

METHOD AND SYSTEM FOR DETERMINING AUTHENTICITY OF AN OFFICIAL DOCUMENT

TECHNICAL FIELD

[0001] The present disclosure relates broadly, but not exclusively, to a method and system for determining authenticity of an official document.

BACKGROUND

[0002] Know Your Customer (KYC) is a form of due diligence that a business does in order to verify the authenticity, identity, risks, etc. of its customers/clients either before or during the time that it starts doing business with them. Electronic Know Your Customer (eKYC), or digital KYC, is a paperless process that is performed by the business, usually through use of a computer, and may sometimes be initiated by a customer. In the eKYC process, there are typical steps including scanning an identity (ID) card and detecting a live face. During the process of scanning an ID card, it is usually necessary to check the authenticity of the ID card.

[0003] Techniques to detect fake ID cards have been proposed in the art. One previous fake ID card detection method involves detecting security features, such as landmarks or holograms, to verify the authenticity of the ID card. In such method, it is necessary to capture ID card images from multiple different angles, and then verify the different color changes to recognize the authenticity of the ID card. This and other conventional methods typically require the users to cooperate when taking ID card images. For example, the ID card is required to be located in a predefined user interface (UI) box exactly when taking several images of the ID card from different angles. The above processes are considered too cumbersome and can make the user experience unpleasant.

[0004] A need therefore exists to provide methods and devices that can improve the detection of abnormal ID cards.

SUMMARY

[0005] An embodiment of the present disclosure provides a method for determining authenticity of an official document. The method includes receiving document image data and background image data of a single image of the official document; applying a first trained residual neural network to extract global features of the official document from both the document image data and the background image data and to calculate a first score indicating normality of the official document and at least one second score indicating abnormality of the official document; applying a second trained residual neural network to extract local features of the official document from only the document image data and to calculate at least one third score indicating abnormality of the official document; and determining whether the official document is authentic based on a comparison of the first score with the at least one second score and at least one third score.

[0006] Another embodiment of the present disclosure provides a system for determining authenticity of an official document. The system includes a processor and a computer-readable memory coupled to the processor and having instructions stored thereon. The instructions are executable by the processor to identify document image data and background image data of a single image of the official document; apply a first trained residual neural network to extract global features of the official document from both the document image data and the background image data and to calculate a first score indicating normality of the official document and at least one second score indicating abnormality of the official document; apply a second trained residual neural network to extract local features of the official document from only the document image data and to calculate at least one third score indicating abnormality of the official document; and determine whether the official document is authentic based on a comparison of the first score with the at least one second score and at least one third score.

[0007] Another embodiment of the present disclosure provides an apparatus including an input device configured to receive document image data and background image data of a single image of an official document, and a processing device configured to feed the data to a first trained residual neural network and a second trained residual neural network respectively. The first trained residual neural network includes an algorithm to extract global features of the official document from both the document image data and the background image data and

to calculate a first score indicating normality of the official document and at least one second score indicating abnormality of the official document. The second trained residual neural network includes an algorithm to extract local features of the official document from only the document image data and to calculate at least one third score indicating abnormality of the official document. The processing device is further configured to determine whether the official document is authentic based on a comparison of the first score with the at least one second score and at least one third score.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Embodiments of the disclosure will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

[0009] Figure 1 shows a flowchart illustrating a method for determining authenticity of an official document according to an embodiment.

[0010] Figure 2 shows a flowchart illustrating a detailed example implementation of the method of Figure 1.

[0011] Figure 3 shows a schematic diagram of an apparatus suitable for implementing the method of Figure 1.

[0012] Figure 4 shows a schematic diagram illustrating a computer system suitable for implementing the method of Figure 1.

[0013] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been depicted to scale. For example, the dimensions of some of the elements in the illustrations, block diagrams or flowcharts may be exaggerated in respect to other elements to help to improve understanding of the present embodiments.

