

AUTHENTICATION SYSTEM AND METHOD

FIELD OF INVENTION

[001] The present invention relates broadly, but not exclusively, to authentication systems and methods.

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 clients and to assess potential risks of illegal intentions towards the business relationship (e.g. money laundering). Many eKYC processes involve potential clients submitting photographs of themselves (specifically their faces) and of their official identification (ID) documents, e.g. ID card, passport etc.

[003] Fraudsters are a serious problem for eKYC processes. Currently, there are a number of methods to detect fraudsters. However, these known methods focus on an analysis of same characteristics in the submitted photographs of potential clients and/or of their official ID documents, including identical face images, identical ID documents, identical name in the ID document, etc.

[004] However, another type of fraudster attack, known as “Human Flesh Fraudster Attack”, has recently risen and cannot be detected by such known methods. This is because during such attacks, fraudsters use rewards like daily necessities to attract and organize people, most of whom are less educated and do not know or care about personal privacy. The fraudsters get these unknowing people to use their true official ID documents and faces to complete the eKYC process.

[005] To attract new bona fide clients, business entities or service providers may offer benefits for completing a eKYC process. However, any rewards are enjoyed by the fraudsters, and the accounts created after the eKYC process is completed become zombie accounts and make no contribution to the revenue of the business entities or service providers.

SUMMARY

[006] Many eKYC processes involve potential clients submitting photographs of themselves (specifically their faces) and of their official identification (ID) documents, e.g. ID card, passport etc. A type of fraudster attack, known as “Human Flesh Fraudster Attack” involves victims using their true official ID documents and faces to complete a eKYC process with little or no benefit for themselves.

[007] According to one embodiment, to detect “Human Flesh Fraudster Attacks”, an authentication method is proposed which involves using a similarity of backgrounds in users’ photographs (specifically their faces) and in photographs of their official identification (ID) documents to detect groups with similar background. In most “Human Flesh Fraudster Attack” cases, victims are organized and gathered at the same place to complete the fraudulent eKYC process, so the background in their face photographs and/or in photographs of their official identification (ID) documents may be similar.

[008] According to another embodiment, there is provided an authentication system, including a background image extraction device configured to: extract first background images from each of a plurality of human face photographs submitted by users for a particular digital due diligence process; and extract second background images from each of a plurality of identification document photographs submitted by users for the particular digital due diligence process. The system also includes a processing device configured to: generate a background vector for each of the extracted first background images and the extracted second background images using a trained image similarity model, wherein the trained image similarity model is trained with historical background images; detect a presence of similar backgrounds from the generated background vectors; and trigger an authentication alarm signal if the presence of similar backgrounds is detected.

[009] According to another embodiment, there is provided a computer-implemented method for authentication, including the following steps: (a) extracting, using a background image extraction device, first background images from each of a plurality of human face photographs submitted by users for a particular digital due diligence process; (b) extracting, using the background image extraction device, second background images from each of a plurality of identification document photographs submitted by users for the particular digital due diligence process; (c) generating, using a processing device, a background vector for each of the extracted first background

images and the extracted second background images using a trained image similarity model, wherein the trained image similarity model is trained with historical background images; (d) detecting, using the processing device, a presence of similar backgrounds from the generated background vectors; and (e) triggering, using the processing device, an authentication alarm signal if the presence of similar backgrounds is detected.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] 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:

[0011] Figure 1A is a flow chart illustrating a method for authentication, according to an embodiment.

[0012] Figure 1B shows an example of a “selfie” image previously submitted by a user.

[0013] Figure 1C shows an example of a “selfie” image in which the detected human face is removed such that only the background image remains, according to an embodiment.

[0014] Figure 1D is an example photograph of an identification document.

[0015] Figure 1E is an example photograph of an identification document with the actual identification document removed, according to an embodiment.

[0016] Figure 2 is a schematic of an authentication system, according to an embodiment.

[0017] Figure 3 is a flow chart illustrating a computer-implemented method for authentication, according to an embodiment.

[0018] Figure 4 shows a schematic diagram of a computer system suitable for use in executing at least some steps of the method for authentication.

DETAILED DESCRIPTION

[0019] 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.

[0020] 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.

[0021] 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.

[0022] 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.

[0023] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the invention.

[0024] 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.

