(12)Indian Patent Application

(21) Application Number: 202341087040

(22) Filing Date: 19/12/2023 (43) Publication Date: 20/06/2025

(71) Applicant(s): L&T TECHNOLOGY SERVICES LIMITED

(72) Inventor(s): Babu, Akshaya Poothanappilli

(51) International Classifications: G06F 21/32 H04L 51/046 H04W 8/18 H04M 1/72448 G06F 21/36

(54) Title: METHOD AND SYSTEM OF PERFORMING FACE RECOGNITION BASED AUTHENTICATION

(57) Abstract: A method (600) and system (100) of performing face recognition-based authentication is disclosed. A processor (104) receives a registration input image (300A) and an input image for a plurality of registered users. The input image and the registration input image (300A) are preprocessed. A user ID is generated based on the registration input image (300A). A portion of a set of predefined features in the input image comprising at least a portion of a face of a user is detected. The user is authenticated based on a match between the input image and a predefined user data. Upon authentication, a user ID is displayed corresponding to the input image on a display.

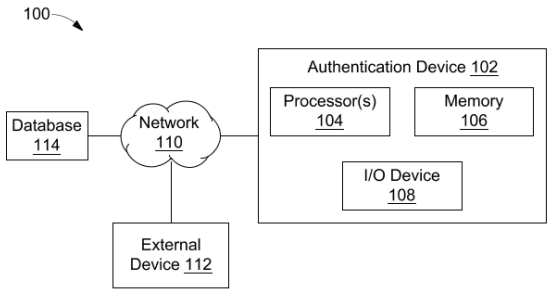

FIG. 1

FORM 2

THE PATENTS ACT 1970
(39 OF 1970)
&
The Patent Rules, 2003

Complete Specification
(See Section 10 and Rule 13)

1. TITLE OF THE INVENTION

METHOD AND SYSTEM OF PERFORMING FACE RECOGNITION BASED AUTHENTICATION

2. APPLICANT(S)

(a) NAME : **L&T TECHNOLOGY SERVICES LIMITED**
(b) NATIONALITY : **INDIAN**
(c) ADDRESS : **DLF IT SEZ Park, 2nd Floor – Block 3**
1/124, Mount Poonamallee Road,
Ramapuram, Chennai – 600 089,
INDIA.

3. PREAMBLE TO THE DESCRIPTION

COMPLETE

The following specification particularly describes the invention and the manner in which it is to be performed

DESCRIPTION

Technical Field

[001] This disclosure relates generally to image processing methodology and more particularly to a method and system of performing face recognition-based authentication using image processing methodology.

BACKGROUND

[002] Face recognition methods are extensively employed to enhance security in various essential operations, such as offices, laptops, and other secure areas. Therefore, it is crucial for the system to be user-friendly, avoid complex functionalities, and incorporate the latest technological advancements. Face recognition operates by capturing and analysing facial features to establish the identity of individuals. Conventional algorithms employ a comparison of facial features detected in a current image frame with the facial features previously registered. However, conventional face recognition algorithms indeed confront significant challenges, particularly concerning accuracy. In practical scenarios, faces might appear at extreme angles or be obscured by accessories like masks or goggles, posing a considerable hurdle for accurate recognition. Images having multiple faces or obscured facial features may fail to get authenticated. Therefore, conventional algorithms burden the users to either reregister in case they change their facial look by changing their hairstyle, sporting a moustache or a beard, or wearing sunglasses. Further, registration of users may include creation of a database. However, creation of such database may be resource extensive and may lead to privacy issues. Privacy concerns may arise due to the sensitive nature of biometric data, prompting the need for secure storage and handling of image data to prevent unauthorized access or misuse.

[003] Accordingly, such limitations impact the real-world applicability of conventional face recognition systems, particularly in scenarios where users may not consistently present an ideal and an unobstructed facial view.

[004] Therefore, there is a requirement for an efficient and effective methodology for performing face recognition-based authentication.

SUMMARY OF THE INVENTION

[005] In an embodiment, a method for performing face recognition-based authentication is disclosed. The method may include, detecting, by a processor, a portion of a set of predefined

features in an input image comprising at least a portion of a face of a user. The method may further include authenticating by the processor, the user based on a match between the input image and a predefined user data. In an embodiment, the predefined user data may include a plurality of user IDs. In an embodiment, each of the plurality of user IDs may be associated to a registered user from a plurality of registered users. In an embodiment, the generation of each of the plurality of user IDs may include receiving by the processor, a registration input image for each of the plurality of registered users comprising a front view of a face of a corresponding registered user. The generation of each of the plurality of user IDs may further include generating by the processor, a first set of images for each of the plurality of registered users based on the registration input image using a first deep learning model. In an embodiment, each of the first set of images may include a unique angle of the face of the corresponding registered user. In an embodiment, the first deep learning model may be trained to generate a plurality of images from the registration input image based on the set of predefined features. The generation of each of the plurality of user IDs may further include generating by the processor, a second set of images for each of the plurality of registered user based on the registration input image using a second deep learning model. In an embodiment, the second set of images may be generated based on occlusion of one facial feature from a set of predefined facial features. In an embodiment, the second deep learning model may be trained to generate a plurality of images from the registration input image based on masking one of the set of predefined facial features in the registration input image. The generation of each of the plurality of user IDs may further include generating by the processor, a first set of embeddings for each of the plurality of registered user based on the first set of images, a second set of embeddings based on the second set of images and third embeddings based on the registration input image using a third deep learning model. The generation of each of the plurality of user IDs may further include determining by the processor, weighted embeddings for each of the plurality of registered user based on a weighted average of the first set of embeddings, the second set of embeddings and the third embeddings. The generation of each of the plurality of user IDs may further include associating by the processor, the weighted embeddings to a user ID associated to the corresponding registered user from the plurality of registered users. The method may further include, upon authentication, displaying by the processor, a user ID corresponding to the input image on a display.

[006] In another embodiment, a system of performing face recognition-based authentication is disclosed. The system may include a processor and a memory communicably coupled to the processor, wherein the memory may store processor-executable instructions, which when

executed by the processor may cause the processor to detect a portion of the set of predefined features in an input image comprising at least a portion of a face of the user. The processor may further authenticate the user based on the match between the input image and a predefined user data. In an embodiment, the predefined user data may include a plurality of user IDs. In an embodiment, each of the plurality of user IDs may be associated to a registered user from a plurality of registered users. In an embodiment, the generation of each of the plurality of user IDs may include, the processor may receive a registration input image for each of the plurality of registered users that may include a front view of a face of a corresponding registered user. In order to generate each of the plurality of user IDs, the processor may further generate a first set of images for each of the plurality of registered users based on the registration input image using a first deep learning model. In an embodiment, each of the first set of images may include a unique angle of the face of the corresponding registered user. In an embodiment, the first deep learning model may be trained to generate a plurality of images from the registration input image based on the set of predefined features. Further, to generate each of the plurality of user IDs, the processor may further generate a second set of images based on the registration input image using a second deep learning model. In an embodiment, the second set of images may be generated based on occlusion of one facial features from a set of predefined facial features. In an embodiment, the second deep learning model may be trained to generate a plurality of images from the registration input image based on masking one of the set of predefined facial features in the registration input image. The generation of each of the plurality of user IDs may further include generation of a first set of embeddings for each of the plurality of registered user based on the first set of images, a second set of embeddings based on the second set of images and third embeddings based on the registration input image using a third deep learning model. Further, for the generation of each of the plurality of user IDs, the processor may determine weighted embeddings for each of the plurality of registered user based on a weighted average of the first set of embeddings, the second set of embeddings and the third embeddings. Further, for the generation of each of the plurality of user IDs, the processor may associate the weighted embeddings to a user ID associated to the corresponding registered user from each of the plurality of registered user. Upon the authentication of the user, the processor may display a user ID corresponding to the input image on display upon authentication.

[007] Various objects, features, aspects, and advantages of the inventive subject matter will become more apparent from the following detailed description of preferred embodiments, along with the accompanying drawing figures in which like numerals represent like components.

BRIEF DESCRIPTION OF THE DRAWINGS

[008] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, serve to explain the disclosed principles.

[009] **FIG. 1** illustrates a block diagram of an exemplary authentication system for face recognition-based authentication, in accordance with an embodiment of the present disclosure.