DETAILED DESCRIPTION

[0014] The present disclosure provides methods and devices to determine whether an official document, such as an identity card, is genuine based on a single image of the official document. In the present disclosure, it is recognized that a fake official document may be broadly categorized as one that is not physically present (for example, a screenshot or photocopy is being used), or one that has irregular features (for example, signs of tampering, or features which are occluded, erased, out of position, etc.). By utilizing both global features and local features extracted by neural networks, the present methods and devices can recognize various types of fake documents, thereby distinguishing an authentic document from a fake document. In the context of eKYC applications, for example, the present methods and devices can help to determine (1) whether the user (e.g. a customer) is actually in physical possession of a required official document, and (2) whether the official document being submitted for verification is genuine or not.

[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 “scanning”, “calculating”, “determining”, “applying”, “extracting”, “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 conventional computer will appear from the description below.

[0019] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the 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 scope of the disclosure.

[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, GPRS, 3G, 4G or 5G mobile telephone systems, as well as other wireless systems such as Bluetooth, ZigBee, Wi-Fi. 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] The present disclosure may also be implemented as hardware elements. More particularly, in the hardware sense, an element is a functional hardware unit designed

for use with other components or elements. For example, an element may be implemented using discrete electronic components, or it can form a portion of an entire electronic circuit such as an Application Specific Integrated Circuit (ASIC) or Field Programmable Gate Array (FPGA). Numerous other possibilities exist. Those skilled in the art will appreciate that the system can also be implemented as a combination of hardware and software elements.

[0022] According to various embodiments, a “circuit” may be understood as any kind of a logic implementing entity, which may be special purpose circuitry or a processor executing software stored in a memory, firmware, or any combination thereof. Thus, in an embodiment, a “circuit” may be a hard-wired logic circuit or a programmable logic circuit such as a programmable processor, e.g. a microprocessor (e.g. a Complex Instruction Set Computer (CISC) processor or a Reduced Instruction Set Computer (RISC) processor). A “circuit” may also be a processor executing software, e.g. any kind of computer program, e.g. a computer program using a virtual machine code such as e.g. Java. Any other kind of implementation of the respective functions which may be described in more detail herein may also be understood as a “circuit” in accordance with an alternative embodiment.

[0023] Figure 1 shows a flowchart 100 illustrating a method for determining authenticity of an official document according to an embodiment.

[0024] At step 102, document image data and background image data of a single image of the official document is received. The official document may be, for example, an identity card as discussed in further details below with reference to Figure 2. Other non-limiting examples of a suitable official document include a passport, a driving license, a social security card, a certificate (birth certificate, marriage certificate, education certificate, etc.). Typically, the official document may be scanned or photographed, and provided as an image that includes both the document and the background. The background image data normally can be distinguished from the document image data.

[0025] At step 104, a first trained residual neural network is applied to extract global features of the official document from both the document image data and the background image data and to calculate a first score indicating normality of the official document and at least one second score indicating abnormality of the official document. As discussed in further details below, the global features

comprise features which are extracted by a global neural network classifier, which is pre-trained based on official document images with backgrounds. The at least one second score may comprise a score indicating the official document is not physically present (e.g. a screenshot or photocopy is being used).

[0026] At step 106, a second trained residual neural network is applied to extract local features of the official document from only the document image data and to calculate at least one third score indicating abnormality of the official document. As discussed in further details below, the local features comprise features which are extracted by a local neural network classifier, which is pre-trained based on official document images without backgrounds. The at least one third score may comprise a score indicating the official document has one or more irregular features. Examples of such irregular features include, but are not limited to, signs of tampering, or features which are occluded, missing, out of shape, out of position, etc.

[0027] At step 108, whether the official document is authentic is determined based on a comparison of the first score with the at least one second score and at least one third score. For example, the official document is determined to be authentic if the first score is greater than a maximum value from a set of the at least one second score and at least one third score. Conversely, the official document is determined to be not authentic if the first score is less than a maximum value from a set of the at least one second score and at least one third score.

