A USER AUTHENTICATION METHOD AND SYSTEM

TECHNICAL FIELD

[001] The present specification relates broadly, but not exclusively, to a user authentication method and to a user authentication system.

BACKGROUND

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

[003] In a typical eKYC process, a customer is required to first take a photograph of his/her ID document, followed by taking a photograph of his/her face (i.e. a "selfie"). Face anti-spoofing methods are then implemented to prevent false facial verification whereby attackers use a photograph, video, or other substitutes for a person's face.

[004] Current face anti-spoofing technologies are effective for detecting screenshot, paper printing and video replay. However, some attacks use very similar face images from an initial enrollment process to attack a subsequent verification process. It is relatively easy for attackers to obtain face images from enrollment processes. For example, if the users enroll their face images using that from their ID cards, the attacker can print the face images of the ID cards in high resolution to attack the verification process.

[005] A need therefore exists to improve the manner in which a user can be authenticated.

SUMMARY

[006] Embodiments seek to provide a user authentication method which involves a combination of different authentication methods such as computing face similarity, background similarly and moiré pattern.

[007] According to one embodiment, there is provided a user authentication method, comprising: extracting, from a user enrollment image comprising a first human face image and a first background image, the first human face image and the first background image; extracting, from a user authentication image comprising a second human face image and a second background image, the second human face image and the second background image; generating, using trained image spoof model, a first score (S1) associated with the user authentication image; generating a second score (S2) corresponding to a similarity between the first background image and the second background image; generating a third score (S3) corresponding to a similarity between the first human face image and the second human face image; and authenticating the user based on the first score (S1), the second score (S2) and the third score (S3).

[008] According to another embodiment, there is provided a user authentication system, comprising: an extracting device configured to: extract, from a user enrollment image comprising a first human face image and a first background image, the first human face image and the first background image; and extract, from a user authentication image comprising a second human face image and a second background image, the second human face image and the second background image; a first score generating device configured to generate, using a trained image spoof model, a first score (S1) associated with the user authentication image; a second score generating device configured to generate a second score (S2) corresponding to a similarity between the first background image and the second background image; a third score generating device configured to generate a third score (S3) corresponding to a similarity between the first human face image and the second human face image; and an authenticating device configured to authenticate the user based on the first score (S1), the second score (S2) and the third score (S3).

BRIEF DESCRIPTION OF THE DRAWINGS

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

[0010] Figure 1 is a flow chart illustrating an example of a user authentication method, according to an embodiment.

[0011] Figure 2 shows an example of a face photograph submitted by a user.

[0012] Figure 3 shows a schematic diagram of a computer system suitable for use in executing at least some steps of the user authentication method.

[0013] Figure 4 is a schematic diagram illustrating an example of a user authentication system, according to an embodiment.

DETAILED DESCRIPTION

[0014] Embodiments will be described, by way of example only, with reference to the drawings. Like reference numerals and characters in the drawings refer to like elements or equivalents.

[0015] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0016] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “receiving”, “scanning”, “calculating”, “determining”, “replacing”, “generating”,

“initializing”, “outputting”, or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0017] The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes, or may comprise a computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer suitable for executing the various methods / processes described herein will appear from the description below.

[0018] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the 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.

[0019] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM mobile telephone system. The

computer program when loaded and executed on such a computer effectively results in an apparatus that implements the steps of the preferred method.

[0020] electronic-Know Your Customer (eKYC) is a digital due diligence process performed by a business entity or service provider to verify the identity of its customers to prevent falsification of identity. Authentication can be considered as a form of fraud detection in which legitimacy of users are verified and potential fraudsters may be detected before fraudulent acts are carried out. Effective authentication can enhance data security of systems so that digital data is protected from unauthorized users.

[0021] In a typical eKYC process, a customer is required to first take a photograph of his/her ID document, followed by taking a photograph of his/her face (i.e. a “selfie”). Face anti-spoofing methods are then implemented to prevent false facial verification whereby attackers use a photograph, video, or other substitutes for a person’s face.

[0022] Current face anti-spoofing technologies are effective for detecting screenshot, paper printing and video replay. However, some attacks use very similar face images from an initial enrollment process to attack a subsequent verification process. The current face anti-spoofing methods are generally focused on identifying moiré pattern or face similarity and may not be able to fully utilize available information such as background similarity. Verifying background similarity of images may be useful in detecting attacks which use similar face images from the initial enrollment process.