[0025] 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 clients and to assess potential risks of illegal intentions towards the business relationship (e.g. money laundering). Many eKYC processes involve potential clients submitting photographs of themselves (specifically their faces) and of their official identification (ID) documents, e.g. ID card, passport etc.

[0026] A type of fraudster attack, known as “Human Flesh Fraudster Attack” involves victims using their true official ID documents and faces to complete a eKYC process with little or no benefit for themselves.

[0027] 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. Authentication can be implemented remotely using a remote authentication server, as embodied by

authentication system 200 that is described in detailed below. Remote authentication allows fraud detection to be performed centrally (typically requiring less resources) and away from user terminals over unsecure communication channels.

[0028] According to one embodiment, to detect “Human Flesh Fraudster Attacks”, an authentication method involves using similarity of backgrounds in users’ photographs (specifically their faces) and/or in photographs of their official identification (ID) documents to detect groups with similar background. In most “Human Flesh Fraudster Attack” cases, victims are organized and gathered at the same place to complete the fraudulent eKYC process, so the background in their face photographs and/or photographs of their official identification (ID) documents may be similar. Similar background data can be automatically generated from historical data, without manual input/human effort. By applying face detection and ID alignment models to remove face images and ID document images, respectively, only the background is considered.

[0029] This is in stark contrast to some known methods to detect “Human Flesh Fraudster Attacks”, which either (i) focus on a similarity of entire users’ photographs (i.e. their faces and background) and the entire ID documents (i.e. face image printed on the ID document and other text (e.g. ID number, name, date of birth, etc.)) or (ii) use geographical information to detect repetitions, suggesting a presence of fraudulence. With regard to (i), the similarity of entire users’ photographs and entire ID documents is easily influenced by the person and image of the ID documents, which affects reliability of detecting fraud. With regard to (ii), it is relatively easy to provide false geographical information, which also affects the reliability of detecting fraud.

[0030] The techniques described in this specification produce one or more technical effects. In particular, by focusing on the similarity of backgrounds in (i) human face photographs submitted by users for a particular digital due diligence process and/or (ii) identification document photographs that are submitted by users for the same particular digital due diligence process, it is possible to ignore the influence of faces and actual identification documents. This results in more reliable and robust fraud detection and authentication. Furthermore, the similarity of backgrounds in (i) human face photographs and (ii) identification document photographs is more reliable than geographical information, especially for “Human Flesh Fraudster Attacks”. The similarity of backgrounds can help to detect victims that have been exploited by fraudsters, especially when the victims use their true identification documents and actual photographs of themselves.

[0031] Figure 1A is a flow chart 100 illustrating a method for authentication, according to an embodiment.

[0032] The method involves a phase for building a similar background data set for both (i) human face photographs submitted by users for a particular digital due diligence process and (ii) identification document photographs that are submitted by users for the same particular digital due diligence process. The phase for building a similar background data set includes steps 102, 104, 106 and 108. Steps 106 and 108 can be performed before steps 102 and 104.

[0033] At step 102, multiple human face photographs (e.g. “selfie” images) previously submitted by users for a particular digital due diligence process are collected. At step 104, a face detection model is used to detect a human face from each of the plurality of human face photographs previously submitted by users. Thereafter, the detected human face is removed from each photograph such that the background image remains.

[0034] Figure 1B shows an example of a “selfie” image previously submitted by a user. A face detection model is used to detect a human face and thereafter the detected human face is removed from each photograph such that only the background image remains, as shown in Figure 1C.

[0035] At step 106, multiple identification (ID) document photographs that were previously submitted by users for the same particular digital due diligence process are collected. Some ID documents are printed on both the front and back side. In such cases, photographs of both the front and back side of the ID document are collected.

[0036] At step 108, an ID alignment model is used to detect an actual identification document in a digital image of an identification document. The ID alignment model provides a method to detect and align identification documents in digital images. In most cases, a photograph of an identification document includes an image of the actual identification document and a background (e.g. table on which the identification document was placed when the photograph was taken, or image of a person holding up the identification document as shown in Figure 1D). Once the actual identification document is detected in the photograph of the identification document using the ID alignment model, the image of the actual identification document is removed, leaving

behind the background of the photograph of the identification document as shown in Figure 1E.

