

AUTHENTICATION METHOD AND SYSTEM

TECHNICAL FIELD

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

BACKGROUND

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

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

[004] One of the most common forms of identity fraud during the eKYC process involves attackers uploading photos of ID cards that are displayed on an electronic display screen, instead of a physical ID card. Current methods to detect such forms of fraud include training a classification model of two classes: real card and "fake" card image captured from an electronic display screen, or by designing an algorithm to detect special patterns observed on an electronic display screen such as moiré pattern. However, there are several limitations to these methods. First, the data labelling task is very time consuming. Second, in some cases the special patterns observed on an electronic display screen such as moiré pattern are difficult to detect due to the high resolution of the display screen.

[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 system which involves a flash light based anti-spoofing method to detect images of electronic display screens that are displaying an ID document.

[007] According to one embodiment, there is provided an authentication method, including: receiving an image of an ID document, wherein the image is either captured whilst a flash light is projected onto (i) the ID document or (ii) an electronic display of the ID document; generating an authentication score associated with the image using a convolutional neural network (CNN), wherein the CNN is trained with training data comprising images of ID documents captured whilst a flash light is projected onto each of the ID documents and images of electronic displays of ID documents captured whilst the flash light is projected onto each of the electronic displays; and authenticating the ID document based on a comparison between the authentication score and a predetermined threshold.

[008] According to another embodiment, there is provided an authentication system, including: a receiver device configured to receive an image of an ID document, wherein the image is either captured whilst a flash light is projected onto (i) the ID document or (ii) an electronic display of the ID document; a score generating device configured to generate an authentication score associated with the image using a convolutional neural network (CNN), wherein the CNN is trained with training data comprising images of ID documents captured whilst a flash light is projected onto each of the ID documents and images of electronic displays of ID documents captured whilst the flash light is projected onto each of the electronic displays; and an authenticating device configured to authenticate the ID document based on a comparison between the authentication score and a predetermined 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 1a shows an image of a physical ID card and Figure 1b shows an image of an ID card that is displayed on an electronic display screen.

[0011] Figure 2a shows an example of a physical ID card having a flash light projected thereon; and Figure 2b shows an example of an electronic display screen that is displaying an image of an ID card, having a flash light projected on the electronic display screen.

[0012] Figure 3 is a flow chart 300 illustrating an example of an identification (ID) document authentication method, 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 identification document authentication method.

[0014] Figure 5 is a schematic diagram illustrating an example of an identification document authentication system, according to an embodiment.

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 described herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the invention.

[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 to commit identity fraud. The replicates of ID documents may include high resolution copies of genuine ID documents or fraudulent ID documents. One of the most common forms of identity fraud during the eKYC process involves attackers uploading photos of ID documents that are displayed on an electronic display screen, instead of a physical ID card.

[0023] Embodiments seek to provide an identification (ID) document authentication method and system which involves a flash light based anti-spoofing method to detect images of electronic display screens that are displaying an ID document.

[0024] Current methods to detect identity fraud during the eKYC process involve training a classification model of two classes: real physical card and “fake” card image captured from an electronic display screen. However, the data labelling task for the classification model is very time consuming and creates a bottleneck. Accordingly, optimization of the process is very difficult. Furthermore, in some cases the special patterns observed on an electronic display screen such as moiré pattern are difficult to detect due to the high resolution of the display screen.

[0025] The techniques described in the present specification produce one or more technical effects. In particular, by implementing a flash light based anti-spoofing

method to detect images of electronic display screens that are displaying an ID document, the difficulty of classification is reduced. In particular, by projecting a flash light during the ID document image capturing process and classifying the resulting flash feature, it is possible to overcome the bottleneck of classifying of physical documents and “screen-retaken” documents (i.e. ID documents that are being displayed on an electronic display screen).

[0026] Figure 1a shows an image of a physical ID card while Figure 1b shows an image of an ID card that is displayed on an electronic display screen (i.e. a high resolution display of a genuine ID card, such as a screenshot or photograph). Due to the high resolution of the electronic display screen, there is minimal screen pattern (e.g. moiré pattern) in the image, thus it is difficult to distinguish the two images Figure 1a and 1b.

[0027] However, if a flash light function is activated when capturing the images (e.g. using a mobile phone camera with flash light activated), the flash pattern between these two ID card images becomes significantly more distinguishable due to the difference in material and surface between a physical ID card and an electronic display screen (e.g. a screen of another mobile phone or computer monitor). In this context, capturing an image of an ID card that is displayed on an electronic display screen refers to taking a photo of an electronic display screen, wherein the electronic display screen is displaying at least an image of an ID card.

