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. Generally, a business entity or service provider is unable to cross verify the identity of its customers against information in official databases, such as governments' databases. Therefore, many business entities and service providers use eKYC processes to verify the identity of their customers.

[003] 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.

[004] 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, screenshots of genuine ID documents or high resolution copies of genuine ID documents, during the eKYC processes.

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

SUMMARY

[006] Embodiments seek to provide an identification (ID) document authentication method and an ID document authentication system which involve obtaining labelled illuminated images of ID documents whilst different coloured lights are projected thereon, and verifying the colour changes on the ID documents to detect attacks which use replicates of ID documents. The replicates of ID documents may include screenshots of genuine ID documents, high resolution copies of genuine ID documents or fraudulent ID documents.

[007] According to one embodiment, there is provided an identification (ID) document authentication method, comprising: obtaining a plurality of labelled illuminated images, wherein each labelled illuminated image is an image of the ID document captured whilst a different coloured light is projected thereon, and tagged with a label corresponding to the different coloured light projected; generating, using a softmax function of a trained classifier model, a confidence score associated with the plurality of labelled illuminated images, wherein the plurality of labelled illuminated images is a consolidated input to the trained classifier model; and authenticating the ID document based on a comparison between the confidence score and a threshold.

[008] According to another embodiment, there is provided an identification (ID) document authentication system, comprising: an image obtaining device to obtain a plurality of labelled illuminated images, wherein each labelled illuminated image is an image of the ID document captured whilst a different coloured light is projected thereon, and tagged with a label corresponding to the different coloured light projected; a score generating device to generate, using a softmax function of a trained classifier model, a confidence score associated with the plurality of labelled illuminated images, wherein the plurality of labelled illuminated images is a consolidated input to the trained classifier model; and an authenticating device to authenticate the ID document based on a comparison between the confidence score and a threshold.

BRIEF DESCRIPTION OF THE DRAWINGS

[009] 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 identification (ID) document authentication method, according to an embodiment.

[0011] Figure 2 is a schematic representation illustrating an example of an ID document authentication method, according to another embodiment.

[0012] Figure 3 is a schematic diagram illustrating an example of an ID document 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 ID document authentication method.

DETAILED DESCRIPTION

[0014] 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.

[0015] 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.

[0016] 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.

[0017] 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.

[0018] 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 without departing from the spirit or scope of the invention.

[0019] 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.

[0020] 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.

[0021] 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. Current ID document authentication technologies may determine authenticity of an ID document by identifying moiré patterns or inconsistencies in the single ID document image. However, some attackers may use replicates of ID documents during the eKYC processes. The replicates of ID documents may include screenshots of genuine ID documents, high resolution copies of genuine ID documents or fraudulent ID documents. By making use of a single ID document image, current ID document authentication methods may not fully utilize available features of a genuine ID document to effectively authenticate the ID document. Therefore, it may be useful to make use of more than one ID document image in detecting attacks which use replicates of ID documents.

[0022] In addition, a genuine ID document may have different light reflecting properties and light absorption properties as compared to a replicate of ID document. For example, when red coloured light is projected onto a genuine ID document, visible colour changes on the ID document may be observed as the genuine ID document reflects the red coloured light. On the other hand, when the same red coloured light is projected onto a replicate of ID document, colour changes on the replicate of ID document may not be visible, or the colour changes observed on the replicate of ID document may be different from the colour changes that would have been observed on a genuine ID document. Therefore, projecting coloured lights onto ID documents and verifying the colour changes on the ID documents may be useful in detecting attacks which use replicates of ID documents.

[0023] 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 project different coloured lights onto his/her ID document and capture photographs of his/her ID document 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. The main focus of the present specification is on the authentication of an ID document in the user enrollment process.

[0024] According to one embodiment, the user may be required to project at least two different coloured lights onto his/her ID document and capture the respective images of his/her illuminated ID document for submission as user enrollment images.

[0025] In order to reduce the success rate of attacks that use replicates of ID documents, an ID document authentication method which involves analyzing the illuminated images of ID documents may be implemented. The method may include transmitting the illuminated images to a trained classifier model to generate a confidence score. Thereafter, the confidence score can be compared against a predefined threshold to determine if the ID document is genuine.

[0026] As mentioned above, a genuine ID document may have different light reflecting properties and light absorption properties as compared to a replicate of ID document. When projecting coloured lights onto a replicate of ID document, colour changes on the replicate of ID document may not be visible, or the colour changes observed on the replicate of ID document may be different from the colour changes that would have been observed on a genuine ID document.