[010] **FIG. 2** illustrates a functional block diagram of an authentication device, in accordance with an embodiment of the present disclosure.

[011] **FIG. 3A** illustrates an exemplary registration input image, in accordance with an embodiment of the present disclosure.

[012] **FIG. 3B** illustrates exemplary first set of images, in accordance with an embodiment of the present disclosure.

[013] **FIG. 3C** illustrates exemplary second set of images, in accordance with an embodiment of the present disclosure.

[014] **FIG. 4** illustrates a flowchart of a method of pre-processing an image, in accordance with an embodiment of the present disclosure.

[015] **FIG. 5** illustrates a flowchart of a method of generating user IDs, in accordance with an embodiment of the present disclosure.

[016] **FIG. 6** illustrates a flowchart of a method of performing face recognition-based authentication, in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION OF THE DRAWINGS

[017] Exemplary embodiments are described with reference to the accompanying drawings. Wherever convenient, the same reference numbers are used throughout the drawings to refer to the same or like parts. While examples and features of disclosed principles are described herein, modifications, adaptations, and other implementations are possible without departing from the scope of the disclosed embodiments. It is intended that the following detailed description be considered exemplary only, with the true scope being indicated by the following claims. Additional illustrative embodiments are listed.

[018] Further, the phrases “in some embodiments”, “in accordance with some embodiments”, “in the embodiments shown”, “in other embodiments”, and the like mean a particular feature,

structure, or characteristic following the phrase is included in at least one embodiment of the present disclosure and may be included in more than one embodiment. In addition, such phrases do not necessarily refer to the same embodiments or different embodiments. It is intended that the following detailed description be considered exemplary only, with the true scope being indicated by the following claims.

[019] Referring now to **FIG. 1**, a block diagram of an exemplary authentication system 100 for face recognition-based authentication is illustrated, in accordance with an embodiment of the present disclosure. The authentication system 100 may include an authentication device 102, an external device 112, and a database 114 communicably coupled to each other through a wired or wireless communication network 110. The authentication device 102 may include a processor 104, a memory 106 and an input/output (I/O) device 108.

[020] In an embodiment, examples of processor(s) 104 may include, but are not limited to, an Intel® Itanium® or Itanium 2 processor(s), or AMD® Opteron® or Athlon MP® processor(s), Motorola® lines of processors, Nvidia®, FortiSOC™ system on a chip processors or other future processors.

[021] In an embodiment, the memory 106 may store instructions that, when executed by the processor 104, and cause the processor 104 to authenticate an entity also referred to hereinafter as a user based on an input face image of the entity, as discussed in more detail below. In an embodiment, the memory 106 may be a non-volatile memory or a volatile memory. Examples of non-volatile memory may include but are not limited to, a flash memory, a Read Only Memory (ROM), a Programmable ROM (PROM), Erasable PROM (EPROM), and Electrically EPROM (EEPROM) memory. Further, examples of volatile memory may include but are not limited to, Dynamic Random Access Memory (DRAM), and Static Random-Access memory (SRAM).

[022] In an embodiment, the I/O device 108 may comprise of variety of interface(s), for example, interfaces for data input and output devices, and the like. The I/O device 108 may facilitate inputting of instructions by a user communicating with the authentication device 102. In an embodiment, the I/O device 108 may be wirelessly connected to the authentication device 102 through wireless network interfaces such as Bluetooth®, infrared, or any other wireless radio communication known in the art. In an embodiment, the I/O device 108 may be connected to a communication pathway for one or more components of the authentication device 102 to

facilitate the transmission of inputted instructions and output results of data generated by various components such as, but not limited to, processor(s) 104 and memory 106. In an embodiment, the I/O device 108 may include an imaging device (not shown). In an embodiment, the imaging device may generally include one or more imaging sensors to generate an input image or a registration input image of an entity.

[023] In an embodiment, the database 114 may be enabled in a cloud or a physical database and may store an input image, a registration input image for each of a plurality of registered users, and training data. In an embodiment, the training data may include a plurality of images that may be output by the authentication device 102. In an embodiment, the database 114 may store data input by an external device 112 or output generated by the authentication device 102. Further, in some embodiment, the database 114 may include the images generated by the imaging device of the I/O device 108.

[024] In an embodiment, the communication network 110 may be a wired or a wireless network or a combination thereof. The network 110 can be implemented as one of the different types of networks, such as but not limited to, ethernet IP network, intranet, local area network (LAN), wide area network (WAN), the internet, Wi-Fi, LTE network, CDMA network, 5G and the like. Further, network 110 can either be a dedicated network or a shared network. The shared network represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), and the like, to communicate with one another. Further network 110 can include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, and the like.

[025] In an embodiment, the authentication device 102 may receive a request for performing face recognition-based authentication from the external device 112 through the network 110. In an embodiment, the authentication device 102 and the external device 112 may be a computing system, including but not limited to, a smart phone, a laptop computer, a desktop computer, a notebook, a workstation, a portable computer, a handheld, a scanner, or a mobile device. In an embodiment, the authentication device 102 may be, but not limited to, in-built into the external device 112 or may be a standalone computing device.

[026] In an embodiment, the authentication device 102 may perform various processing for performing face recognition-based authentication. By way of an example, the authentication device 102 may generate a plurality of user IDs based on registration of a plurality of users. In

order to register a user, the authentication device 102 may receive a registration input image that may include a front view of a face of the user being registered. In an embodiment, the registration input image may be captured by the imaging device of the I/O device 108. It is to be noted that the authentication system 102 may not be limited to authenticating human entities. In some embodiments, the authentication system 102 may be used to authenticate entities such as animals, birds, etc.

[027] The authentication device 102 may pre-process the registration input image based on determination of a bounding box based on detection of a face in the registration input image. In an embodiment, the bounding box may be generated using an object detection methodology or a deep learning based object detection methodology. In an embodiment, the deep learning based object detection methodology used may be such as, but not limited to, YOLO, SSD, R-CNN, etc. that may be pre-trained to determine face of an entity. Further, the authentication device 102 may generate a resized input image by cropping the registered input image based on the bounding box and based on a predefined size. In an embodiment, the registered input image may be cropped based on the predefined size to generate the resized input image. The authentication device 102 may further determine a mean of pixels of the resized input image and a standard deviation of each of the pixels of the resized input image. The authentication device 102 may then generate a standardised image from the resized input image by subtracting the mean from each of the pixels and dividing each of the pixels by the standard deviation.

[028] Upon pre-processing of the registration input image, the authentication device 102 may generate a first set of images based on the pre-processed registration input image using a first deep learning model. In an embodiment, each of the first set of images may include a unique angle of the face of the user. In an embodiment, the first deep learning model may be trained to generate a plurality of images from the registration input image based on a set of predefined features. In an embodiment, the set of predefined features may be determined by the first deep learning model based on a training data comprising a plurality of images having faces of entities. Accordingly, the first deep learning model may be trained to distinguish between various entities based on their facial features based on the set of predefined features. The authentication device 102 may further generate a second set of images based on the registration input image using a second deep learning model. Each of the second set of images may be generated based on occlusion of one facial feature from a set of predefined facial features. In an embodiment, the set of predefined facial features may include, but are not limited to, eyes, mouth, nose, ears, chin, etc. The second deep learning model may be trained to generate a

plurality of images from the registration input image based on masking one of the set of predefined facial features in the registration input image.

[029] The authentication device 102 may generate a first set of embeddings based on the first set of images, a second set of embeddings based on the second set of images and third embeddings based on the pre-processed registration input image using a third deep learning model. The authentication device 102 may determine weighted embeddings based on a weighted average of the first set of embeddings, the second set of embeddings and the third embeddings. In an embodiment, the weighted average may be determined based on predefined weights corresponding to each of the first set of embeddings, the second set of embeddings and the third embeddings. The authentication device 102 may associate the weighted embeddings to a user ID associated to the user in order to register the user as a registered user. Similarly, a plurality of user IDs may be determined corresponding to each of the plurality of registered users by the authentication device 102.

[030] The authentication device 102 in order to authenticate a registered user from the plurality of registered users may receive an input image that may include at least a portion of a face of the registered user. In an embodiment, the input image may be a real-time image of the face of the corresponding registered user that may be captured by the imaging device of the I/O device 108. In an embodiment, the input image may be captured as a live video or an image frame by the imagine device of the I/O device 108.