[0028] Figure 2a shows an example of a physical ID card having a flash light projected thereon; and Figure 2b shows an example of an electronic display screen that is displaying an image of an ID card, having a flash light projected on the electronic display screen. In this instance, it can be observed that a flash pattern on the physical ID has a relatively higher reflection intensity / brightness and larger flash-size compared to a “screen-retaken” card (i.e. an ID card that is being displayed on an electronic display screen). In other instances, a flash pattern on the physical ID may have a relatively lower reflection intensity / brightness and/or smaller flash-size compared to a “screen-retaken” card,

[0029] According to an implementation, a convolutional neural network (CNN) is trained to distinguish and classify a flash pattern observed on a surface of a physical ID document and an electronic display screen (that is displaying an image of an ID document), whilst a flash light is projected thereon. In this manner, it is possible to

determine whether an image presented for authentication is an image of a physical card or a “screen-retaken” card.

[0030] The training dataset may include (i) images of physical ID documents, each having a flash light projected on the physical document and (ii) images of electronic display screens that are displaying an ID document, each having a flash light projected on the electronic display screen. For (ii), a wide variety of electronic display screens may be used to increase robustness of the model. For example, mobile phone screens, computer monitor screens, laptop computer screens, tablet computer screens and television screens having various specification (e.g. resolution, refresh rate, contrast ratio, response time, curved screen, flat screen, panel type (e.g. In-plane Switching (IPS), Organic light-emitting diode (OLED)), screen material (e.g. glass, plastic)), etc.

[0031] Additionally, the training dataset may include images of all types of ID documents from a variety of organizations/jurisdictions/states/countries such as, but not limited to: ID card, driving license, passport, membership card.

[0032] Flash patterns may vary across electronic display screens and physical ID documents. For example, a desktop monitor screen may have different flash pattern from a mobile phone screen. By training the CNN with a training dataset as described above, the CNN model can learn the diversity of flash patterns observed on surfaces of physical ID documents and electronic display screens.

[0033] The output of the CNN model is a score ranging from 0 to 1. The score represents a probability of whether the image is (i) an image of a physical ID document or (ii) an image of an electronic screen that is displaying an ID document. Whether the score being close to 1 or close to 0 implying a physical card is determined by how the class is defined. If physical ID document is set to be positive class and “screen-retaken” ID document is set to be negative class, then a score close to 1 implies physical ID document. On the other hand, if “screen-retaken” ID document is set to be positive class and physical ID is set to be negative class, then a score close to 0 implies a “screen-retaken” ID document. In an embodiment, the naturally ‘abnormal’ case is set to be positive class, which means the “screen-retaken” ID document is set to positive class. Therefore a score close to 0 implies that the image is an image of a physical ID document whereas a score close to 1 implies that the image is an image of an electronic screen that is displaying an ID document.

[0034] The score can be compared to a threshold to provide an output whether the image is authentic or not, i.e. an image of a physical ID document or not. The threshold can be established depending on application requirements (e.g. some applications require relatively higher accuracy than others and therefore the threshold is set higher). The threshold may be determined based on a validation dataset. The validation dataset comprises both (i) images of physical ID documents, each having a flash light projected on the physical document and (ii) images of electronic display screens that are displaying an ID document, each having a flash light projected on the electronic display screen. A receiver operating characteristic (ROC) curve can be established from the validation data. In an implementation, from the ROC curve, the threshold is set when the FAR (false accepted rate) is equal to 0.01 or 0.001.

[0035] In an implementation, before feeding an image to the CNN to determine whether the image is of a physical card or a “screen-retaken” card, one or more pre-processing steps can be performed to further increase accuracy of authentication, e.g. cropping to remove any background image surrounding the ID document and/or rotating the ID document. In one implementation, for proper orientation and avoidance of unnecessary background, a user interface at the user / client end can display a frame to guide the user to align the ID document within the frame.

[0036] Figure 3 is a flow chart 300 illustrating an example of an identification (ID) document authentication method, according to an embodiment. At step 302, an image of the ID document is received (e.g. from a user / client end). In an example scenario, the user / client wishes to submit his/her ID document during an eKYC process. The user / client is instructed (e.g. by a user interface of a mobile application) to capture an image of his/her ID document using a mobile phone camera with a flash light activated. If a bona fide user presents his/her own physical ID document, the image is captured whilst a flash light is projected onto the ID document. On the other hand, a fraudster presents an image which is captured whilst a flash light is projected onto an electronic display of the ID document (i.e. an image of an electronic screen that is displaying the ID document). The electronic display of the ID document includes a display screen of an electronic device that is displaying a photograph or screenshot of the ID document.

