 - cropping a first region of interest from the aligned first ID document image, wherein the first region of interest comprises a multi-angle security feature;
 - searching the aligned second ID document image to locate a second region of interest that corresponds to the first region of interest, wherein searching the aligned second ID document image comprises varying a size of a search window in a first set of steps, wherein each step in the first set of steps comprises varying a position of the search window in a second set of steps;
 - calculating a similarity score between the first region of interest and the second region of interest; and
 - determining the authenticity of the ID document based on a comparison between the similarity score and a similarity threshold, wherein the ID document is authenticated in response to determining that the similarity score is lower than the similarity threshold.
2. The method as claimed in claim 1, wherein the first ID document image and the second ID document image are images of an ID document captured at different angles.
3. The method as claimed in claim 1 or 2, wherein aligning a first ID document image and a second ID document image comprises:
 - performing image regression of the first ID document image to determine first coordinates of four corner points of the first ID document image;
 - performing the image regression of the second ID document image to determine second coordinates of four corner points of the second ID document image;
 - performing image warping of the first ID document image based on the first coordinates of four corner points; and
 - performing the image warping of the second ID document image based on the second coordinates of four corner points.
4. The method as claimed in any one of the preceding claims, wherein cropping the first region of interest from the aligned first ID document image comprises:
 - determining an ID document type based on a classification model;
 - selecting an ID document template corresponding to the determined ID document type;

defining a frame based on the identified ID document template; and
 cropping the first region of interest from the aligned first ID document image based on the defined frame.

5. The method as claimed in any one of the preceding claims, wherein varying the size of the search window in the first set of steps further comprises varying the size of the search window based on size ratios between the first region of interest and the second region of interest.

6. The method as claimed in any one of the preceding claims, wherein a comparison score is calculated at each step of the second set of steps, and wherein a highest comparison score is output as the similarity score.

7. The method as claimed in claim 6, wherein calculating the comparison score comprises:

converting the first region of interest to a first grayscale image, wherein the first grayscale image is represented by a first region of interest grayscale image matrix;

converting the second region of interest to a second grayscale image, wherein the second grayscale image is represented by a second region of interest grayscale image matrix;

performing normalization for the first region of interest grayscale image matrix and the second region of interest grayscale image matrix; and

performing a dot product operation on the normalized first region of interest grayscale image matrix and the normalized second region of interest grayscale image matrix.

8. An identification (ID) document authentication system, comprising:

an alignment device configured to align a first ID document image and a second ID document image;

an image cropping device configured to crop a first region of interest from the aligned first ID document image, wherein the first region of interest comprises a multi-angle security feature;

a search device configured to:

search the aligned second ID document image to locate a second region of interest that corresponds to the first region of interest,

vary a size of a search window in a first set of steps, wherein each step in the first set of steps comprises varying a position of the search window in a second set of steps;

a score calculation device configured to calculate a similarity score between the first region of interest and the second region of interest; and

an authentication device configured to determine the authenticity of the ID document based on a comparison between the similarity score and a similarity threshold, wherein the ID document is authenticated in response to determining that the similarity score is lower than the similarity threshold.

9. The system as claimed in claim 9, wherein the first ID document image and the second ID document image are images of an ID document captured at different angles.

10. The system as claimed in claim 9 or 10, wherein the alignment device is further configured to:

perform image regression of the first ID document image to determine first coordinates of four corner points of the first ID document image;

perform the image regression of the second ID document image to determine second coordinates of four corner points of the second ID document image;

perform image warping of the first ID document image based on the first coordinates of four corner points; and

perform the image warping of the second ID document image based on the second coordinates of four corner points.

11. The system as claimed in any one of claims 9 to 11, wherein the image cropping device is further configured to:

determine an ID document type based on a classification model;

select an ID document template corresponding to the determined ID document type;

define a frame based on the identified ID document template; and

crop the first region of interest from the aligned first ID document image based on the defined frame.

12. The system as claimed in any one of claims 9 to 12, wherein the search device is further configured to vary the size of the search window based on size ratios between the first region of interest and the second region of interest.

13. The system as claimed in any one of claims 9 to 13, wherein the score calculation device is further configured to calculate a comparison score at each step of the second set of steps, and wherein a highest comparison score is output as the similarity score.

14. The system as claimed in claim 14, wherein the score calculation device is further configured to:

- convert the first region of interest to a first grayscale image, wherein the first grayscale image is represented by a first region of interest greyscale image matrix;

- convert the second region of interest to a second grayscale image, wherein the second grayscale image is represented by a second region of interest greyscale image matrix;

- perform normalization for the first region of interest greyscale image matrix and the second region of interest greyscale image matrix; and

- perform a dot product operation on the normalized first region of interest greyscale image matrix and the normalized second region of interest greyscale image matrix.