[031] It is to be noted that the authentication device 102 may pre-process the input image as described above as performed when registering a user or an entity as a registered user. Further, the authentication device 102 may further detect a portion of the set of predefined features in the input image comprising at least the portion of a face of the user. In order to authenticate the user, the authentication device 102 may determine input image embeddings based on the portion of the set of predefined features detected in the input image using the third deep learning model.

[032] The authentication device 102 may further authenticate the user based on a match between the input image and a predefined user data. The predefined user data may include a plurality of user IDs. The each of the plurality of user IDs may be associated to a registered user from a plurality of registered users. The authentication device 102 may further determine the weighted embeddings corresponding to which a minimum distance may be determined between the input image embeddings and each of the weighted embeddings in the predefined

user data. The authentication device 102 may determine the user ID from the plurality of user IDs in the predefined user data based on the determination of the weighted embeddings corresponding to which the minimum distance may be determined. In an embodiment, a Euclidian distance may be determined between the input image embeddings and each of the weighted embeddings in the predefined user data.

[033] Further, in an embodiment, the user may be authenticated in case the minimum distance may be less than a predefined threshold. Upon authentication, the authentication device 102 may further display the user ID corresponding to the input image of the user being authenticated on a display of the I/O device 108. In an embodiment, user ID may be name of the registered user. Further, in some embodiments, the authentication device 102 may display the user ID, name of the user and/or the input image on a display of the I/O device 108 corresponding to the user being authenticated.

[034] Referring now to **FIG. 2** a functional block diagram of an authentication device 102, in accordance with some embodiments of the present disclosure is illustrated. In an embodiment, the authentication device 102 may include an image receiving module 202, an image pre-processing module 204, a feature detection module 206, a user ID generation module 207, an embeddings generation module 208 a user authentication module 210, and a display module 212.

[035] The image receiving module 202 may receive images captured by the imaging device during registration of users or authentication of users. Referring now to **FIG. 3A,** an exemplary registration input image 300A, in accordance with some embodiments of the present disclosure is illustrated. The registration input image 300A may include a front view of a face of a user to be registered. Referring back to **FIG. 2**, the image pre-processing module 204 may pre-process the registration input image 300A and may determine a bounding box based on detection of the face in the registration input image 300A. The image pre-processing module 204 may further increase margins of the bounding box based on a predefined percentage. In an embodiment, the predefined percentage may be, but is not limited to, 20% of width and height of the bounding box. The pre-processing module 204 may generate a resized input image by cropping the input image based on the bounding box and based on a predefined size. Accordingly, the resized input image may be generated based on the bounding box and as per the predefined size that may include the face detected. In an embodiment, the predefined size may be but is not limited to 160x160. The image pre-processing module 204 may then

determine a mean of all the pixels of the resized input image and a standard deviation of each of the pixels of the resized input image. The image pre-processing module 204 may then generate a standardized image from the resized input image by subtracting the mean from each of the pixels of the resized image and further dividing each of the pixels by the standard deviation.

[036] Upon pre-processing, the feature detection module 206 may detect a portion of a set of predefined features in the pre-processed image 300A determined by the image pre-processing module 204 after pre-processing. The feature detection module 206 may determine a set of features using a deep learning model that may be trained to distinguish between images containing faces of different entities. In an embodiment, the deep learning model may be pretrained based on images of various entities.

[037] The reference image generation module 207 may generate a first set of images based on the pre-processed registration input image 300A using a first deep learning model. Example of the first deep learning model may include, but is not limited to, Frontalization Generative Adversarial Network (GAN), etc. In an embodiment, the first deep learning model may be trained to generate a first set of images based on the registration input image 300A and based on the set of predefined features determined by the feature detection module 206. The first deep learning model may be trained to determine the first set of images each having the face detected in the pre-processed input image at a predefined angle. In some embodiments, each of the first set of images may be generated to include the face detected in the pre-processed input image at a predefined angle selected from, but is not limited to, a range of +/- 25 degrees, +/- 30 degrees, +/- 45, +/- 60 degrees, +/- 90 degrees of angle in a horizontal axis, a vertical axis or a diagonal axis with respect to a point of centre of the face in the registration input image.

[038] Referring now to **FIG. 3B,** exemplary first set of images 300B are shown, in accordance with an embodiment of the present disclosure. As can be seen, the exemplary first set of images 300B may include a plurality of images 302, 304, 306 each having the face detected in the registration input image 300A at a unique angle. In an embodiment, each of the exemplary first set of images 300B may include the face detected in the registration input image 300A at a unique angle selected from a range of predefined angles. In some embodiment, the range of predefined angles may be selected as +/- 25 degrees, +/- 30 degrees, +/- 45, +/- 60 degrees, +/- 90 degrees of angle in a horizontal axis, a vertical axis, or a diagonal axis with respect to a point of centre of the face in the registration input image 300A. Further, each of the first set of

images may be determined by turning the face detected at each of the range of predefined angles with respect to the face angle detected in the registration input image 300A.

[039] Referring back to **FIG. 2**, the reference image generation module 207 may further generate a second set of images based on the registration input image 300A using a second deep learning model. Example of the second deep learning module may include but is not limited to, autoencoder, context encoders, etc. The second deep learning model may be trained to generate a second set of images from the registration input image 300A based on the detection of a set of predefined facial features in the registration input image 300A. Further, the second deep learning model may generate a second set of images based on the registration input image 300A by masking one of the set of predefined facial features in each of the second set of images.

[040] In an embodiment, each of the second set of images may be generated based on occlusion of one facial feature from the set of predefined facial features. The set of predefined facial features may include, but are not limited to, eyes, mouth, nose, ears, etc.

[041] Referring now to **FIG. 3C,** exemplary second set of images 300C are shown, in accordance with an embodiment of the present disclosure. The second set of images may include a plurality of images 308, 310. In an embodiment, each of the second set of images 308, 310 may be generated by occluding one facial feature from the set of predefined facial features. As shown, exemplary image 308 is generated by occluding or masking the eyes of the entity detected in the registration input image 300A. Further, the exemplary image 310 is generated by occluding or masking the mouth of the entity detected in the registration input image 300A. Further, more images of the second set of images may be generated by masking features such as ears, nose, etc. of the entity detected in the registration input image 300A.

[042] Referring back to **FIG. 2**, the embeddings generation module 208 may further generate a first set of embeddings based on the first set of images 300B, a second set of embeddings based on the second set of images 300C and third embeddings based on the registration input image 300A using a third deep learning model. In an embodiment, examples of the third deep learning model may include but are not limited to squeeze net model, VCG-Net, FaceNet, Mobilenet, etc. In an embodiment, the first set of embeddings may be determined by determining embeddings corresponding to each image (302, 304, 306) in the first set of images 300B and merging each of the embeddings corresponding to each image (302, 304, 306) in the

first set of images 300B together. Further, the second set of embeddings may be determined by determining embeddings corresponding to each image (308, 310) in the second set of images 300C and merging each of the embeddings corresponding to the images (308, 310) in the second set of images 300C together. Further, the third embeddings may be determined by determining embeddings corresponding to the pre-processed registration input image 300A. It may be noted that the embeddings generated by the embeddings generation module 208 may not take any additional storage in the memory 106.

[043] The embeddings generation module 208 may then determine weighted embeddings based on a weighted average of the first set of embeddings, the second set of embeddings, and the third embeddings. The weighted average may be determined based on predefined weights corresponding to each of the first set of embeddings, the second set of embeddings, and the third embeddings. In an embodiment, the third embeddings may be given a weight of 50 percent or 0.5. Further, each image of the first set of embeddings and the second set of embeddings may be given weights based on formula (1) given below:

$$\frac{0.5}{number\ of\ images\ in\ the\ first\ set\ and\ the\ second\ set} \quad \ldots\ldots (1)$$

[044] The user ID generation module 209 may then associate the weighted embeddings to a user ID associated to the entity or the user in order to register the entity or the user as a registered user. Similarly, for each of the plurality of registered users a user ID may be associated to the corresponding weighted embeddings determined for each of the plurality of registered users. In an embodiment, the weighted embeddings may be of size about but is not limited to 128x1. In an embodiment, the weighted embeddings may represent the features from the set of features detected of each of the corresponding registered user. In an embodiment, the authentication module 210 may include a predefined user data including a list of the plurality of registered user and their corresponding weighted embeddings and user IDs.