[0028] In other words, a high first score is indicative of the official document being authentic. On the other hand, if any one of the other scores is high, the official document is considered not authentic.

[0029] Figure 2 shows a flowchart 200 illustrating a detailed example implementation of the method of Figure 1. In this example, the official document is an identity card (hereinafter interchangeably referred to as ID card), but it will be appreciated by a person skilled in the art that the method can be similarly applied to other types of official documents.

[0030] At step 202, an ID card image I1 which may be a photo taken by the user by using, for example, a camera-enabled cell phone, is provided. Typically, the user only needs one ID card image I1 taken at a single angle. If the ID card is placed on a table, for example, the ID card image I1 may include both the ID card and the

table surface as background. Alternatively, the ID card image I1 may be a scan obtained from a scanner in other embodiments. At step 204, the original ID card image I1 is provided to a global neural network (Net_Global) to recognize the fake ID cards, such as a screenshot or photocopy, by utilizing the ID card's global features.

[0031] In this example, the global neural network (Net_Global) is designed and trained to predict the probabilities of a normal/abnormal ID card. As a non-limiting example, the global neural network (Net_Global) contains 4 residual blocks. For each block, the network utilizes skip connections to jump triple layers and contains nonlinearities (ReLU) and batch normalization in between. Moreover, an additional weight matrix is used to learn the skip weight. This residual neural network is pre-trained with collected large-scale data including labelled ID card images with backgrounds. Some examples of the global features that may be recognized by the global neural network classifier include, but are not limited to, reflectivity of the card in the image, shape of the card in the image, and depth/thickness of the card.

[0032] To calculate the probabilities, a pre-processing step is adopted to normalize the original ID card image I1 from pixel values 0-255 to $(-1)-1$. When the original ID card image I1 is fed to the global neural network (Net_Global), the network is able to extract the ID card's global features and, at step 206, to predict the probabilities, including score1, score2 and score3 which correspond to a normal ID card, a screenshot ID card, and a photocopy ID card, respectively.

[0033] Additionally, a local neural network (Net_Local) is used to extract the local features from the ID card image I1 to recognize fake ID cards, such as a tampered ID card or an occluded ID card. The local neural network (Net_Local) also contains residual blocks and is designed to extract local features from ID card. This local residual neural network is pre-trained with collected large-scale data including labelled ID card images without backgrounds. Some examples of the local features that may be recognized by the local neural network classifier include, but are not limited to, positions of text fields, presence/absence of biometric data or face photo, and colour of card.

[0034] To obtain the local features, background subtraction is first performed on the card image I1. Here, the four corners C1, C2, C3, C4 of the ID card are detected at step 208, and only ID card portion I2 is detected by removing the background at step 210. The extracted ID card portion I2 only contains ID card information and is fed to the

local residual neural network (Net_Local), at step 212, to extract the local features. Then, at step 214, the local neural network (Net_Local) predicts the probabilities, including score4 and score5 corresponding to a tampered ID card and an occluded ID card, respectively.

[0035] In an example implementation, the scores (score1, score2, score3, score4 and score5) may be calculated using elements of the Convolutional Architecture for Fast Feature Embedding (CAFFE) framework. It will be appreciated that other deep learning frameworks may be used in alternate embodiments.

[0036] At step 216, a final score is calculated based on the following formula:

$$F(\text{score}) = \max(\text{score1}, \max(\text{score2}, \text{score3}, \text{score4}, \text{score5}))$$

[0037] In this example, if $\text{score1} > \max(\text{score2}, \text{score3}, \text{score4}, \text{score5})$, which means $F(\text{score}) = \text{score1}$, the ID card is determined to be authentic (i.e. a normal ID card). On the other hand, if $\text{score1} < \max(\text{score2}, \text{score3}, \text{score4}, \text{score5})$, which means $F(\text{score}) = \max(\text{score2}, \text{score3}, \text{score4}, \text{score5})$, the ID card is determined to be not authentic (i.e. an abnormal ID card). Furthermore, in the latter case, as an example, if $\max(\text{score2}, \text{score3}, \text{score4}, \text{score5}) = \text{score2}$, it is possible to determine that the ID card is a screenshot. Similarly, another category of fake ID card can be identified if the final score corresponds to the score of that category.