[0023] According to one embodiment, in order to reduce the success rate of attacks that use very similar face images from the initial enrollment process, a user authentication method which involves authenticating a user’s identity through a combination of different authentication methods may be implemented. The different authentication methods may include computing face similarity, background similarly and moiré pattern.

[0024] Embodiments described in the present specification may involve an eKYC process that includes two general processes: a user enrollment process and a user authentication process. In the user enrollment process, a user may take a photograph of his/her ID document or take a selfie photograph for submission as a user enrollment image. In the user authentication process, the same user may take a selfie photograph for submission as a user authentication image if he/she has submitted the photograph of his/her ID document as user enrollment image. In some implementations, the same

user may take another selfie photograph for submission as a user authentication image if he/she has submitted a selfie photograph as user enrollment image.

[0025] As mentioned above, current face anti-spoofing methods may not be able to fully utilize available information such as background similarity. The techniques described in the present specification produce one or more technical effects. In particular, by computing the similarity between background images of the user enrollment image and the user authentication image, the user authentication method and system may reduce the success rate of attacks to the eKYC process, and may be especially effective identifying attacks that use very similar face images from enrollment processes. If the background images of the user enrollment image and the user authentication image are determined to be similar, the user authentication image can be identified as an attack.

[0026] Further, the user authentication method and system may provide higher accuracy in detecting attacks by authenticating users using various modes such as comparing face similarities, comparing background similarities and detecting moiré patterns of the submitted photographs for the eKYC processes.

[0027] Figure 1 is a flow chart 100 illustrating an example of a user authentication method, according to an embodiment. At step 102, the first human face image and the first background image are extracted from a user enrollment image comprising a first human face image and a first background image. At step 104, the second human face image and the second background image are extracted from a user authentication image comprising a second human face image and a second background image. At step 106, a first score (S1) associated with the user authentication image is generated using a trained image spoof model. At step 108, a second score (S2) corresponding to a similarity between the first background image and the second background image is generated. At step 110, a third score (S3) corresponding to a similarity between the first human face image and the second human face image is generated. At step 112, the user is authenticated based on the first score (S1), the second score (S2) and the third score (S3).

[0028] According to an embodiment, the user may be positively authenticated on a condition that S1 is lower than a first threshold; S2 is lower than a second threshold and S3 is greater than a third threshold. The generated scores S1, S2 and S3 may be computed with a mathematical function. The user authentication image can be

determined to be an authentic image if the mentioned conditions are met. Otherwise, the user authentication image can be determined to be an attack image.

[0029] The first threshold, the second threshold and the third threshold may be separately determined based on a receiver operating characteristic (ROC) curve. As a non-limiting example, the third threshold is set as 68. At this point of the ROC curve, the false accept rate is 1E-4 while the true accept rate is 99%.

[0030] The user enrollment image may be obtained during an initial user enrollment process and the user authentication image may be obtained during a subsequent user authentication process. The user enrollment image may comprise a face photograph of the user or a photograph of the user's identification document that is taken during the initial user enrollment process. The user authentication image may comprise another face photograph of the user or another photograph of the user's identification document that is taken during the subsequent user authentication process.

[0031] Figure 2 shows an example of a face photograph 200 submitted by a user. The face photograph 200 may be a selfie photograph taken by the user for submission during the user enrollment process or user authentication process.

[0032] The step of extracting the first human face image 202 and the first background image 204 from the user enrollment image may comprise applying a face detection method to the user enrollment image to generate a face bounding box 206 that demarcates the first human face image 202 such that an area of the user enrollment image within the face bounding box 206 corresponds to the first human face image 202 and an area of the user enrollment image outside the face bounding box 206 corresponds to the first background image 204. In other words, the first human face image 202 can be obtained by cropping the area demarcated by the face bounding box 206. To obtain the first background image 204, the first human face image 202 may then be removed such that only the first background image 204 remains.

[0033] The step of extracting the second human face image 202 and the second background image 204 from the user authentication image may comprise applying the face detection method to the user authentication image to generate another face bounding box 206 that demarcates the second human face image 202 such that an area of the user authentication image within the other face bounding box 206 corresponds to the second human face image 202 and an area of the user authentication image outside the other face bounding box 206 corresponds to the

second background image 204. In other implementations, a face detection method different from that used in the step of extracting the first human face image 202 and the first background image 204 from the user enrollment image, may be used. The second human face image 202 can be obtained by cropping the area demarcated by the face bounding box 206. To obtain the second background image 204, the second human face image 202 may then be removed such that only the second background image 204 remains.