[0027] The techniques described in the present specification produce one or more technical effects. In particular, by projecting coloured lights onto ID documents and verifying the colour changes on the ID documents, the ID document authentication method and system may reduce the success rate of attacks to the eKYC process. If the confidence score generated by the trained classifier model is higher than the predefined threshold, the ID document can be identified as a replicate of an ID document.

[0028] Further, the ID document authentication method and system may provide higher accuracy in detecting attacks that use replicates of ID documents. The classifier model may be trained using a large training dataset, thus can generate relatively accurate confidence scores. In addition, if a replicate of an ID document is used, the

confidence score is expected to be relatively high. As such, a replicate of an ID document can be accurately identified using the ID document authentication method and system.

[0029] 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 plurality of labelled illuminated images is obtained. Each labelled illuminated image is an image of the ID document captured whilst a different coloured light is projected thereon, and tagged with a label corresponding to the different coloured light projected. At step 104, a confidence score is generated using a softmax function of a trained classifier model. The confidence score is associated with the plurality of labelled illuminated images. The plurality of labelled illuminated images is a consolidated input to the trained classifier model. At step 106, the ID document is authenticated based on a comparison between the confidence score and a threshold. The classifier model can be a convolutional neural network (CNN) classifier. The last full connected layer of the CNN classifier may be a softmax layer which comprises a softmax function. The softmax function can have a vector as an input and a confidence score is a possible output. The softmax function can generate a confidence score between 0 and 1. A confidence score of 1 may indicate a high confidence level that the ID document is a replicate of an ID document.

[0030] The number of labelled illuminated images and the different coloured lights to be used in the ID authentication method may be pre-determined. Positive sample data and negative sample data may be prepared accordingly. The classifier model may then be trained using a large dataset of the positive and negative sample data.

[0031] As a non-limiting example, the number of labelled illuminated images may be pre-determined to be three. Accordingly, three different coloured lights may be used in the ID authentication method. Further, the three different coloured lights may be pre-determined to be red light, green light and blue light. In this example, the positive sample data can be labelled illuminated images of genuine ID documents projected with red light, green light and blue light separately. The labelled illuminated images may be tagged with labels corresponding to the red light, green light and blue light. On the other hand, the negative sample data can be labelled illuminated images of replicates of ID documents projected with red light, green light and blue light separately. Similarly, the labelled illuminated images may be tagged with labels

corresponding to the red light, green light and blue light. The same labels may be used for the labelled illuminated images of genuine ID documents and that of the replicates of ID documents.

[0032] The size of the training dataset may be represented by NxIxHxW, with N indicating the number of training images used in each iteration of the training process, I corresponding to the number of training images used in a set of consolidated input, H indicating the height of the training images and W indicating the width of the training images. In the above example which three labelled illuminated images are pre-determined to be used in the ID authentication method, the set of consolidated input may consist three training images. Accordingly, the value of I can be 9.

[0033] According to one embodiment, the trained classifier model may comprise a plurality of kernels with each kernel corresponding to a feature of an image of a genuine ID document captured whilst a coloured light is projected thereon.

[0034] As mentioned above, the user may be required to project at least two different coloured lights onto his/her ID document and capture the respective images of his/her illuminated ID document for submission as user enrollment images. The ID document authentication method can be implemented on illuminated ID document images of different sizes. The method can also be implemented on illuminated ID document images which have different alignments, for example the images of the ID documents may be captured at different angles.

[0035] Figure 2 is a schematic representation 200 illustrating an example of an ID document authentication method, according to another embodiment. The plurality of labelled illuminated images may comprise three labelled illuminated images. A first labelled illuminated image can be a first image of the ID document projected with a first coloured light. A second labelled illuminated image can be a second image of the ID document projected with a second coloured light, and a third labelled illuminated image can be a third image of the ID document projected with a third coloured light. The first coloured light can be red light, the second coloured light can be green light, and the third coloured light can be blue light. Further, the first coloured light, the second coloured light and the third coloured light can be projected onto the ID document in any order.

[0036] The source of the coloured lights can be a display screen of a mobile phone. As shown in Figure 2, the user may be required to configure the mobile phone screen 202 to display a coloured screen. Further, the user may be required to hold his/her ID document 222 and capture an image of the ID document using the front camera of the mobile phone, whilst the displayed coloured screen is shined thereon. As mentioned above, the coloured lights can be red light, green light and blue light. Accordingly, the mobile phone screen 202 may be set to display red coloured screen, green coloured screen and blue coloured screen separately and in any order. Consequently, three different illuminated images of the ID document can be captured.