[045] The image receiving module 202 in order to authenticate an entity to be a registered user from the plurality of registered users may further receive an input image that may include at least a portion of a face of the entity. In an embodiment, the input image may be a real-time image of the face of the corresponding entity that may be captured by the imaging device of the I/O device 108. In an embodiment, the input image may be captured as a frame of a live video captured by the image device of the I/O device 108.

[046] The image pre-processing module 204 may pre-process the input image of the entity in order to authenticate the entity to be a registered user from the plurality of registered users. It is to be noted that the image pre-processing module 204 may pre-process the input image of the entity to be authenticated in similar manner as described above to generate the pre-processed registration input image. It is to be noted that the pre-processed registration input image was generated based on the pre-processing of the registration input image to when registering a user or an entity as a registered user.

[047] Further, the feature detection module 206 in order to authenticate the entity to be a registered user from the plurality of registered users may detect a portion of a set of predefined features in the pre-processed input image comprising at least a portion of a face of the entity. Further, the embeddings generation module 208 may determine input image embeddings based on the portion of the set of predefined features detected in the pre-processed input image using the third deep learning model. In an embodiment, the input embeddings may be of size of about, but is not limited to, 128x1.

[048] Further, the user authentication module 210 may authenticate the entity to be a registered user based on a match between the input image and the predefined user data. The predefined user data may include a plurality of user IDs and their associated weighted embeddings. Each of the plurality of user IDs may be associated with a registered user from a plurality of registered users. The user authentication module 210 may further determine weighted embeddings in the predefined user data corresponding to which a minimum distance may be determined between the input image embeddings and each of the weighted embeddings in the predefined user data. The user authentication module 210 may further determine the user ID from the plurality of user IDs in the predefined user data based on the determination of the weighted embeddings corresponding to which the minimum distance may be determined. In an embodiment, a Euclidean distance may be determined between the input image embeddings and each of the weighted embeddings in the predefined user data.

[049] Further, the entity may be authenticated by the user authentication module 210 as a registered user in case the minimum distance may be less than a predefined threshold. Upon authentication of the entity to be a registered user, the user ID display module 212 may display the user ID determined corresponding to the weighted embeddings corresponding to which the minimum distance is determined. The user ID determined corresponding to the input image of

the entity may be displayed on a display. In an embodiment, the user ID may be name of the registered user being authenticated.

[050] It should be noted that all such aforementioned modules 202-212 may be represented as a single module or a combination of different modules. Further, as will be appreciated by those skilled in the art, each of the modules 202-212 may reside, in whole or in parts, on one device or multiple devices in communication with each other. In some embodiments, each of the modules 202-212 may be implemented as dedicated hardware circuit comprising custom application-specific integrated (ASIC) or gate arrays, off-the-shelf semiconductors such as logic chips, transistors, or other discrete components. Each of the modules 202-212 may also be implemented in a programmable hardware device such as a field programmable gate array (FGPA), programmable array logic, programmable logic device, and so forth. Alternatively, each of the modules 202-212 may be implemented in software for execution by various types of processors (e.g. processor 104). An identified module of executable code may, for instance, include one or more physical or logical blocks of computer instructions, which may, for instance, be organized as an object, procedure, function, or other construct. Nevertheless, the executables of an identified module or component need not to be physically located together but may include disparate instructions stored in different locations which, when joined logically together, include the module, and achieve the stated purpose of the module. Indeed, a module of executable code could be a single instruction, or many instructions, and may even be distributed over several different code segments, among different applications, and across several memory devices.

[051] As will be appreciated by one skilled in the art, a variety of processes may be employed for performing face recognition-based authentication. For example, the exemplary system 100 and the associated authentication device 102 may perform face recognition-based authentication by the processes discussed herein. In particular, as will be appreciated by those of ordinary skill in the art, control logic and/or automated routines for performing the techniques and steps described herein may be implemented by the system 100 and the associated authentication device 102 either by hardware, software, or combinations of hardware and software. For example, suitable code may be accessed and executed by the one or more processors on the system 100 to perform some or all of the techniques described herein. Similarly, application-specific integrated circuits (ASICs) configured to perform some, or all

of the processes described herein may be included in the one or more processors on the system 100.

[052] Referring now to **FIG. 4,** a flowchart of a method 400 of pre-processing an image is illustrated, in accordance with an embodiment of the present disclosure. In an embodiment, method 300 may include a plurality of steps that may be performed by the processor 104 to preprocess the image captured by the imaging device. It is to be noted that the image captured may be an input image of the entity to be authenticated or the registration input image captured to register an entity as a registered user.

[053] **FIG. 4** is explained in conjunction with **FIGs. 1** and **2**. Each step of the method 400 may be executed by various modules, of the authentication device 102.

[054] At step 402, a bounding box may be determined based on detection of a face in the image captured by the imaging device.

[055] Further at step 404, a resized image may be generated by cropping the image based on the bounding box and based on a predefined size. It is to be noted that a cropped image may be determined by expanding the size of the bounding box by a predefined margin. In an embodiment, the height and width of the bounding box may be expanded by 20% predefined margin to generate the cropped input image including the face detected of the entity. Further, from the cropped input image a resized image may be determined that may be of a predefined size such as, but not limited to, 160x160.

[056] Further at step 406, a mean of each pixel of the resized image and a standard deviation of each of the pixels of the resized image may be determined.

[057] Further at step 408, a standardised image from the resized image may be generated by subtracting the mean from each of the pixels and dividing each of the pixels by the standard deviation.

[058] Referring now to **FIG**. **5**, a flowchart of a method 500 of generating user IDs is illustrated, in accordance with an embodiment of the present disclosure. In an embodiment, method 500 may include a plurality of steps that may be performed by the processor 104 to generate user IDs based on the pre-processing of the input image or the registration input image as described above in method 400.

[059] **FIG. 5** is explained in conjunction with **FIGs. 1** and **2**. Each step of the method 300 may be executed by various modules, of the authentication device 102.

[060] At step 502, a registration input image may be received that may include a front view of a face of a corresponding entity or a user to be registered. In an embodiment, the imaging device may capture an image comprising a front view of a face of the corresponding entity to be registered. The image captured may be pre-processed to generate the registration input image based on the methodology described in flowchart 400 of **FIG. 4**.

[061] Further at step 504, a first set of images may be generated based on the registration input image using a first deep learning module. Each of the first set of images may include a unique angle of the face of the corresponding registered user. In an embodiment, the first deep learning module may be trained to generate a plurality of images from the registration input image based on the set of predefined features.

[062] Further at step 506, a second set of images may be generated based on the registration input image using a second deep learning model. In an embodiment, each of the second set of images may be generated based on occlusion of one facial feature from a set of predefined facial features. In an embodiment, the second deep learning model may be trained to generate a plurality of images from the registration input image by masking one of the set of predefined facial features in the registration input image.

[063] Further at step 508, a first set of embeddings may be generated based on the first set of images. Further, a second set of embeddings may be generated based on the second set of images and third embeddings may be generated based on the registration input image. It is to be noted that the first set of embeddings, the second set of embeddings and the third embeddings may be determined using a third deep learning model. In an embodiment, the third deep learning model may be a, but not limited to, sqeezenet model.

[064] Further at step 510, weighted embeddings may be determined based on a weighted average of the first set of embeddings, the second set of embeddings and the third embeddings. In an embodiment, the weighted average may be determined based on pre-defined weights assigned to each of the first set of embeddings, the second set of embeddings and the third embeddings. In an embodiment, the third embeddings are assigned a weight of about 0.5, further each of the first set of embeddings and the second set of embeddings may be assigned a weight determined based on the formula (1) mentioned above.

[065] Further at step 512, the weighted embeddings may be associated to a user ID associated to the corresponding registered user.

[066] Referring now to **FIG. 6,** a flowchart of a method 600 of performing face recognition-based authentication, in accordance with an embodiment of the present disclosure is illustrated. In an embodiment, method 600 may include a plurality of steps that may be performed by the processor 104 to perform face recognition-based authentication based on the plurality of registered user IDs as described above in method 500.

[067] **FIG. 6** is explained in conjunction with **FIGs. 1** and **2**. Each **s**tep of the method 600 may be executed by various modules, of the authentication device 102.