[0034] According to an embodiment, the step of generating the second score (S2) may comprise a pixel-wise comparison between the first background image and the second background image to determine the similarity between the first background image and the second background image. Image subtraction or pixel subtraction processes can be used to subtract digital numeric values of the second background image from the first background image to determine similarity between the two images. An absolute value can be obtained from the subtraction because each background image is an integer value in the range of 0 to 255. The similarity between the first background image and the second background image can be determined by comparing the absolute value obtained from the subtraction of the images, with a predefined threshold value.

[0035] As mentioned above and with reference to Figure 1, at step 106, a first score (S1) associated with the user authentication image is generated using a trained image spoof model. The user authentication method may further comprise training the image spoof model using a CNN with a softmax function. To conduct face anti-spoofing, the user authentication image may be transmitted to the trained image spoof model to generate the first score (S1). The first score (S1) may then be compared with the predetermined first threshold value. The user authentication image can be determined to be an attack image if the first score (S1) is greater than the predetermined first threshold value. The trained image spoof model may be a convolutional neural network (CNN) based binary classifier, which may be trained using a large dataset of live face images and spoof images to determine if an image transmitted to it is a live image or a spoof image. In other implementations, the first score (S1) may be generated using a CNN based multi-class classifier.

[0036] The step of generating the third score (S3) may comprise extracting first features (F1) corresponding to the first human face image using a trained CNN, extracting second features (F2) corresponding to the second human face image using

the trained CNN, and generating the third score (S3) based on a cosine similarity between the first features (F1) and the second features (F2). The trained CNN may be a trained image similarity model that has been trained with historical images to perform face verification tasks. The first features (F1) and the second features (F2) may be extracted separately and compared to generate the third score (S3) based on the similarity between first features (F1) and second features (F2). In some implementations, first features (F1) and second features (F2) may be feature vectors with 256 dimensions and cosine similarity may be used to measure the similarity between first features (F1) and second features (F2), generating a value range between -1 and 1.

[0037] Other implementations of the user authentication method may include using face parsing method to identify human face images from the user enrollment image and user authentication image, and obtain the human face images with possibly high accuracy. The human face images can then be removed from the user enrollment image and user authentication image to obtain the respective background images. The implementations may further include generating face bounding boxes for each of the user enrollment image and user authentication image in order to extract the respective background images.

[0038] Figure 3 shows a schematic diagram of a computer system suitable for use in executing at least some steps of the user authentication method.

[0039] The following description of the computer system / computing device 300 is provided by way of example only and is not intended to be limiting.

[0040] As shown in Figure 3, the example computing device 300 includes a processor 304 for executing software routines. Although a single processor is shown for the sake of clarity, the computing device 300 may also include a multi-processor system. The processor 304 is connected to a communication infrastructure 306 for communication with other components of the computing device 300. The communication infrastructure 306 may include, for example, a communications bus, cross-bar, or network.

[0041] The computing device 300 further includes a main memory 308, such as a random access memory (RAM), and a secondary memory 310. The secondary memory 310 may include, for example, a hard disk drive 312 and/or a removable storage drive 314, which may include a magnetic tape drive, an optical disk drive, or

the like. The removable storage drive 314 reads from and/or writes to a removable storage unit 318 in a well-known manner. The removable storage unit 318 may include a magnetic tape, optical disk, or the like, which is read by and written to by removable storage drive 314. As will be appreciated by persons skilled in the relevant art(s), the removable storage unit 318 includes a computer readable storage medium having stored therein computer executable program code instructions and/or data.

[0042] In an alternative embodiment, the secondary memory 310 may additionally or alternatively include other similar devices for allowing computer programs or other instructions to be loaded into the computing device 300. Such devices can include, for example, a removable storage unit 322 and an interface 320. Examples of a removable storage unit 322 and interface 320 include a removable memory chip (such as an EPROM or PROM) and associated socket, and other removable storage units 322 and interfaces 320 which allow software and data to be transferred from the removable storage unit 322 to the computer system 300.

[0043] The computing device 300 also includes at least one communication interface 324. The communication interface 324 allows software and data to be transferred between computing device 300 and external devices via a communication path 326. In various embodiments, the communication interface 324 permits data to be transferred between the computing device 300 and a data communication network, such as a public data or private data communication network. The communication interface 324 may be used to exchange data between different computing devices 300 which such computing devices 300 form part an interconnected computer network. Examples of a communication interface 324 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 324 may be wired or may be wireless. Software and data transferred via the communication interface 324 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by communication interface 324. These signals are provided to the communication interface via the communication path 326.