[0037] Specifically, the mobile phone screen 202 may be set to display a red screen, and the red light from the screen may then be projected 204 onto the ID document. An image of the ID document illuminated with red light may be captured 210 and labelled as I_r. Similarly, the mobile phone screen 202 may be set to display a green screen, and the green light from the screen may then be projected 206 onto the same ID document. An image of the ID document illuminated with green light may be captured 212 and labelled as I_g. Further, the mobile phone screen 202 may be set to display a blue screen, and the blue light from the screen may then be projected 208 onto the ID document. An image of the ID document illuminated with blue light may be captured 214 and labelled as I_b. Labelled illuminated images I_r, I_g and I_b may be transmitted to a trained classifier model. The labelled illuminated images may be a consolidated input to the trained classifier model.

[0038] The classifier model may be a convolutional neural network (CNN) classifier 216. The CNN classifier 216 may generate a confidence score or live score 218 based on the labelled illuminated images. The ID document may then be determined to be a genuine ID document or replicate of ID document, or live or spoof 220, based on a comparison between the confidence score and a threshold.

[0039] According to one embodiment, the ID document authentication method may further comprise performing image processing on the plurality of labelled illuminated images to remove background images from the plurality of labelled illuminated images. An example of an image processing technique is an ID document detection method that can extract ID document images and remove background images from the labelled illuminated images. The ID document detection method may include a set of instructions based on open source software libraries such as TensorFlow, NumPy and OpenCV. By performing the image processing techniques on the labelled illuminated

images before transmitting them to the trained classifier model, more accurate results may be achieved.

[0040] As mentioned above and with reference to Figure 1, the ID document is authenticated based on a comparison between the confidence score and a threshold at step 106. According to one embodiment, the threshold may be set based on a receiver operating characteristic (ROC) curve, and authenticating the ID document may comprise authenticating the ID document on a condition that the confidence score is lower than the threshold. In some implementations, the ROC curve may be plotted based on testing data of the particular ID document type collected. The threshold may be the value on the ROC curve that corresponds to one percent false acceptance rate. In other implementations, testing data of different ID document types may be collected to plot the ROC curve. The threshold that is set based on the ROC curve plotted in this manner may be a fixed value for the different types of ID documents.

[0041] Instead of capturing each of the plurality of labelled illuminated images of an ID document individually, a video of the ID document illuminated with different coloured lights may be obtained. In some implementations, frames can be extracted from the video to obtain the respective labelled illuminated images. In other implementations, the video may be analyzed to determine the authenticity of the ID document.

[0042] For more robust fraud detection and greater accuracy of the ID document authentication method, a large number of different coloured lights may be used. The different coloured lights may include pink, yellow, purple, etc. Coloured lights of different shades, for example light red and dark red, may be used as well. In addition, the ID document authentication method may further comprise obtaining an additional ID document image which does not have any coloured light projected thereon.

[0043] 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.

[0044] 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 image obtaining device 302 to obtain a plurality of labelled illuminated images. Each labelled illuminated image is an image of the ID document captured whilst a different coloured light is projected thereon, and tagged with a label corresponding to the different coloured light projected. The ID document authentication system also comprises a score generating device 304 to generate, using a softmax function of a trained classifier model, a confidence score associated with the plurality of labelled illuminated images. The plurality of labelled illuminated images is a consolidated input to the trained classifier model. The ID document authentication system further comprises an authenticating device 306 to authenticate the ID document based on a comparison between the confidence score and a threshold.

[0045] As mentioned above, according to one embodiment, the image obtaining device 302 can be a front camera of a mobile phone. With reference to Figure 2, a user may be required to hold his/her ID document 222 and capture an image of the ID document using the front camera of the mobile phone, whilst a displayed coloured screen of the mobile phone is projected thereon. The score generating device 304 can be implemented using a processor for executing software routines of the trained classifier model. The classifier model can be a convolutional neural network (CNN) classifier. The authenticating device 306 can be the same processor or a different processor for executing another set of software routines to compare the confidence score and the threshold for determining the authenticity of the ID document.

[0046] The trained classifier model may comprise a plurality of kernels with each kernel corresponding to a feature of an image of a genuine ID document captured whilst a coloured light is projected thereon.