[068] At step 602, a portion of a set of predefined features may be detected in an input image that may include at least a portion of a face of a user. It is to be noted that the input image may be captured by the imaging device and may be pre-processed based on the methodology described in flowchart 400 of **FIG. 4**. The portion of the set of predefined features in the input image may be detected by a deep learning model. In an embodiment, the set of predefined features may be determined by the deep learning model when being trained to distinguish between various images of entities based on their facial features.

[069] Further at step 604, the user input image embeddings may be determined based on the portion of the set of predefined features in the input image using the deep learning model. Further, at step 606, a distance between each of the weighted embeddings in the predefined user data and the input image embeddings may be determined. Further, the weighted embeddings corresponding to which a minimum distance is determined may be selected. Further, at step 608, the user authentication module 210 may determine if the minimum distance is less than a predefined threshold value.

[070] At step 610 in case the minimum distance is determined to be less than the predefined threshold value at step 608, the user may be authenticated. Further, a user ID may be determined from the plurality of user IDs in the predefined user data based on the determination of the weighted embeddings corresponding to which the minimum distance is determined.

[071] Further at step 612, a user ID corresponding to the input image may be displayed on a display. In an embodiment, a user authentication successful notification may be displayed on the display. In an embodiment, the user ID may be name of the registered user being

authenticated. Further, in some embodiments, the authentication device 102 may display the user ID, name of the user and/or the input image on a display of the I/O device 108 corresponding to the user being authenticated.

[072] In case, at step 608, the minimum distance is determined to be greater than the predefined threshold then a user authentication failure notification may be displayed on the display.

[073] Thus, the disclosed method and system try to overcome the various technical problems explained earlier when performing face recognition-based authentication.

[074] As will be appreciated by those skilled in the art, the techniques described in the various embodiments discussed above are not routine, or conventional, or well-understood in the art. The techniques discussed above provide for performing face recognition-based authentication.

[075] In light of the above-mentioned advantages and the technical advancements provided by the disclosed method and system, the claimed steps as discussed above are not routine, conventional, or well understood in the art, as the claimed steps enable the following solutions to the existing problems in conventional technologies. Further, the claimed steps bring an improvement in the functioning of the device itself as the claimed steps provide a technical solution to a technical problem.

[076] The specification has described method and system for performing face recognition-based authentication. The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purpose of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[077] It is intended that the disclosure and examples be considered as exemplary only, with a true scope of disclosed embodiments being indicated by the following claims.

WE CLAIM:

1. A method (600) of performing face recognition-based authentication, the method (600) comprising:

detecting (602), by a processor (104), a portion of a set of predefined features in an input image comprising at least a portion of a face of a user;

authenticating, by the processor (104), the user based on a match between the input image and a predefined user data,

wherein the predefined user data comprises a plurality of user IDs, wherein each of the plurality of user IDs is associated to a registered user from a plurality of registered users,

wherein generation of each of the plurality of user IDs comprises:

for each of the plurality of registered users:

receiving (502), by the processor (104), a registration input image comprising a front view of a face of a corresponding registered user;

generating (504), by the processor (104), a first set of images based on the registration input image using a first deep learning model,

wherein each of the first set of images comprises a unique angle of the face of the corresponding registered user, and

wherein the first deep learning model is trained to generate a plurality of images from the registration input image based on the set of predefined features;

generating (506), by the processor (104), a second set of images based on the registration input image using a second deep learning model,

wherein each of the second set of images are generated based on occlusion of one facial feature from a set of predefined facial features, and

wherein the second deep learning model is trained to generate a plurality of images from the registration input image based on masking one of the set of predefined facial features in the registration input image;

generating (508), by the processor (104), a first set of embeddings based on the first set of images, a second set of embeddings

based on the second set of images and third embeddings based on the registration input image using a third deep learning model;

determining (510), by the processor (104), weighted embeddings based on a weighted average of the first set of embeddings, the second set of embeddings and the third embeddings; and

associating (512), by the processor (104), the weighted embeddings to a user ID associated to the corresponding registered user; and

upon the authentication of the user, displaying (612), by the processor (104), a user ID corresponding to the input image on a display.

2. The method (600) as claimed in claim 1, wherein the authentication comprises:

determining (604), by the processor (104), input image embeddings based on the portion of the set of predefined features in the input image using the third deep learning model;

determining (606), by the processor (104), the weighted embeddings corresponding to which a minimum distance is determined between the input image embeddings and each of the weighted embeddings in the predefined user data; and

determining (610), by the processor (104), the user ID from the plurality of user IDs in the predefined user data based on the determination of the weighted embeddings corresponding to which the minimum distance is determined.

3. The method (600) as claimed in claim 2, wherein the user is authenticated in case the minimum distance is less than a predefined threshold.

4. The method (400) as claimed in claim 1, wherein the input image and the registration input image are pre-processed by:

determining (402), by the processor (104), a bounding box based on detection of a face in the corresponding input image;

generating (404) a resized input image, by the processor (104), by cropping the corresponding input image based on the bounding box and based on a predefined size;

determining (406), by the processor (104), a mean of pixels of the resized corresponding input image and a standard deviation of each of the pixels of the resized corresponding input image; and

generating (408) a standardised image from the resized corresponding input image, by the processor (104), by subtracting the mean from each of the pixels and dividing each of the pixels by the standard deviation.

5. The method (600) as claimed in claim 1, wherein the weighted average is determined based on predefined weights corresponding to each of the first set of embeddings, the second set of embeddings and the third embeddings.

6. The method (600) as claimed in claim 1, wherein the set of predefined facial features comprises eyes, mouth, nose, and ears.

7. A system (100) for performing face recognition-based authentication, comprising:

a processor (104); and

a memory (106) communicably coupled to the processor (104), wherein the memory (106) stores processor-executable instructions, which, on execution, cause the processor (104) to:

detect a portion of a set of predefined features in an input image comprising at least a portion of a face of a user;

authenticate the user based on a match between the input image and a predefined user data,

wherein the predefined user data comprises a plurality of user IDs, wherein each of the plurality of user IDs is associated to a registered user from a plurality of registered users,

wherein generation of each of the plurality of user IDs comprises:

for each of the plurality of registered users:

receive a registration input image (300A) comprising a front view of a face of a corresponding registered user;

generate a first set of images (300B) based on the registration input image using a first deep learning model,

wherein each of the first set of images (300B) comprises a unique angle of the face of the corresponding registered user, and

wherein the first deep learning model is trained to generate a plurality of images from the registration input image based on the set of predefined features;

generate a second set of images (300C) based on the registration input image using a second deep learning model,

wherein each of the second set of images are generated based on occlusion of one facial feature from a set of predefined facial features, and

wherein the second deep learning model is trained to generate a plurality of images from the registration input image based on masking one of the set of predefined facial features in the registration input image;

generate a first set of embeddings based on the first set of images, a second set of embeddings based on the second set of images and third embeddings based on the registration input image using a third deep learning model;

determine weighted embeddings based on a weighted average of the first set of embeddings, the second set of embeddings and the third embeddings; and

associate the weighted embeddings to a user ID associated to the corresponding registered user; and

upon the authentication of the user, display a user ID corresponding to the input image on a display.

8. The system (100) as claimed in claim 7, wherein the authentication of the user comprises configuring the processor (104) to:

determine input image embeddings based on the portion of the set of predefined features in the input image using the third deep learning model;

determine the weighted embeddings corresponding to which a minimum distance is determined between the input image embeddings and each of the weighted embeddings in the predefined user data; and

determine the user ID from the plurality of user IDs in the predefined user data based on the determination of the weighted embeddings corresponding to which the minimum distance is determined;

wherein the weighted average is determined based on predefined weights corresponding to each of the first set of embeddings, the second set of embeddings and the third embeddings.

9. The system (100) as claimed in claim 8, wherein the user is authenticated in case the minimum distance is less than a predefined threshold.

10. The system (100) as claimed in claim 7, wherein the processor (104) is configured to pre-process the input image and the registration input image (300A) by:

determining a bounding box based on detection of a face in the input image and in the registration input image (300A);

generating a resized input image and a resized registration input image, by cropping the input image and the registration input image based on the bounding box and based on a predefined size;

determining a mean of pixels of the resized input image and the resized registration input image and a standard deviation of each of the pixels of the resized input image and the resized registration input image; and

generating a standardised image from the resized input image and the resized registration input image, by subtracting the mean from each of the pixels and dividing each of the pixels by the standard deviation.