[0044] Optionally, the computing device 300 further includes a display interface 302 which performs operations for rendering images to an associated display 330 and an audio interface 332 for performing operations for playing audio content via associated speaker(s) 334.

[0045] As used herein, the term "computer program product" may refer, in part, to removable storage unit 318, removable storage unit 322, a hard disk installed in hard disk drive 312, or a carrier wave carrying software over communication path 326 (wireless link or cable) to communication interface 324. Computer readable storage media refers to any non-transitory tangible storage medium that provides recorded instructions and/or data to the computing device 300 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 300. 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 300 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.

[0046] The computer programs (also called computer program code) are stored in main memory 308 and/or secondary memory 310. Computer programs can also be received via the communication interface 324. Such computer programs, when executed, enable the computing device 300 to perform one or more features of embodiments discussed herein. In various embodiments, the computer programs, when executed, enable the processor 304 to perform features of the above-described embodiments. Accordingly, such computer programs represent controllers of the computer system 300.

[0047] Software may be stored in a computer program product and loaded into the computing device 300 using the removable storage drive 314, the hard disk drive 312, or the interface 320. Alternatively, the computer program product may be downloaded to the computer system 300 over the communications path 326. The software, when executed by the processor 304, causes the computing device 300 to perform functions of embodiments described herein.

[0048] It is to be understood that the embodiment of Figure 3 is presented merely by way of example. Therefore, in some embodiments one or more features of the computing device 300 may be omitted. Also, in some embodiments, one or more features of the computing device 300 may be combined together. Additionally, in some

embodiments, one or more features of the computing device 300 may be split into one or more component parts.

[0049] 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.

[0050] Figure 4 is a schematic diagram 400 illustrating an example of a user authentication system, according to an embodiment. The user authentication system comprises an extracting device 402 configured to extract, from a user enrollment image comprising a first human face image and a first background image, the first human face image and the first background image. The extracting device 402 is also configured to extract, from a user authentication image comprising a second human face image and a second background image, the second human face image and the second background image. The user authentication system further comprises a first score generating device 404 configured to generate, using a trained image spoof model, a first score (S1) associated with the user authentication image. The user authentication system further comprises a second score generating device 406 configured to generate a second score (S2) corresponding to a similarity between the first background image and the second background image. The user authentication system further comprises a third score generating device 408 configured to generate a third score (S3) corresponding to a similarity between the first human face image and the second human face image. Further, the user authentication system comprises an authenticating device 410 configured to authenticate the user based on the first score (S1), the second score (S2) and the third score (S3).

[0051] The authenticating device 410 may be further configured to positively authenticate the user on a condition that S1 is lower than a first threshold; S2 is lower than a second threshold and S3 is greater than a third threshold.

[0052] The first threshold, the second threshold and the third threshold may be separately determined based on a receiver operating characteristic (ROC) curve.

[0053] The extracting device 402 may be further configured to apply a face detection method to the user enrollment image to generate a face bounding box that demarcates the first human face image such that an area of the user enrollment image within the face bounding box corresponds to the first human face image and an area of the user enrollment image outside the face bounding box corresponds to the first background image.

[0054] The extracting device 402 may be further configured to apply the face detection method to the user authentication image to generate another face bounding box that demarcates the second human face image such that an area of the user authentication image within the other face bounding box corresponds to the second human face image and an area of the user authentication image outside the other face bounding box corresponds to the second background image.

[0055] The second score generating device 406 may be further configured to perform a pixel-wise comparison between the first background image and the second background image to determine the similarity between the first background image and the second background image.

[0056] The image spoof model may be trained using a CNN with a softmax function.

[0057] The third score generating device 408 may be further configured to extract, using a trained CNN, first features (F1) corresponding to the first human face image. The third score generating device 408 may also be configured to extract, using the trained CNN, second features (F2) corresponding to the second human face image. Further, the third score generating device 408 may be configured to generate the third score (S3) based on a cosine similarity between the first features (F1) and the second features (F2).

[0058] 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. A user authentication method, comprising:

extracting, from a user enrollment image comprising a first human face image and a first background image, the first human face image and the first background image;

extracting, from a user authentication image comprising a second human face image and a second background image, the second human face image and the second background image;

generating, using a trained image spoof model, a first score (S1) associated with the user authentication image;

generating a second score (S2) corresponding to a similarity between the first background image and the second background image;

generating a third score (S3) corresponding to a similarity between the first human face image and the second human face image; and

authenticating the user based on the first score (S1), the second score (S2) and the third score (S3), wherein the user is positively authenticated on a condition that S1 is lower than a first threshold; S2 is lower than a second threshold and S3 is greater than a third threshold.