[0038] Figure 3 shows a schematic diagram of an apparatus 300 suitable for implementing the method of Figure 1. The apparatus 300 includes an input device 302 and a processing device 304. The input device 302 is configured to receive document image data and background image data of a single image of an official document. The processing device 304 is configured to feed the data to a first trained residual neural network 306 and a second trained residual neural network 308 respectively. The first trained residual neural network 306 comprises an algorithm to extract global features of the official document from both the document image data and the background image data and to calculate a first score 310 indicating normality of the official document and at least one second score 312 indicating abnormality of the official document. The second trained residual neural network 308 comprises an algorithm to extract local features of the official document from only the document image data and to calculate at least one third score 314, 316 indicating abnormality of the official document. The processing

device 304 is further configured to determine whether the official document is authentic based on a comparison of the first score 310 with the at least one second score 312 and at least one third score 314, 316.

[0039] In the above examples, the first and second residual neural networks are described as respective neural networks, and the global features are learned separately from the local features. However, it would be appreciated by a person skilled in the art that in alternate embodiments, the first and second residual neural networks may be implemented as respective branches of the same neural network capable of jointly learning the global and local features simultaneously.

[0040] Compared to conventional techniques which require the users to cooperate to take ID card images with multiple angles (hence the user experience is not pleasant and the EKYC process is not efficient), the method described in the present disclosure does not require the user to take multiple images. Rather, only one ID card image with normal angle is sufficient to extract global and local features at the same time. In other words, the present disclosure does not require affirmatively detecting specific features, such as security features or landmarks, which are sometimes physically obscure hence difficult to detect. Instead, several different scores, each indicative or representatively of an authenticity outcome, are simultaneously obtained and compared. Accordingly, the time taken to input and process the ID card image can be reduced, thereby improving user experience and overall efficiency. Furthermore, by using a combination of both global features and local features in the present disclosure, it is possible to both distinguish an ID card that is authentic from one that is not and recognize various types fake ID cards, such as screenshot ID card, photocopy ID card, tampered ID card, occluded ID card, etc. at high accuracy.

[0041] Figure 4 depicts an exemplary computing device 400, hereinafter interchangeably referred to as a computer system 400, where one or more such computing devices 400 may be used for apparatus 300. The following description of the computing device 400 is provided by way of example only and is not intended to be limiting.

[0042] 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.

[0043] 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 floppy disk drive, 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 floppy disk, 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.

[0044] In an alternative implementation, the secondary memory 410 may additionally or alternatively include other similar means for allowing computer programs or other instructions to be loaded into the computing device 400. Such means 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 program cartridge and cartridge interface (such as that found in video game console devices), 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.

[0045] 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 of the disclosure, 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.

[0046] As shown in Figure 4, 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.

[0047] 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.

[0048] 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.

[0049] 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.

[0050] 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.

[0051] It will be appreciated that the elements illustrated in Figure 4 function to provide means for performing the various functions and operations of the servers as described in the above embodiments.

[0052] In an implementation, a server may be generally described as a physical device comprising at least one processor and at least one memory including computer program code. The at least one memory and the computer program code are configured to, with the at least one processor, cause the physical device to perform the requisite operations.