[0047] According to one embodiment, the plurality of labelled illuminated images may comprise three labelled illuminated images. A first labelled illuminated image can be a first image of the ID document projected with a first coloured light. A second labelled illuminated image can be a second image of the ID document projected with a second coloured light, and a third labelled illuminated image can be a third image of the ID document projected with a third coloured light. The first coloured light can be red light,

the second coloured light can be green light, and the third coloured light can be blue light. Further, the first coloured light, the second coloured light and the third coloured light can be projected onto the ID document in any order.

[0048] According to one embodiment, the ID document authentication system may further comprise an image processing device to perform image processing on the plurality of labelled illuminated images to remove background images from the plurality of labelled illuminated images.

[0049] As mentioned above, the ID document authentication system comprises an authenticating device 306 to authenticate the ID document based on a comparison between the confidence score and a threshold. According to one embodiment, the threshold may be determined based on a receiver operating characteristic curve, and the ID document may be authenticated on a condition that the confidence score is lower than the threshold.

[0050] 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.

[0051] The following description of the computer system / computing device 400 is provided by way of example only and is not intended to be limiting.

[0052] 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.

[0053] 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.

[0054] 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.

[0055] 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.

[0056] 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.

[0057] 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.

[0058] 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.

[0059] 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.

[0060] 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.

[0061] 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:

obtaining a plurality of labelled illuminated images, wherein each labelled illuminated image is an image of the ID document captured whilst a different coloured light is projected thereon, and tagged with a label corresponding to the different coloured light projected;

generating, using a softmax function of a trained classifier model, a confidence score associated with the plurality of labelled illuminated images, wherein the plurality of labelled illuminated images is a consolidated input to the trained classifier model; and

authenticating the ID document based on a comparison between the confidence score and a threshold.

2. The method as claimed in claim 1, wherein the trained classifier model comprises a plurality of kernels with each kernel corresponding to a feature of an image of a genuine ID document captured whilst a coloured light is projected thereon.

3. The method as claimed in any one of the preceding claims, wherein the plurality of labelled illuminated images comprises three labelled illuminated images, and wherein:

a first labelled illuminated image is a first image of the ID document projected with a first coloured light;

a second labelled illuminated image is a second image of the ID document projected with a second coloured light; and

a third labelled illuminated image is a third image of the ID document projected with a third coloured light.

4. The method as claimed in claim 3, wherein the first coloured light is red light, the second coloured light is green light, and the third coloured light is blue light, and wherein the first coloured light, the second coloured light and the third coloured light are projected onto the ID document in any order.

5. The method as claimed in any one of the preceding claims, further comprising performing image processing on the plurality of labelled illuminated images to remove background images from the plurality of labelled illuminated images.

6. The method as claimed in any one of the preceding claims, wherein the threshold is determined based on a receiver operating characteristic curve, and wherein authenticating the ID document comprises authenticating the ID document on a condition that the confidence score is lower than the threshold.

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

an image obtaining device to obtain a plurality of labelled illuminated images, wherein each labelled illuminated image is an image of the ID document captured whilst a different coloured light is projected thereon, and tagged with a label corresponding to the different coloured light projected;

a score generating device to generate, using a softmax function of a trained classifier model, a confidence score associated with the plurality of labelled illuminated images, wherein the plurality of labelled illuminated images is a consolidated input to the trained classifier model; and

an authenticating device to authenticate the ID document based on a comparison between the confidence score and a threshold.

8. The system as claimed in claim 7, wherein the trained classifier model comprises a plurality of kernels with each kernel corresponding to a feature of an image of a genuine ID document captured whilst a coloured light is projected thereon.

9. The system as claimed in claim 7 or 8, wherein the plurality of labelled illuminated images comprises three labelled illuminated images, and wherein:

a first labelled illuminated image is a first image of the ID document projected with a first coloured light;

a second labelled illuminated image is a second image of the ID document projected with a second coloured light; and

a third labelled illuminated image is a third image of the ID document projected with a third coloured light.

10. The system as claimed in claim 9, wherein the first coloured light is red light, the second coloured light is green light, and the third coloured light is blue light, and wherein the first coloured light, the second coloured light and the third coloured light are projected onto the ID document in any order.

11. The system as claimed in any one of claims 7 to 10, further comprising an image processing device to perform image processing on the plurality of labelled illuminated images to remove background images from the plurality of labelled illuminated images.

12. The system as claimed in any one of claims 7 to 11, wherein the threshold is determined based on a receiver operating characteristic curve, and wherein the ID document is authenticated on a condition that the confidence score is lower than the threshold.