[0037] At step 304, an authentication score associated with the image (received at step 302) is generated using a convolutional neural network (CNN). The CNN is trained with training data comprising images of ID documents captured whilst a flash light is

projected onto each of the ID documents and images of electronic displays of ID documents captured whilst a flash light is projected onto each of the electronic displays. Details on the training dataset have been provided above.

[0038] In an embodiment, the CNN is configured to generate the authentication score by classifying a flash pattern that is present on the ID document or the electronic display of the ID document whilst the flash light is projected thereon. As shown in Figures 2a and 2b, a characteristic of the flash pattern comprises at least one of: brightness of the flash light that is reflected off a surface of the ID document or the electronic display, and size of the flash light that is reflected off the surface of the ID document or the electronic display.

[0039] In an embodiment, the authentication score corresponds to a probability of the image being captured whilst the flash light is projected onto (i) the ID document and/or (ii) the electronic display of the ID document.

[0040] At step 306, the ID document is authenticated based on a comparison between the authentication score and a predetermined threshold. In the case that an authentication score close to 0 is set to imply that the image is an image of a physical ID document whereas an authentication score close to 1 is set to imply that the image is an image of an electronic screen that is displaying an ID document, it follows that if the authentication score being less than the predetermined threshold provides an indication that the image is captured whilst the flash light is projected onto the physical ID document. The predetermined threshold can be established based on a validation dataset, as described above.

[0041] In an embodiment, one or more pre-processing steps can be performed to further increase accuracy of authentication, e.g. cropping to remove any background image surrounding the ID document. Cropping may involve the following steps. First, a raw image of the ID document is received from the user / client end. A supplementary CNN is used to determine a type of the ID document (e.g. a Hong Kong Identity Card) in the raw image. The supplementary CNN can be trained with images of all types of ID documents from a variety of organizations/jurisdictions/states/countries such as, but not limited to: ID card, driving license, passport, membership card. A frame is selected based on the determined type of the ID document. This is because different types of ID documents are expected to have different sizes, features, etc. The raw image of the ID

document can be cropped using the selected frame to generate the image of the ID document that is used for authentication at step 302.

[0042] 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.

[0043] The following description of the computer system / computing device 400 is provided by way of example only and is not intended to be limiting.

[0044] As shown in Figure 4, the example computing device 400 includes a processor 304 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.

[0045] 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.

[0046] 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.

[0047] The computing device 400 also includes at least one communication interface 424. The communication interface 424 allows software and data to be transferred between computing device 400 and external devices via a communication path 426. In various embodiments, the communication interface 424 permits data to be transferred between the computing device 400 and a data communication network, such as a public data or private data communication network. The communication interface 424 may be used to exchange data between different computing devices 400 which such computing devices 400 form part an interconnected computer network. Examples of a communication interface 424 can include a modem, a network interface (such as an Ethernet card), a communication port, an antenna with associated circuitry and the like. The communication interface 424 may be wired or may be wireless. Software and data transferred via the communication interface 424 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by communication interface 424. These signals are provided to the communication interface via the communication path 426.

[0048] 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.

[0049] 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.

[0050] 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.

[0051] 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.

[0052] 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.

[0053] Figure 5 is a schematic diagram illustrating an identification (ID) document authentication system 500, according to an embodiment. The system 500 includes a receiver device 502, a score generating device 504 and an authenticating device 506. The receiver device 502 receives an image of the ID document. The image is either captured whilst a flash light is projected onto (i) the ID document or (ii) an electronic display of the ID document. The score generating device 504 generates an authentication score associated with the image using a convolutional neural network (CNN). The CNN is trained with training data comprising images of ID documents captured whilst a flash light is projected onto each of the ID documents and images of electronic displays of ID documents captured whilst the flash light is projected onto each of the electronic displays. The authenticating device 506 authenticates the ID

document based on a comparison between the authentication score and a predetermined threshold.

[0054] The authentication score corresponds to a probability of the image being captured whilst the flash light is projected onto (i) the ID document and/or (ii) the electronic display of the ID document. The authentication score being less than the predetermined threshold provides an indication that the image is captured whilst the flash light is projected onto the ID document. The predetermined threshold can be established based on a validation dataset.