[0037] After the phase for building a similar background data set (steps 102, 104, 106 and 108) is completed, the extracted background images from each of the plurality of human face photographs and identification document photographs are used to train an image similarity model separately at step 110. In other words, the extracted background images from each of the plurality of human face photographs are used to train the image similarity model. Separately, during another training process, the extracted background images from each of the plurality of identification document photographs are used to train the image similarity model.

[0038] A neural network can comprise a “backbone” portion and a “head” portion. The “backbone” portion is to generate a vector for a given image while the “head” portion is to calculate loss for the training process. Accordingly, the image similarity model can be trained using different model architectures - the backbone portion can be ResNet, IR_SE, etc., while the head portion can be softmax, triplet loss, arcFace, etc.

[0039] The method for further involves an authentication phase, which includes steps 112, 114 and 116.

[0040] At step 112, a series of new data associated with the particular digital due diligence process is received. Similar to step 104 for preparing the training data, a face detection model is used to detect a human face from each of the plurality of human face photographs newly submitted by users. Thereafter, the detected human face is removed from each photograph such that the background image remains. Concurrently or sequentially, similar to step 108 for preparing the training data, an ID alignment model is used to detect an actual identification document in digital images of identification documents newly submitted by users. The ID alignment model provides a method to detect and align identification documents in digital images. Once the actual identification document is detected, the image of the actual identification document is removed, leaving behind the background of the photograph of the identification document.

[0041] At step 114, using the trained image similarity model (i.e. trained at step 110), background vectors are generated for each of the extracted backgrounds from the human face photographs and identification document photographs.

[0042] At step 116, a cluster algorithm (e.g. DBSCAN, K-means, spectral clustering) is used to detect similar background groups. The presence of similar background groups suggests that a “Human Flesh Fraudster Attack” has occurred.

[0043] At step 118, (i) the newly extracted background data from the human face photographs and identification document photographs [from step 112] and (ii) the similarity results [obtained from step 116] are both added to the historical data to enrich the historical dataset.

[0044] Figure 2 is a schematic of an authentication system 200, according to an embodiment. The system 200 includes a background image extraction device 202 and a processing device 204.

[0045] The background image extraction device 202 extracts first background images from each of a plurality of human face photographs submitted by users for a particular digital due diligence process. For example, Figure 1C shows a human face photograph with only the background image remaining. The corresponding background image data is extracted by the background image extraction device 202.

[0046] Concurrently or sequentially, the background image extraction device 202 also extracts second background images from each of a plurality of identification document photographs submitted by users for the particular digital due diligence process. For example, Figure 1E shows an identification document photograph with only the background image remaining. The corresponding background image data is extracted by the background image extraction device 202.

[0047] The processing device 204 generates a background vector for each of the extracted first background images and the extracted second background images using a trained image similarity model. The trained image similarity model is trained with historical background images.

[0048] The processing device 204 detects a presence of similar backgrounds from the generated background vectors. In an implementation, the processing device 204

detects the presence of similar backgrounds from the generated background vectors using a cluster algorithm. The cluster algorithm may be DBSCAN, K-means or spectral clustering. The processing device 204 triggers an authentication alarm signal if the presence of similar backgrounds is detected.

[0049] The above-mentioned historical background images include first historical background images and second historical background images. The background image extraction device 202 can also extract the first historical background images from each of a plurality of human face photographs previously submitted by users for the particular digital due diligence process. The background image extraction device 202 can also extract the second historical background images from each of a plurality of identification document photographs previously submitted by users for the particular digital due diligence process. The first historical background images, second historical background images, first background images and/or the extracted second background images can be stored in a memory device 206.

[0050] The trained image similarity model can be trained separately with (i) the first historical background images and (ii) the second historical background images. The first historical background images and the second historical background images may have different distribution. Accordingly, better performance of the trained model can be expected by training the image similarity model separately.

[0051] The background image extraction device 202 can use a face detection model to detect a human face in each of the plurality of human face photographs submitted by users for the particular digital due diligence process. The background image extraction device 202 removes the detected human face from each of the plurality of human face photographs such that the background image remains in each of the plurality of human face photographs. This is shown, for example, in Figure 1C.

[0052] The background image extraction device 202 can use an identification document alignment model to detect an identification document in each of the plurality of identification document photographs submitted by users for the particular digital due diligence process. The background image extraction device 202 removes the detected identification document from each of the plurality of identification document photographs such that the background image remains in each of the plurality of identification document photographs. This is shown, for example, in Figure 1E.