Dated this 19th day of December 2023

--Digitally Signed--
Bhanu Prasad (INPA No: 3253)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai, TN, 600089.

ABSTRACT

METHOD AND SYSTEM OF PERFORMING FACE RECOGNITION-BASED AUTHENTICATION

A method (600) and system (100) of performing face recognition-based authentication is disclosed. A processor (104) receives a registration input image (300A) and an input image for a plurality of registered users. The input image and the registration input image (300A) are pre-processed. A user ID is generated based on the registration input image (300A). A portion of a set of predefined features in the input image comprising at least a portion of a face of a user is detected. The user is authenticated based on a match between the input image and a predefined user data. Upon authentication, a user ID is displayed corresponding to the input image on a display.

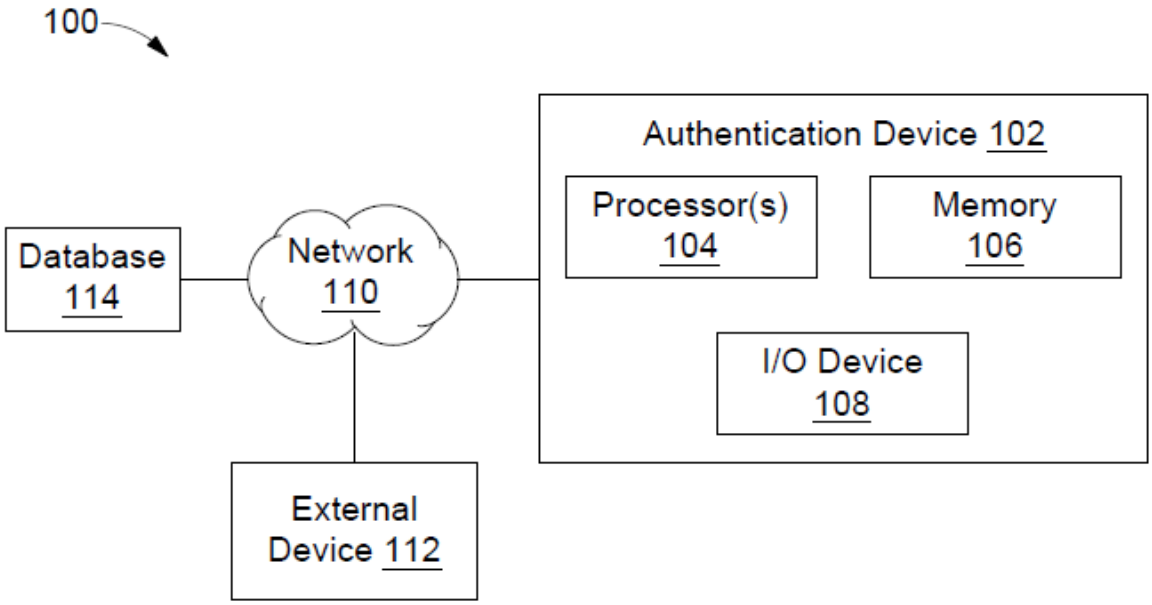

FIG. 1

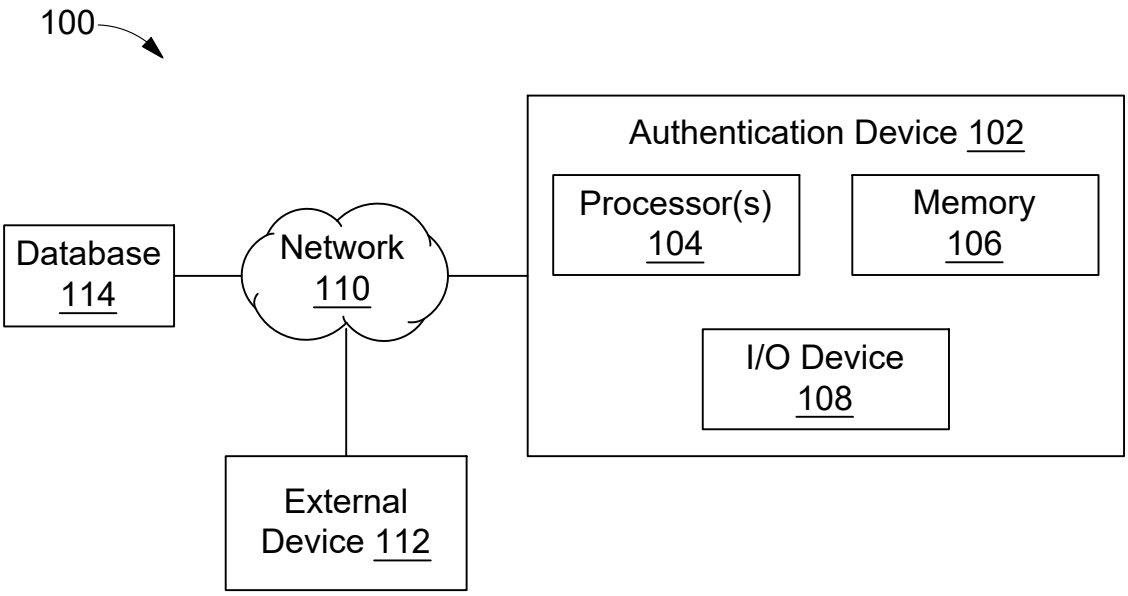

FIG. 1

--Digitally Signed--
Bhanu Prasad (INPA No: 3253)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, TN, Chennai - 600089.

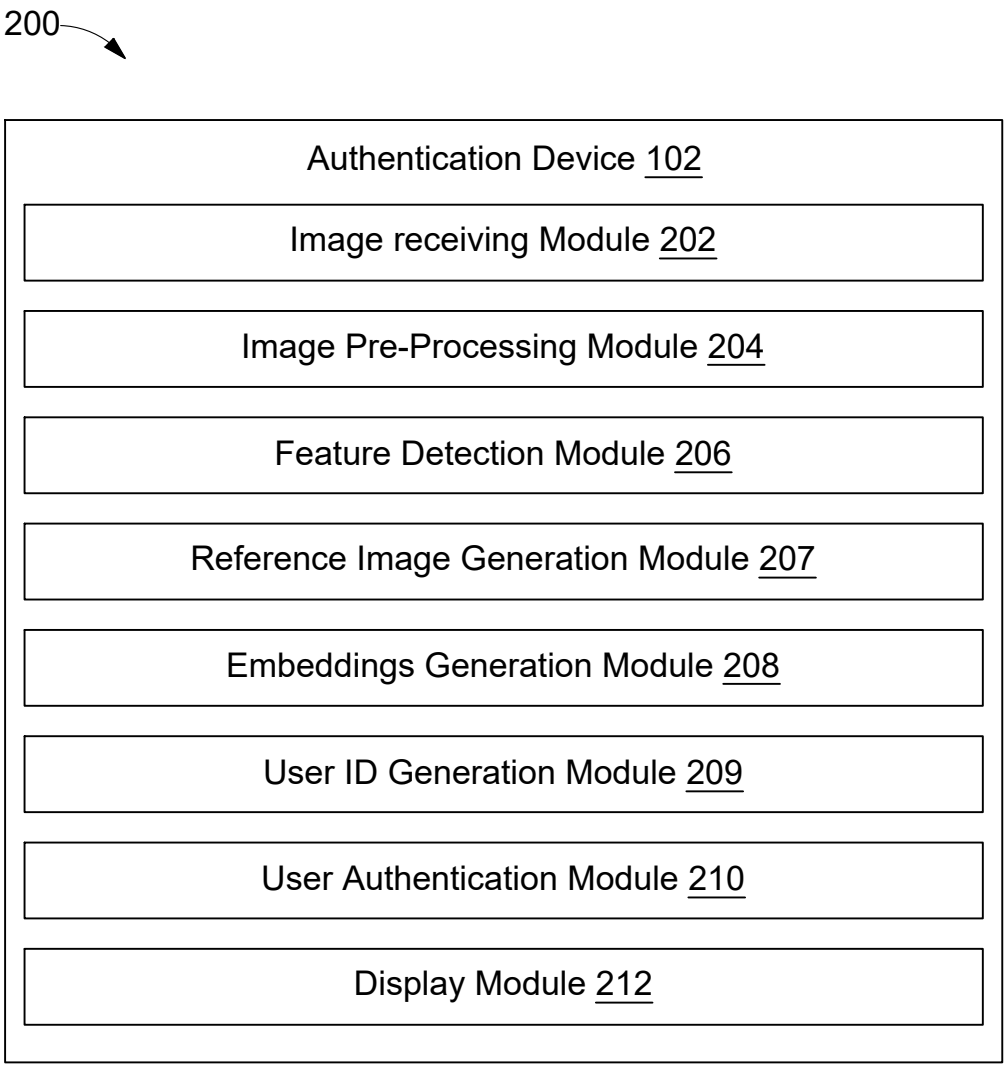

FIG. 2

--Digitally Signed--
Bhanu Prasad (INPA No: 3253)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, TN, Chennai - 600089.