2. The method as claimed in claim 1, wherein the first threshold, the second threshold and the third threshold are separately determined based on a receiver operating characteristic (ROC) curve.

3. The method as claimed in any one of the preceding claims, wherein:

the user enrollment image is obtained during an initial user enrollment process and the user authentication image is obtained during a subsequent user authentication process;

the user enrollment image comprises a face photograph of the user or a photograph of the user's identification document that is taken during the initial user enrollment process; and

the user authentication image comprises another face photograph of the user or another photograph of the user's identification document that is taken during the subsequent user authentication process.

4. The method as claimed in any one of the preceding claims, wherein the step of extracting the first human face image and the first background image from the user enrollment image comprises:

applying a face detection method to the user enrollment image to generate a face bounding box that demarcates the first human face image such that an area of the user enrollment image within the face bounding box corresponds to the first human face image and an area of the user enrollment image outside the face bounding box corresponds to the first background image.

5. The method as claimed in claim 4, wherein the step of extracting the second human face image and the second background image from the user authentication image comprises:

applying the face detection method to the user authentication image to generate another face bounding box that demarcates the second human face image such that an area of the user authentication image within the other face bounding box corresponds to the second human face image and an area of the user authentication image outside the other face bounding box corresponds to the second background image.

6. The method as claimed in any one of the preceding claims, wherein the step of generating the second score (S2) comprises a pixel-wise comparison between the first background image and the second background image to determine the similarity between the first background image and the second background image.

7. The method as claimed in any one of the preceding claims, further comprising:

training the image spoof model using a CNN with a softmax function.

8. The method as claimed in any one of the preceding claims, wherein the step of generating the third score (S3) comprises:

extracting, using a trained CNN, first features (F1) corresponding to the first human face image;

extracting, using the trained CNN, second features (F2) corresponding to the second human face image; and

generating the third score (S3) based on a cosine similarity between the first features (F1) and the second features (F2).

9. A user authentication system, comprising:

an extracting device configured to:

extract, from a user enrollment image comprising a first human face image and a first background image, the first human face image and the first background image; and

extract, from a user authentication image comprising a second human face image and a second background image, the second human face image and the second background image;

a first score generating device configured to generate, using a trained image spoof model, a first score (S1) associated with the user authentication image;

a second score generating device configured to generate a second score (S2) corresponding to a similarity between the first background image and the second background image;

a third score generating device configured to generate a third score (S3) corresponding to a similarity between the first human face image and the second human face image; and

an authenticating device configured to authenticate the user based on the first score (S1), the second score (S2) and the third score (S3), wherein the authenticating device is further configured to positively authenticate the user on a condition that S1 is lower than a first threshold; S2 is lower than a second threshold and S3 is greater than a third threshold.

10. The system as claimed in claim 9, wherein the first threshold, the second threshold and the third threshold are separately determined based on a receiver operating characteristic (ROC) curve.

11. The system as claimed in any one of claims 9 to 10, wherein the extracting device is further configured to apply a face detection method to the user enrollment image to generate a face bounding box that demarcates the first human face image such that an area of the user enrollment image within the face bounding box corresponds to the first human face image and an area of the user enrollment image outside the face bounding box corresponds to the first background image.

12. The system as claimed in claim 11, wherein the extracting device is further configured to apply the face detection method to the user authentication image to generate another face bounding box that demarcates the second human face image such that an area of the user authentication image within the other face bounding box

corresponds to the second human face image and an area of the user authentication image outside the other face bounding box corresponds to the second background image.

13. The system as claimed in any one of claims 9 to 12, wherein the second score generating device is further configured to perform a pixel-wise comparison between the first background image and the second background image to determine the similarity between the first background image and the second background image.

14. The system as claimed in any one of claims 9 to 13, wherein the image spoof model is trained using a CNN with a softmax function.

15. The system as claimed in any one of claims 9 to 14, wherein the third score generating device is further configured to:

extract, using a trained CNN, first features (F1) corresponding to the first human face image;

extract, using the trained CNN, second features (F2) corresponding to the second human face image; and

generate the third score (S3) based on a cosine similarity between the first features (F1) and the second features (F2).