[0053] It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present disclosure as shown in the specific embodiments without departing from the scope of the disclosure as broadly described. For example, the structure of the residual neural networks may be adapted or optimised based on performance. The number of scores may be varied based on the attributes of the official document that may be faked. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

CLAIMS

1. A method for determining authenticity of an official document, the method comprising:

receiving document image data and background image data of a single image of the official document;

applying a first trained residual neural network to extract global features of the official document from both the document image data and the background image data and to calculate a first score indicating normality of the official document and at least one second score indicating abnormality of the official document;

applying a second trained residual neural network to extract local features of the official document from only the document image data and to calculate at least one third score indicating abnormality of the official document; and

determining whether the official document is authentic based on a comparison of the first score with the at least one second score and at least one third score.

2. The method as claimed in claim 1, wherein the official document is determined to be authentic if the first score is greater than a maximum value from a set of the at least one second score and at least one third score.

3. The method as claimed in claim 1, wherein the official document is determined to be not authentic if the first score is less than a maximum value from a set of the at least one second score and at least one third score.

4. The method as claimed in any one of the preceding claims, wherein the official document comprises an identity card.

5. The method as claimed in any one of the preceding claims, wherein the at least one second score comprises a score indicating the official document is not physically present.

6. The method as claimed in any one of the preceding claims, wherein the at least one third score comprises a score indicating the official document has one or more irregular features.

7. The method as claimed in any one of the preceding claims, wherein the first residual neural network is trained based on a plurality of labelled official document images with backgrounds.
8. The method as claimed in any one of the preceding claims, wherein the second residual neural network is trained based on a plurality of labelled official document images without backgrounds.
9. The method as claimed in any one of the preceding claims, wherein the first and second trained residual neural networks comprise respective branches of the same neural network.
10. A system for determining authenticity of an official document, comprising:
 - a processor; and
 - a computer-readable memory coupled to the processor and having instructions stored thereon that are executable by the processor to:
 - identify document image data and background image data of a single image of the official document;
 - apply a first trained residual neural network to extract global features of the official document from both the document image data and the background image data and to calculate a first score indicating normality of the official document and at least one second score indicating abnormality of the official document;
 - apply a second trained residual neural network to extract local features of the official document from only the document image data and to calculate at least one third score indicating abnormality of the official document; and
 - determine whether the official document is authentic based on a comparison of the first score with the at least one second score and at least one third score.
11. The system as claimed in claim 10, wherein the instructions are executable by the processor to determine the official document to be authentic if the first score is greater than a maximum value from a set of the at least one second score and at least one third score.

12. The system as claimed in claim 10, wherein instructions are executable by the processor to determine the official document to be not authentic if the first score is less than a maximum value from a set of the at least one second score and at least one third score.

13. The system as claimed in any one of claims 10 to 12, wherein the official document comprises an identity card.

14. The system as claimed in any one claims 10 to 13, wherein the at least one second score comprises a score indicating the official document is not physically present.

15. The system as claimed in any one of claims 10 to 14, wherein the at least one third score comprises a score indicating the official document has one or more irregular features.

16. The system as claimed in any one of claims 10 to 15, wherein the first residual neural network comprises one trained based on a plurality of labelled official document images with backgrounds.

17. The system as claimed in any one of claims 10 to 16, wherein the second residual neural network comprises one trained based on a plurality of labelled official document images without backgrounds.

18. The system as claimed in any one of claims 10 to 17, wherein the first and second trained residual neural networks comprise respective branches of the same neural network.

19. An apparatus comprising:

an input device configured to receive document image data and background image data of a single image of an official document; and

a processing device configured to feed the data to a first trained residual neural network and a second trained residual neural network respectively,

wherein the first trained residual neural network comprises an algorithm to extract global features of the official document from both the document image data and the background image data and to calculate a first score indicating normality of

the official document and at least one second score indicating abnormality of the official document;

wherein the second trained residual neural network comprises an algorithm to extract local features of the official document from only the document image data and to calculate at least one third score indicating abnormality of the official document; and

wherein the processing device is further configured to determine whether the official document is authentic based on a comparison of the first score with the at least one second score and at least one third score.

20. The apparatus as claimed in claim 19, wherein the first and second trained residual neural networks comprise respective branches of the same neural network.