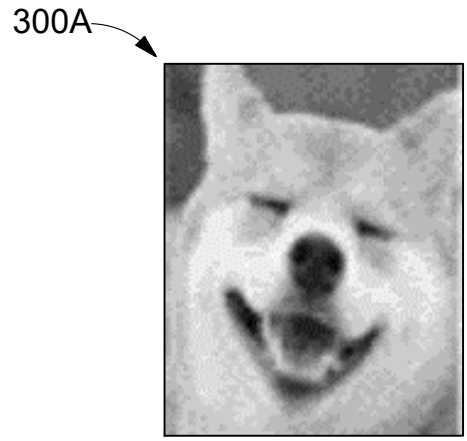

FIG. 3A

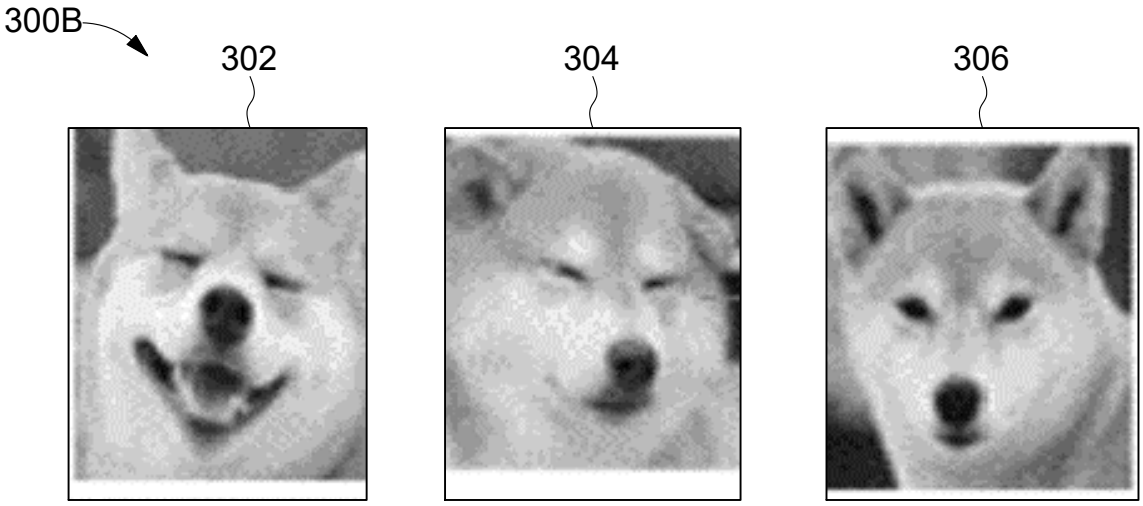

FIG. 3B

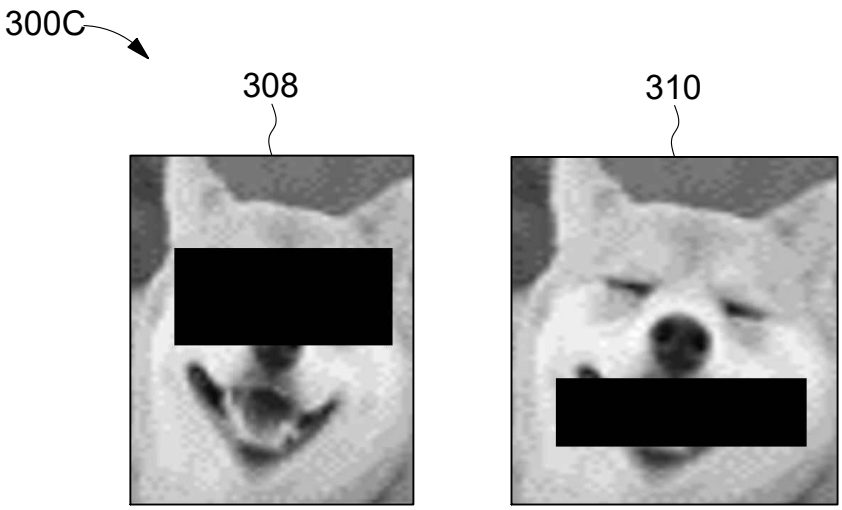

FIG. 3C

--Digitally Signed--
Bhanu Prasad (INPA No: 3253)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, TN, Chennai - 600089.

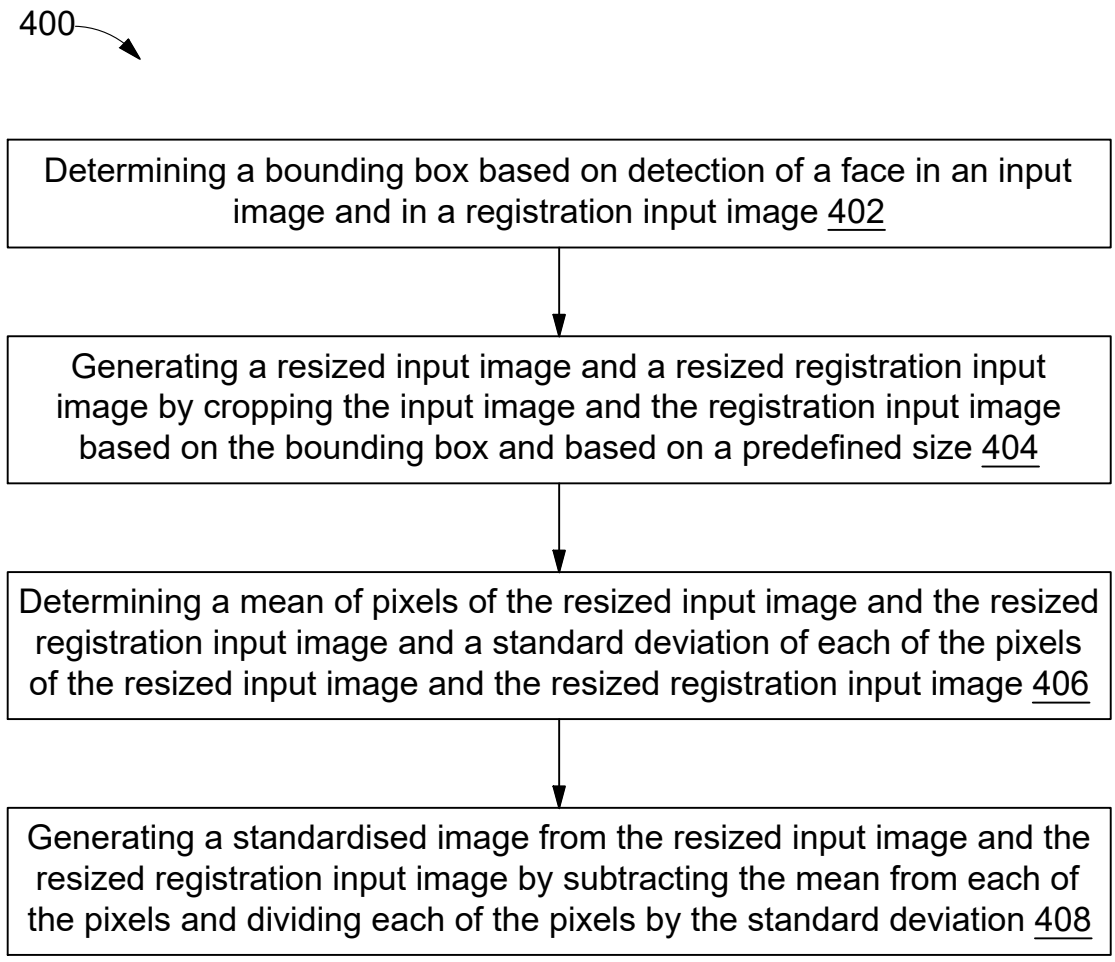

FIG. 4

--Digitally Signed--
Bhanu Prasad (INPA No: 3253)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, TN, Chennai - 600089.