[0053] A neural network can comprise a “backbone” portion and a “head” portion. Accordingly, the image similarity model can be trained using different model architectures - the backbone can be ResNet, IR_SE, etc., while the head can be softmax, triplet loss, arcFace, etc.

[0054] The processing device can add the extracted first background images and the extracted second background images to a collection of the first historical background images and a collection of the second historical background images, respectively. As a result, the collection of the first historical background images and the collection of the second historical background images are enriched to increase the accuracy of fraud detection and authentication. In addition or alternatively, the processing device can add the generated background vectors to a collection of historical background vectors. As a result, the collection of historical background vectors is enriched to increase the accuracy of fraud detection and authentication.

[0055] Figure 3 is a flow chart illustrating a computer-implemented method 300 for authentication, according to an embodiment. The method 300 includes the step 302 of extracting, using a background image extraction device, first background images from each of a plurality of human face photographs submitted by users for a particular digital due diligence process. The method 300 further includes the step 304 of extracting, using the background image extraction device, second background images from each of a plurality of identification document photographs submitted by users for the particular digital due diligence process. The method 300 further includes the step 306 of generating, using a processing device, a background vector for each of the extracted first background images and the extracted second background images using a trained image similarity model. The trained image similarity model is trained with historical background images.

[0056] The method 300 further includes the step 308 of detecting, using the processing device, a presence of similar backgrounds from the generated background vectors. The method 300 further includes the step 310 of triggering, using the processing device, an authentication alarm signal if the presence of similar backgrounds is detected.

[0057] The method 300 may further include the steps of (i) extracting, using the background image extraction device, first historical background images from each of a

plurality of human face photographs previously submitted by users for the particular digital due diligence process; and (ii) extracting, using the background image extraction device, second historical background images from each of a plurality of identification document photographs previously submitted by users for the particular digital due diligence process. The historical background images include the first historical background images and the second historical background images.

[0058] The method 300 may further include the step of training the image similarity model separately with (i) the first historical background images and (ii) the second historical background images.

[0059] The method 300 may further include the steps of (i) using a face detection model to detect a human face in each of the plurality of human face photographs submitted by users for the particular digital due diligence process; and (ii) removing the detected human face from each of the plurality of human face photographs such that the background image remains in each of the plurality of human face photographs.

[0060] The method 300 may further include the steps of (i) using an identification document alignment model to detect an identification document in each of the plurality of identification document photographs submitted by users for the particular digital due diligence process; and (ii) removing the detected identification document from each of the plurality of identification document photographs such that the background image remains in each of the plurality of identification document photographs.

[0061] A cluster algorithm (e.g. DBSCAN, K-means or spectral clustering) may be used to detect the presence of similar backgrounds from the generated background vectors.

[0062] The image similarity model can be trained using one of the following artificial neural network (ANN) architectures: (a) residual neural network (ResNet) or IR_SE for a backbone portion of the ANN; and (b) softmax, triplet loss or arcFace for a head portion of the ANN.

[0063] The method 300 may further include the steps of (i) adding the extracted first background images and the extracted second background images to a collection of the first historical background images and a collection of the second historical background images, respectively; and (ii) adding the generated background vectors to a collection of historical background vectors.

[0064] Figure 4 shows a schematic diagram of a computer system suitable for use in executing at least some steps of the method for authentication.

[0065] The following description of the computer system / computing device 400 is provided by way of example only and is not intended to be limiting.

[0066] 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.

[0067] 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.

[0068] 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.

[0069] 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.

[0070] 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.

[0071] 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.

[0072] 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.

[0073] 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.

[0074] 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.

[0075] 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.

[0076] 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 system, comprising:
 - a background image extraction device configured to:
 - extract first background images from each of a plurality of human face photographs submitted by users for a particular digital due diligence process;
 - and
 - extract second background images from each of a plurality of identification document photographs submitted by users for the particular digital due diligence process; and
 - a processing device configured to:
 - generate a background vector for each of the extracted first background images and the extracted second background images using a trained image similarity model, wherein the trained image similarity model is trained with historical background images;
 - detect a presence of similar backgrounds from the generated background vectors; and
 - trigger an authentication alarm signal if the presence of similar backgrounds is detected.
2. The system as claimed in claim 1, wherein:
 - the background image extraction device is further configured to:
 - extract first historical background images from each of a plurality of human face photographs previously submitted by users for the particular digital due diligence process; and
 - extract second historical background images from each of a plurality of identification document photographs previously submitted by users for the particular digital due diligence process,
 - wherein the historical background images comprises the first historical background images and the second historical background images.
3. The system as claimed in claim 2, wherein:
 - wherein the trained image similarity model is trained separately with (i) the first historical background images and (ii) the second historical background images.
4. The system as claimed in claim 2, wherein the background image extraction

device is further configured to:

- use a face detection model to detect a human face in each of the plurality of human face photographs submitted by users for the particular digital due diligence process; and

- remove the detected human face from each of the plurality of human face photographs such that the background image remains in each of the plurality of human face photographs.

5. The system as claimed in claim 2, wherein the background image extraction device is further configured to:

- use an identification document alignment model to detect an identification document in each of the plurality of identification document photographs submitted by users for the particular digital due diligence process; and

- remove the detected identification document from each of the plurality of identification document photographs such that the background image remains in each of the plurality of identification document photographs.

6. The system as claimed in claim 1, wherein the processing device is further configured to detect the presence of similar backgrounds from the generated background vectors using a cluster algorithm.

7. The system as claimed in claim 6, wherein the cluster algorithm comprises: DBSCAN, K-means or spectral clustering.

8. The system as claimed in claim 1, wherein the trained image similarity model is trained using one of the following artificial neural network (ANN) architectures:

- residual neural network (ResNet) or IR_SE for a backbone portion of the ANN;
- and

- softmax, triplet loss or arcFace for a head portion of the ANN.

9. The system as claimed in claim 2, wherein the processing device is further configured to:

- add the extracted first background images and the extracted second background images to a collection of the first historical background images and a collection of the second historical background images, respectively; and

- add the generated background vectors to a collection of historical

background vectors.

10. A computer-implemented method for authentication, comprising:
 - extracting, using a background image extraction device, first background images from each of a plurality of human face photographs submitted by users for a particular digital due diligence process;
 - extracting, using the background image extraction device, second background images from each of a plurality of identification document photographs submitted by users for the particular digital due diligence process;
 - generating, using a processing device, a background vector for each of the extracted first background images and the extracted second background images using a trained image similarity model, wherein the trained image similarity model is trained with historical background images;
 - detecting, using the processing device, a presence of similar backgrounds from the generated background vectors; and
 - triggering, using the processing device, an authentication alarm signal if the presence of similar backgrounds is detected.
11. The method as claimed in claim 10, further comprising:
 - extracting, using the background image extraction device, first historical background images from each of a plurality of human face photographs previously submitted by users for the particular digital due diligence process; and
 - extracting, using the background image extraction device, second historical background images from each of a plurality of identification document photographs previously submitted by users for the particular digital due diligence process,
 - wherein the historical background images comprises the first historical background images and the second historical background images.
12. The method as claimed in claim 11, further comprising:
 - training the image similarity model separately with (i) the first historical background images and (ii) the second historical background images.
13. The method as claimed in claim 11, further comprising:
 - using a face detection model to detect a human face in each of the plurality of human face photographs submitted by users for the particular digital due diligence process; and

removing the detected human face from each of the plurality of human face photographs such that the background image remains in each of the plurality of human face photographs.

14. The method as claimed in claim 11, further comprising:

using an identification document alignment model to detect an identification document in each of the plurality of identification document photographs submitted by users for the particular digital due diligence process; and

removing the detected identification document from each of the plurality of identification document photographs such that the background image remains in each of the plurality of identification document photographs.

15. The method as claimed in claim 10, further comprising:

detecting the presence of similar backgrounds from the generated background vectors using a cluster algorithm.

16. The method as claimed in claim 15, wherein the cluster algorithm comprises: DBSCAN, K-means or spectral clustering.

17. The method as claimed in claim 10, further comprising:

training the image similarity model using one of the following artificial neural network (ANN) architectures:

residual neural network (ResNet) or IR_SE for a backbone portion of the ANN;
and

softmax, triplet loss or arcFace for a head portion of the ANN.

18. The method as claimed in claim 11, further comprising:

adding the extracted first background images and the extracted second background images to a collection of the first historical background images and a collection of the second historical background images, respectively; and

adding the generated background vectors to a collection of historical background vectors.