[0055] The score generating device 504 can classify, using the CNN, a flash pattern that is present on the ID document or the electronic display of the ID document to generate the authentication score. A characteristic of the flash pattern comprises at least one of: brightness of the flash light that is reflected off a surface of the ID document or the electronic display, and size of the flash light that is reflected off the surface of the ID document or the electronic display.

[0056] The electronic display of the ID document comprises a display screen of an electronic device that is displaying a photograph or screenshot of the ID document.

[0057] The system 500 can further comprise an image processing device 508 that: receives a raw image of the ID document; determines a type of the ID document using a supplementary CNN; selects a frame based on the determined type of the ID document; and crops the raw image of the ID document using the selected frame to generate the image of the ID document.

[0058] 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.

[0059] It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

CLAIMS

1. An authentication method, comprising:
 - receiving a raw image of an ID document, wherein the raw image is captured whilst a flash light is projected onto the ID document or an electronic display of the ID document;
 - determining a type of the ID document using a supplementary convolutional neural network (CNN), wherein the supplementary CNN is trained with training data comprising images of different types of ID documents;
 - selecting a frame based on the determined type of the ID document;
 - cropping the raw image of the ID document using the selected frame to generate a cropped image of the ID document.
 - receiving the cropped image of the ID document;
 - generating an authentication score associated with the cropped image using a CNN, wherein the CNN is trained with training data comprising images of ID documents captured whilst a flash light is projected onto each of the ID documents and images of electronic displays of ID documents captured whilst the flash light is projected onto each of the electronic displays; and
 - authenticating the ID document based on a comparison between the authentication score and a predetermined threshold.
2. The method as claimed in claim 1, wherein generating the authentication score using the CNN further comprises:
 - classifying, by the CNN, a flash pattern that is present on the ID document or the electronic display of the ID document.
3. The method as claimed in claim 2, wherein a characteristic of the flash pattern comprises at least one of:
 - brightness of the flash light that is reflected off a surface of the ID document or the electronic display, and
 - size of the flash light that is reflected off the surface of the ID document or the electronic display.
4. The method as claimed in any one of the preceding claims, wherein the authentication score corresponds to a probability of the image being captured whilst

the flash light is projected onto (i) the ID document and/or (ii) the electronic display of the ID document.

5. The method as claimed in claim 4, wherein the authentication score being less than the predetermined threshold provides an indication that the image is captured whilst the flash light is projected onto the ID document, and wherein the predetermined threshold is established based on a validation dataset.

6. The method as claimed in any one of the preceding claims, wherein the electronic display of the ID document comprises a display screen of an electronic device that is displaying a photograph or screenshot of the ID document.

7. An authentication system, comprising:

an image processing device configured to:

receive a raw image of an ID document, wherein the raw image is captured whilst a flash light is projected onto the ID document or an electronic display of the ID document;

determine a type of the ID document using a supplementary convolutional neural network (CNN), wherein the supplementary CNN is trained with training data comprising images of different types of ID documents;

select a frame based on the determined type of the ID document;

crop the raw image of the ID document using the selected frame to generate a cropped image of the ID document;

a receiver device configured to receive the cropped image of the ID document;

a score generating device configured to generate an authentication score associated with the cropped image using a CNN, wherein the CNN is trained with training data comprising images of ID documents captured whilst a flash light is projected onto each of the ID documents and images of electronic displays of ID documents captured whilst the flash light is projected onto each of the electronic displays; and

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

8. The system as claimed in claim 8, wherein the score generating device is further configured to classify, using the CNN, a flash pattern that is present on the ID

document or the electronic display of the ID document to generate the authentication score.

9. The system as claimed in claim 9, wherein a characteristic of the flash pattern comprises at least one of:

brightness of the flash light that is reflected off a surface of the ID document or the electronic display, and

size of the flash light that is reflected off the surface of the ID document or the electronic display.

10. The system as claimed in any one of claims 8 to 10, wherein the authentication score corresponds to a probability of the image being captured whilst the flash light is projected onto (i) the ID document and/or (ii) the electronic display of the ID document.

11. The system as claimed in claim 11, wherein the authentication score being less than the predetermined threshold provides an indication that the image is captured whilst the flash light is projected onto the ID document, and wherein the predetermined threshold is established based on a validation dataset.

12. The system as claimed in any one of claims 8 to 12, wherein the electronic display of the ID document comprises a display screen of an electronic device that is displaying a photograph or screenshot of the ID document.