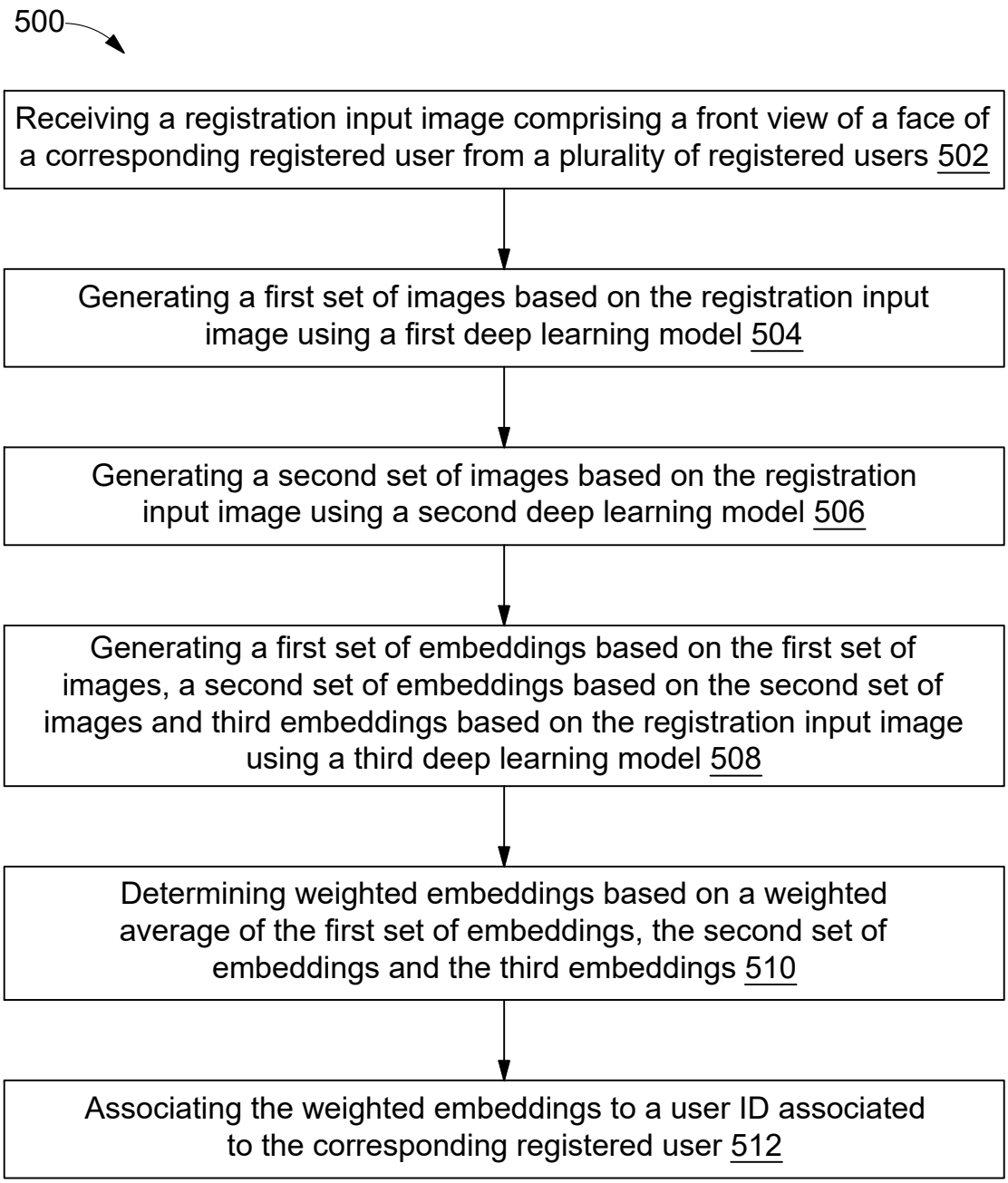

FIG. 5

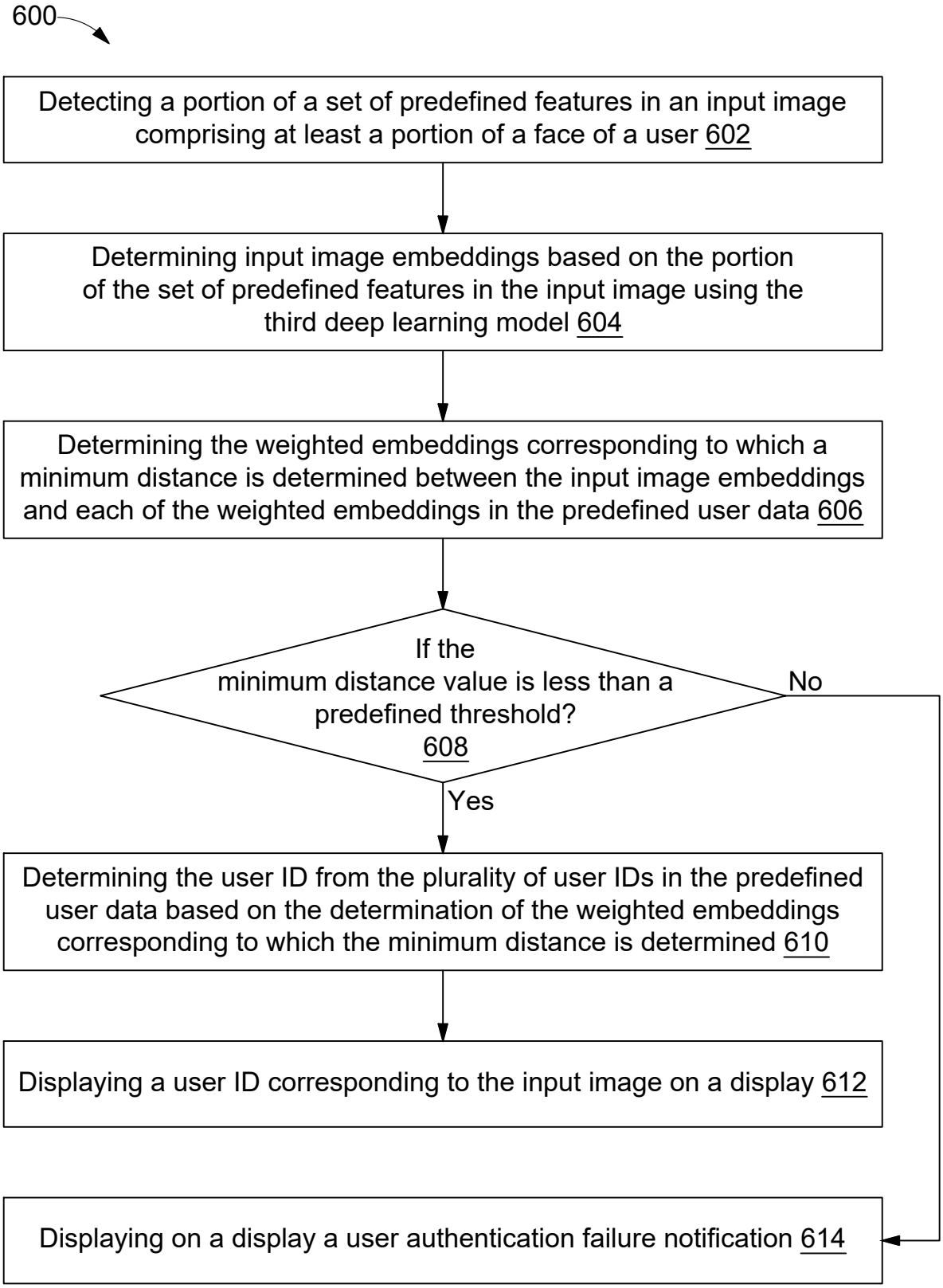

FIG. 6

--Digitally Signed--
Bhanu Prasad (INPA No: 3253)
Head, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, TN, Chennai - 600089.